Jennifer Whitlow_____(print or type)
Authorized Company Representative

Director, Contracts_____(print or type)

End of Award Text

CITATION CODE(S) #
47X4534 2021. 2021. . 296X. AE10. 00. Q00D0000.AF151. H02. DS1409 PLN02, 47X4534 2021. 2021. . 296X. AE10. 00. Q00D0000.AF151. H02. DO2103 PLN01

ITEM NO. (A)	SUPPLIES OR SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
1001	BASE OPS MAINT FPDS SAM	(b) (4) [redacted]			
1002	BASE OPS MAINT FPDS SAM				

21. RECEIVING OFFICE *(Name, symbol and telephone no.)*
Office of GSA IT, 816-823-2313

TOTAL From 300-A(s)

22. SHIPPING POINT
Specified in QUOTE

23. GROSS SHIP WT.

GRAND TOTAL **$8,845,331.00**

24. MAIL INVOICE TO: *(Include zip code)*

General Services Administration (FUND)
The contractor shall follow the invoice instructions identified within the award documentation.

25A. FOR INQUIRIES REGARDING PAYMENT CONTACT:
GSA Finance Customer Support

25B. TELEPHONE NO.
816-926-7287

26A. NAME OF CONTRACTING/ORDERING OFFICER *(Type)*
Chris A Payton

26B. TELEPHONE NO.
(312) 353-0783

26C. SIGNATURE
Chris A Payton 04/20/2021

GENERAL SERVICES ADMINISTRATION | **1. PAYING OFFICE** | **GSA** FORM **300** (REV. 2-93)

ORDER FOR SUPPLIES AND SERVICES

IMPORTANT: See instructions in GSAR 553.370-300-1 for distribution

PAGE 1 OF 1 PAGE(S)

1. DATE OF ORDER	2. ORDER NUMBER	3. CONTRACT NUMBER	4. ACT NUMBER
04/20/2021	47QDCB21F0012	47QDCB19A0008	

FOR GOVERNMENT USE ONLY

5. ACCOUNTING CLASSIFICATION

6. FINANCE DIVISION

FUND	ORG CODE	B/A CODE	O/C CODE	AC	SS	VENDOR NAME
285X	Q00DE000	CP10	25			
FUNC CODE	C/E CODE	PROJ./PROS. NO.	CC-A	MDL	FI	G/L DEBT
AR372	H08					
W/ITEM	CC-B	PRT./CRFT		AI	LC	DISCOUNT

7. TO: CONTRACTOR *(Name, address and zip code)*

(b) (4)

SEVATEC INC.
2815 OLD LEE HIGHWAY
FAIRFAX, VA 22031-4303
United States

(b) (4)

8. TYPE OF ORDER
B. DELIVERY

REFERENCE YOUR

Please furnish the following on the terms specified on both sides of the order and the attached sheets, if any, including delivery as indicated.

This delivery order is subject to instructions contained on this side only of this form and is issued subject to the terms and conditions of the above numbered contract.

C. MODIFICATION NO.
P00000
TYPE OF MODIFICATION:

AUTHORITY FOR ISSUING

9A. EMPLOYER'S IDENTIFICATION NUMBER

(b) (4)

9B. CHECK, IF APPROP WITHHOLD 20%

Except as provided herein, all terms and conditions of the original order, as heretofore modified, remain unchanged.

10A. CLASSIFICATION
Minority Owned Business

10B. TYPE OF BUSINESS ORGANIZATION
C. Corporation

11. ISSUING OFFICE *(Address, zip code, and telephone no.)*
GSA Region 5
Chris A Payton
230 S. DEARBORN STREET
CHICAGO, IL 60604-1505
United States
(312) 353-0783

12. REMITTANCE ADDRESS *(MANDATORY)*
SEVATEC INC.
2815 OLD LEE HIGHWAY
FAIRFAX,VA 22031-4303
United States

13. SHIP TO*(Consignee address, zip code and telephone no.)*
Christopher Mendoza
1800 F STREET NW
Washington DC, DC 20405-0000
United States
202-969-4052

14. PLACE OF INSPECTION AND ACCEPTANCE
Kristen Buzby
1800 F Street NW
Washington, DC 20405
United States

15. REQUISITION OFFICE *(Name, symbol and telephone no.)*
Kristen A. Buzby
GSA Region 15
1800 F ST NW
WASHINGTON, DC 20405-0001
United States
(703) 605-9354

16. F.O.B. POINT	17. GOVERNMENT B/L NO.	18. DELIVERY F.O.B. POINT ON OR BEFORE	19. PAYMENT/DISCOUNT TERMS
Destination		04/21/2022	NET 30 DAYS / 0.00 % 0 DAYS / 0.00 % 0 DAYS

20. SCHEDULE

Project Title: IAE OPS MAINT FPDS SAM
Solicitation Reference: ITSS # ID16210006
Task Order Number: 47QDCB21F0012
BPA Number: 47QDCB19A0008
FSS or GWAC Contract Name and Number: GS35F0687P
Requiring Activity: Office of the Chief Information Officer (OCIO)
Contractor: Sevatec
Contract Type: Combination Firm Fixed Price and T&M
Funding Reference: PR202104160003, QP002
NAICS Code: 541519 Other Computer Related Services
Product Service Code: DA01 IT and Telecom - Business Application/Application Development Support Services (labor)
Inherently Governmental Functions Code: Other Functions
CodesContracting Office: 47QDCB, Funding Agency: 4732, Funding Office: 47QDCB

1. TASK ORDER AWARD

This award is for operations and maintenance support for FPDS and SAM systems. This award is for the BASE PERIOD ONLY.

CONTRACTOR EMPLOYEE NON-DISCLOSURE AGREEMENT

I understand that in the performance of my official duties under contract number TBD (Solicitation No. ID16210006), task/delivery order number ID05180034 between the U.S. General Services Administration and my employer, XYZ, Corp., I may have access to sensitive government or third party contractor information or proprietary business information. I, as a Government contractor, certify that I will not disclose, publish, divulge, release, or make known, in any manner or to any extent, to any individual other than an appropriate or authorized Government employee, with a specific need to know, the content of any sensitive information to which I have access or which is presented to me by the Contracting Officer or other Government Official during the course of my employment, or any time thereafter.

I understand that for the purpose of this agreement, procurement sensitive information and proprietary business information include procurement data, contract information, plans, strategies, trade secrets, financial and cost and price data, technical proposals and any other information that the government or a third party contractor may deem sensitive.

I agree that the described information is "inside information" and shall not be used for private gain by myself or another person, particularly one with whom I have family, business, or financial ties. For the purposes of this agreement, "inside information" means information obtained under Government authority which has not become part of the body of public information. I specifically will not disclose any such information to employees of my company or any other contractor employees who have not signed this agreement. I will take all reasonable precautions to prevent the unauthorized disclosure and use of such information. I agree that I shall not release, publish, or disclose such information to unauthorized personnel, and I shall protect such information in accordance with relevant laws and regulations available for research and review at any Law Library. Among these laws may be various provisions of:

a) 18 U.S.C. 641 (Criminal Code: Public Money, Property or Records; 2 pgs. long)
b) 18 U.S.C. 1905 (Criminal Code: Disclosure of Confidential Information; 2 pgs. long)
c) Public Law 96-511 (Paperwork Reduction Act; Encyclopedic in length)

I hereby certify that I have read the non-disclosure agreement described above and I am familiar with the directives and policies governing the disclosure of procurement sensitive information. I will fully and completely observe these directives and will not disclose such information to any unauthorized person during or after performance of my duties under the contract and task/delivery order referenced above. I affirm that I have received a written and/or verbal briefing by my company concerning my responsibilities under this agreement. I understand that violation of this agreement may subject me to criminal and civil penalties.

_____
Employee Signature Date

_____
Employee's typed/printed name

_____
Witness Signature Date

_____
Witness's typed/printed name

QUALITY ASSURANCE SURVEILLANCE PLAN (QASP)

FOR

Task Order ITSS Solicitation # ID16210006 FPDS & SAM Integration Environment O&M

A procurement by the
U.S. General Services Administration
Region 5 Federal Acquisition Service, Acquisition Operations Division
on behalf of
National Marketing and Communications Division (NMCD)
Chicago, Illinois

NAICS 541519 – Other Computer Related Services
DB02 IT and Telecom – Compute Support Services, Non-HP

Introduction

This QASP (Quality Assurance Surveillance Plan) has been developed in accordance with FAR 46.4.

This QASP has been developed to provide an effective and systematic method for monitoring, evaluating, and documenting contractor performance of the requirements in the PWS (Performance Work Statement), SOW (Statement of Work), or SOO (Statement of Objectives) of this task order. The government will monitor contractor performance to assess the acceptability of the services provided or items delivered and not the details of how the contractor accomplishes the work.

The Government retains the right to inspect all services and supplies furnished under this contract / order in accordance with the provisions of the contract regardless of their specific inclusion in this QASP.

Contractor Responsibility

The contractor, and not the government, is responsible for managing work, ensuring that performance is satisfactory and compliant with contract provisions, and performing quality control and quality assurance functions to ensure that products and/or services meet contract requirements. Additionally, the contractor is responsible for taking all actions necessary to correct unsatisfactory, deficient, or non-compliant work.

Surveillance Monitoring

Contractor performance under this task order will be monitored by the GSA Contracting Officer's Representative (COR).

Surveillance methods will include review and analysis of services and end items, monitoring timeliness of deliveries, and observance of management practices and professionalism exhibited by contractor employees. The specific performance objectives are listed and described in the PWS/SOW/SOO or in the following Surveillance Objectives, Measures, and Expectations (if applicable).

Responsibilities of the Contract Monitors

A. The Contracting Officer's Representative (COR), with assistance from subject matter experts (SMEs) if required, is responsible for monitoring, evaluating, and documenting contractor performance. The COR shall perform the following functions.

   1. Discuss performance requirements with the contractor during the pre-performance conference.

   2. Establish a schedule for routine monitoring events, if applicable.

   3. Review, monitor, and evaluate all items (services performed, work products, and/or delivered items) as listed in the PWS/SOW/SOO in accordance with the stated performance measures. Verification of the level of performance compliance shall be performed by analysis, demonstration, inspection, or test. The evaluator shall determine the degree to which contractor performance meets the established performance standards.

4. Verify timeliness of deliveries and performance.

5. Hold performance assessment meetings with the government SMEs and management, if required.

6. Complete and/or compile performance documents for each evaluation period. These documents include—
   a. The Contractor's Monthly Project Status Reports, if applicable.
   b. The Contractor's Monthly Labor Hour and Expenditure Report, if applicable.
   c. The Contractor Performance Report (using the CPARS (Contractor Performance Assessment Reporting System) Standard Contractor Performance Report, or other approved reporting document) - The Contractor Performance Report should be completed by the COR within two weeks after the end of each evaluation period. The Contractor Performance Report is to include the following information.
      (1) Contract or Order number
      (2) Dates of the evaluation period.
      (3) The standards and measures used to make performance evaluations.
      (4) Input from the contract monitors, COR and any assisting SMEs, including--
         (a) Observations of performance (positive, acceptable, negative, unacceptable, including both successful achievements and deficiencies) in each of the areas listed on the Performance Evaluation Report. This can include observations and input from stakeholders and those reliant upon or recipients of the contractor's performance.
         (b) Notation of deficiencies or non-compliance with contract or delivery order provisions, statement of work requirements, or task directives. These notations will include a narrative describing the deficiencies or non-compliance, a reference to the contractual provisions or requirement related to the deficient or non-compliant performance, and date the deficiency or non-compliance was discovered or became known.
      (5) The date and signature of the COTR, CR and/or ACR on each entry.
   d. Documentation of the date and time the contractor is notified of any deficiency. This documentation shall include a copy of the written deficiency notification sent to and acknowledged by the contractor.
   e. Documentation of the date and time the contracting officer is notified of any contractor deficiency.
   f. Documentation of the action(s) or inaction(s) taken by the contractor to correct any deficiency.
   g. Documentation shall be made on the Performance Evaluation Report (or AF Form 372, if applicable).

7. Ensure that the narrative of all observations is accurate and factual in every respect. The narrative shall be legible and provide the evaluator's observations, evaluation, and conclusions in precise descriptive language. Generalities, personal opinions and vague or ambiguous statements are not acceptable.

8. Provide an updated copy of the Contractor Performance Report to the requiring agency's program manager and to the contracting officer upon completion of the evaluation.

9. Meet with the contracting officer to—
   a. Report the results of contractor surveillance.

b. Report the requesting agency's acceptance of services.
c. Determine the government's plan of action in the event of unacceptable, unsatisfactory, deficient, or non-compliant contractor performance.

10. Recommend needed changes to the QASP to the Contracting Officer.

B. Any assigned technical monitors shall promptly notify the GSA COR should any significant contractor performance problem arise or become known between scheduled evaluation events.

C. The contract monitors are to be objective, fair, and consistent in evaluating contractor performance.

D. Upon completion of the contract or task order, all surveillance documentation shall be included in the contract file along with all other contract documents, i.e., Statement of Work and addenda, contract/task order and all modifications, meeting reports and minutes, correspondence pertaining to this contract or order, etc.

E. Contractor performance and surveillance documentation can be used to complete Contractor performance evaluations that are submitted to the past performance data base.

Taking Corrective Actions.

The government will promptly notify the contractor of any unsatisfactory, unacceptable, deficient, non-conforming, or non-compliant performance or deliverables. The contractor shall have the opportunity to review the government's determination and provide comments.

Any contractor performance problems that result from the failure of the government to fulfill any of its obligations under the contract or order, upon which contractor performance is dependent, will not be assessed and documented as contractor deficiencies or non-compliance, to the extent of Government liability.

The contractor shall be responsible for correcting all unsatisfactory, unacceptable, deficient, or non-compliant performance. For firm fixed-price contracts, the cost of re-performing unsatisfactory, unacceptable, deficient, or non-compliant work will be the sole responsibility of the Contractor, as prescribed by paragraph (e) of the clause entitle Inspection of Services — Fixed Price (Aug 1996)(FAR 52.246-4). For Labor-Hour contracts, the cost of re-performing unsatisfactory, unacceptable, deficient, or non-compliant work will be reimbursed at the approved labor hour rate less an amount for profit, as prescribed by paragraph (f) of the clause entitle Inspection—Time-and-Material and Labor-Hour (May 2001)(FAR 52.246-6).

Disputes between the Contractor and the COR / Agency Representative regarding surveillance results should be referred to the Contracting Officer.

Failure of the contractor to take appropriate and timely corrective action will result in the government's issuance of cure or show-cause notices or pursue other remedies set forth in the provisions of the contract or as provided by law.

When unsatisfactory work is not corrected or unacceptable work is not re-performed to the Government's satisfaction, in addition to other available remedies, the Government may negotiate a reduction in the contract or task order price to reflect the reduced value received.

Additionally, the government reserves the right to include any incidents of unsatisfactory, unacceptable, deficient, or non-compliant performance, especially if uncorrected, in the contractor's past performance record.

Revisions to this QASP

This QASP and its accompanying Surveillance Objectives, Measures, and Expectations, and Contractor Performance Report format shall remain unchanged during the life of this contract or order unless modified to provide clarification or to reflect changes in the PWS/SOW/SOO or other contractual provisions. All modification will be implemented by a contract or order modification signed by the Contracting Officer and the Contractor. Revisions to this QASP are the joint responsibility of the Contracting Officer, COR, and requiring agency representative.

SURVEILLANCE OBJECTIVES, MEASURES, AND EXPECTATIONS

- SERVICES -

PERFORMANCE OBJECTIVE

The Contractor shall perform the services necessary to perform the work set forth in the PWS/SOW/TAG.

PERFORMANCE MEASURES

Contractor performance will be evaluated using the following measures, consistent with CPARS (Contractor Performance Assessment Reporting System) Standard Contractor Performance Report requirements.

1. Quality:
(This is a multi-faceted performance measure that includes work excellence, completeness, effectiveness and document format and clarity)

(Excellence) Using this measure, the Government will assess the degree to which the work performed and items or documents delivered achieve a standard of excellence or adhere to rules established by a recognized authority as a standard of performance. For example, documents will be assessed to determine the degree to which they are technically sound and free of typographical, grammatical, mathematical, and conceptual errors. Using this measure, the Government will also evaluate the degree to which the required document(s) is suitable for assessing the impacts of all reasonable alternatives and how well the recommendations will meet the intended purpose(s).

(Completeness) Using this measure, the Government will assess the degree to which the Contractor identifies, includes, addresses and/or performs all pertinent aspects of the work or all pertinent elements of delivered items, data, or services. Using this measure, the Government will also assess the degree to which the Contractor performs all stipulated or planned activities and captures the results of those activities in the various documents that are to be delivered.

(Effectiveness) Using this measure, the Government will evaluate the degree to which the Contractor's performance (work, products, and data submissions) meets all goals and objectives established in both the PWS (Performance Work Statement), Government Task Directives, and in any required Contractor's project planning documents (e.g., assessments, analysis, project plan, WBS, or execution recommendations).

(Format & Clarity) Using this measure, the Government will assess the design, flow, matrix, and/or layout used by the Contractor to present data (whether presented physically, orally, or electronically). This assessment will focus on the degree of clarity and logical organization with which the data is presented and whether or not the format facilitates easy review and use of the material. Using this measure, the Government will assess the degree to which material presented in documents (narrative, tables, diagrams, footnotes, photographs, etc.) are easy to understand by the intended audience.

2. Schedule/Timeliness:
Using this measure, the Government will assess the degree to which the Contractor meets or exceeds the delivery schedule.

3. Cost Control:
Using this measure, GSA will assess the degree to which the Contractor is able to control costs and accomplish the work at a lower cost than estimated and established in the task order budget without compromising other aspects of performance, e.g., while maintaining quality and timeliness.
[Note: This measure allows for a flexible assessment of costs.]
[Note: This factor will not be evaluated if all work is performed on a fixed price basis.]

4. Business Relationship:
Using this measure, the Government will assess the level of professionalism exhibited by the Contractor staff in interactions with Government and other personnel in connection with work being performed under this or contract.

5. Management:
Using this measure, the Government will assess the degree to which the Contractor's management is able to competently direct the work, resolve problems, interface with government program managers and technical experts, and balance the resource triangle of quality, schedule, and cost.

5. Utilization of Small Business:
Using this measure, the Government will assess the degree to which the uses small businesses to perform the work in comparison to proposed small business use.
[Note: This factor will not be evaluated if all work is performed by the prime contractor.]

5. Security:
Using this measure, the Government will assess the degree to which the Contractor complies with all required security measures and specifications. Using this measure the government will also assess security incidents and violations and subsequent corrective actions taken by the contractor.

PERFORMANCE EXPECTATIONS

Performance will be evaluated against a Performance Criteria Matrix (if provided in the PWS/SOW/SOO or as a separate document) and/or the following Satisfactory Performance Expectations.

Satisfactory Performance Expectations:
The Government will rate the contractor's performance by comparing it against the following expectations for satisfactory performance. Performance ratings will be based on the degree to which the contractor fails to meet, meets, or exceeds these satisfactory performance expectations.

Quality:
The work described and the deliverables listed in the PWS (Performance Work Statement), SOW (Statement of Work), or SOO (Statement of Objectives) shall be performed per applicable regulations, industry standards, and contract/task order requirements.

The content of data deliverables shall address all of the areas and topics prescribed by the PWS/SOW/SOO. The information in the document(s) shall focus on the solution to the Government's need. Material in the documents should be appropriate and pertinent for the scope of the subject being addressed. Documents shall be submitted in the format described in the PWS/SOW/SOO.

If required by the PWS/SOW/SOO, planning documents shall reflect an adequate understanding of the subject matter and of planned and potential activities for this project. Planning documents shall address alternatives and present sound and workable conceptual and technical conclusions and recommendations that are supported by the data acquired during the investigation portion of this project.

Reports shall capture and clearly convey the information they are intended to address per the requirements of the PWS, e.g., project status and milestone updates, problems and solutions, financial and travel information, etc.

The document format should be well organized and clear, making the information easy to find and use. However, draft formats may need minor revision and some information may not be immediately identifiable. These problems should only require minimal effort to correct prior to final submission. Ideas will be logically presented. Documents should contain few, if any, technical errors or inconsistencies between the information presented and that contained in the source documents or raw data. Document(s) will be grammatically and mathematically correct, although drafts may contain errors that require minor editing changes or corrections prior to final submission. Document content shall be consistent with common practice and industry or other established standards or protocols.

Schedule/Timeliness:
The Contractor shall perform work and submit the required documents by the time stated in the delivery schedule of the task order.

Cost:
Final costs of performance shall be within the agreed upon and approved budget.

Professionalism:
All interactions between Contractor personnel and Government personnel shall be professional and appropriate.

Management:
Management will be responsible, responsive, and pro-active in directing the work, resolving problems, interfacing with government program managers and technical experts, and balancing the resource.

Small Business Utilization:
The Contractor shall use small business to the degree originally proposed.

Security:
The Contractor shall comply with all required security measures and specifications and there shall be no security incidents and violations.

PERFORMANCE EVALUATION

The COR, or other Government representative responsible for evaluating Contractor performance, shall complete a contractor performance evaluation at least on an annual basis using the CPARS (Contractor Performance Assessment Reporting System) evaluation form. The report shall address each of the applicable performance measures as they specifically apply to the work described and deliverables furnished in conjunction with this contract/task order. Performance ratings will be based on the degree to which the contractor fails to meet, meets, or exceeds the above stated satisfactory performance expectations. Evaluation results will be provided to the contractor in their annual CPARS evaluation.

Metric Group	Metric	Baseline Recommendation	Period
Availability	FPDS Uptime availability	Average 99.8% across the relevant time period	Monthly
Availability	Process up to 100 real time transactions per second	1 second or less	Monthly
Availability	Home page screen return in 5 seconds	5 seconds or less	Monthly
Availability	Report Response Time	10 seconds or less	Monthly
Availability	Small Report Processing Time	Zero timeout	Monthly
Availability	Large Report Timeout	Less than 5%	Monthly
Availability	DoD User Log-ins	99% across the relevant time period	Monthly
Business Process	CDC Nightly Refresh Process	96% across the relevant time period	Monthly
Business Process	Recovery Report	100% across the relevant time period	Monthly
Business Process	NIA Reports	100% across the relevant time period	Monthly
Business Process	AAC Load	96% across the relevant time period	Monthly
Business Process	EZ Search / ATOM Feed	99% across the relevant time period	Monthly
Help Desk	Outstanding Ticket Age	Less than 10% of all open tickets open are more than 30 days old	Monthly
Help Desk	Ticket Closure Rate	More than 90% of the total tickets escalated to Tier 2 over the last 30 days have been closed	Monthly
Help Desk	Tickets Closed the Same Day	More than 30% of tickets closed within 72 hours	Monthly

Security	Outages due to security incidents (unplanned unavailability)	No more than 1 outage	Monthly
Security	Time lag between detection, reporting and acting upon security incidents.	At least 90% of incidents addressed per response table	Monthly

Definition	Data Source	Business Rules
Number of hours of site availability per month	Rational Performance Test monitoring	Third party data center (hosting vendor) maintains 100% uptime.
Speed of real time transaction processing	Quick Test Professional	Third party data center (hosting vendor) maintains 100% uptime.
Present a screen to users within 5 seconds	Quick Test Professional	Third party data center (hosting vendor) maintains 100% uptime.
Return reports in 10 seconds	Quick Test Professional	Top 7 most executed reports respond within 10 seconds
Reports less than 10K lines no timeouts	Quick Test Professional	Third party data center (hosting vendor) maintains 100% uptime.
Reports more than 10K timeouts less than 5%	Quick Test Professional	Top 7 most executed reports
The number of successful and failed in login attempts for DoD users	Oracle DB	Provided DoD users login Metrics for the previous day at 4:00am
The number of records successfully pushed from the transactional tables to the Vertica database is at or near 100% less any egregious user updates. This will be measured nightly.	Oracle DB	Third party data center (hosting vendor) maintains 100% uptime.
posted with the previous day's updates to the FPDS production site by 12pm (EST)	Oracle DB, Vertica, SOLR	Third party data center (hosting vendor) maintains 100% uptime.
The National Interest Action Reports are posted with the previous week's updates to the FPDS production site by 12pm (EST) on Thursday	Informatica	Third party data center (hosting vendor) maintains 100% uptime.
errors and all records are loaded to FPDS at 8:30 AM and 8:30PM. A failure does not include any issues received from FPDW (e.g., password resets, etc.).	FPDW	Third party data center (hosting vendor) maintains 100% uptime.
The average search time end users have performed across all the 4 servers and aggregate those searches in ms.	EZ Search/ATOM Feed & ElasticSearch	Third party data center (hosting vendor) maintains 100% uptime.
Number of tickets older than 30 days divided by the total ticket number of tickets escalated to Tier 2 in the period.	Help Desk Tracking Tool	System defects and enhancements that prevent closure of the ticket will not be counted since this is not a reflection of the Help Desk effectiveness.
Number of tickets closed in a month divided by the number of tickets escalated to Tier 2	Help Desk Tracking Tool	Escalations must be no greater than 10%.
escalated to Tier 2 that are closed within 72 hours	Help Desk Tracking Tool	3 or external agencies will not be counted.

Number and duration of outages due to incidents (unplanned unavailability). fpds.gov is unavailable due to a security incident.	Stakeholder manual identification	Outages that are requested by GSA as a result of a formally defined security incident as outlined in IT Security Procedural Guide: Incident Response (IR) CIO-IT Security-01-02.
Security incidents are responded to in the timeframes identified in current Incident Response Table.	Stakeholder manual identification	GSA ISSO to maintain and provide agreed upon incident response table.

System	Environment	HW/SW	Category	Maufacturer
FPDS	Prod	SW	Security	Splunk
FPDS	Prod	SW	Security	Splunk
FPDS	Prod-NonProd	SW	Security	Tenable
FPDS	NonProd	SW	Security	Informatica
FPDS	Prod	SW	Security	Informatica
FPDS	Prod	SW	data Mgmt	HP
FPDS	NON-Prod	SW	data Mgmt	HP
FPDS	DR	SW	data Mgmt	HP
FPDS	NON-Prod	SW	Testing	HP
FPDS	NON-Prod	SW	Testing	HP
FPDS	NON-Prod	SW	Testing	HP
FPDS	NON-Prod	SW	Testing	HP
FPDS	NON-Prod	SW	Testing	HP
FPDS	NON-Prod	SW	Development	SmartBear.com
FPDS	NON-Prod	SW	Development	Altova
FPDS	Prod	SW	Operating System	Microsoft
FPDS	NON-Prod	SW	Operating System	Microsoft
FPDS	Prod	SW	Operating System	Red Hat
FPDS	Prod	SW	Operating System	Red Hat
FPDS	NON-Prod	SW	Operating System	Red Hat
FPDS	Prod / Nonprod	SW	Backup	Arcserve
FPDS	Prod	SW	Monitoring	Vmware
FPDS	NON-Prod	SW	Monitoring	Vmware
FPDS	Prod	SW	Security	Symantec
FPDS	NON-Prod	SW	Security	Symantec
FPDS	NON-Prod	SW	Security	Symantec
FPDS	Prod-NonProd	SW	Operating System	Vmware
FPDS	NON-Prod	SW	Operating System	Red Hat
FPDS	NON-Prod	SW	Operating System	Red Hat
FPDS	Prod	SW	data Mgmt	2nd Quadrant
FPDS	Prod	SW	Search Engine	Elastic Search
FPDS	Prod	SW	Big Data	Horton works
FPDS	Prod	SW	Security	McAfee

FPDS	Prod	SW	Security	Netsparker
FPDS	Prod	SW	Security	Safenet
FPDS	Prod	SW	Security	Safenet
FPDS	Prod	SW	Security	Safenet
FPDS	Prod	SW	Ziocode database	Zipinfo
FPDS	Prod	SW	Operating System	Microsoft
FPDS	Prod	SW	Operating System	Red Hat

Description	Qty
Splunk licensed by amount of data indexed per day (GB) (perpetual license) Entitlement: SPL-14154640	5.0 GB
Splunk licensed by amount of data indexed per day (GB) (perpetual license) Entitlement: SPL-14141686	20 GB
Nessus Professional	1
Informatica Power Analyzer Server	3
Informatica Power Analyzer Server	3
HP Vertica (licensed by TB) RENEWAL License for PROD	1.0 TB
HP Vertica (licensed by TB) 2 NEW Licenses	1.0 TB
HP Vertica (licensed by TB) SUPPORT for NEW licenses	1.0 TB
HP UFT CC User SW E-LTU	5
HP 1 YR 9X5 SUPPORT for HO NV for PC 5000-9999 VU SW E-LTU	5
HP LR Web/Mmed 1-499 VU+C SW E-LTU	45
HP LR Foundation Entitlement SW E-LTU	1
HP LR GUI Virtual User SW E-LTU	5
SmartBear Ready! API SoapUI NG Fixed User Subscription License (3 Year Subscription)	5
Altova XML Spy (License Type: 5 Installed users)	1
Microsoft Windows Server 2012 Standard 2012 R2 Non-specific License Only NO MEDIA INCLUDED, Full New License (English), (Open Government Licensing)	2
Microsoft Windows Server 2012 Standard 2012 R2 Non-specific License Only NO MEDIA INCLUDED, Full New License (English), (Open Government Licensing)	6
REDHAT JBoss Enterprise Application Platform, 64 Core Premium Support (24X7 phone and web support) , 1 Year	3
Red Hat Directory Server Small Business Bundle	1
Red Hat Directory Server Small Business Bundle	1
Arcserve UDP Premium Plus Edition - Managed Capacity per TB between 26 - 50 TB - One Year Enterprise Maintenance - Renewal	12.0 TB
TPP L1 U.S. Federal VMware vFabric Hyperic HQ EE Perpetual License	40
TPP L1 U.S. Federal VMware vFabric Hyperic HQ EE Perpetual License	25
Symantec Endpoint Protection 12.1	40
Symantec Endpoint Protection 12.1	56
Symantec Endpoint Protection 12.1	60
TPP L1 U.S. Federal VMware vFabric Hyperic HQ EE Perpetual License	60
Red Hat JBoss Enterprise Application Platform, 16-Core Premium	2
Red Hat JBoss Enterprise Application Platform, 16-Core Premium	1
2nd quadrant Gold postgreSQL 9.6.3 Production Support	3
Elastic Search 5.3 -support, X-Pack - Security component for ES 5.30 Platinum License 10 node	1
Hortonworks (HDP) 2.4 - HP hortonworks Data Platform Enterprise Plus - subscription license +1 Year 24x7 support (per node)	8
McAfee Vulnerability Manager Databases (Security Scanner 4.6 - Perpetual License, 1-25 Database) Instances, with 1 Year Gold Software Support	10

Netsparker Desktop Web Application Security Scanner Desktop Scanner STANDARD (consulting - Unlimited targets)	2
Token 1 - Safenet OTP 110 (Event)	30
Token 2 - MobilePass	30
SAS SPE/PCE Subscription with 24x7 Support (3 Years)	60
ZIP Code Database Redistributable (Congressional District Database)	1
Microsoft Windows Server 2016 Remote Desktop Services - License - 10 user C - Part No: 01GU650	2
REDHAT JBoss Enterprise Application Platform, 64 Core Premium Support (24X7 phone and web support) , 1 Year	1

Coming up For Renewal	Renew
End of Support	Renew
Current	None
New Purchase	Buy
End of Life	Replace

FPDS Non-Production Servers

Instance Type	vCPU	Memory	EBS (GB)	OS
c5.4xlarge	16	32	100	Checkpoint
c4.4xlarge	16	32	100	Checkpoint
m4.xlarge	4	16	500	Checkpoint
m5.xlarge	2	8	600	Checkpoint
t2.2xlarge	8	32	200	Windows
c4.4xlarge	16	32	100	F5 LTM
m4.2xlarge	8	32	740	Red Hat
m4.2xlarge	8	32	740	Red Hat
m4.2xlarge	8	32	740	Red Hat
m4.2xlarge	8	32	740	Red Hat
m4.2xlarge	8	32	740	Red Hat
m4.2xlarge	8	32	740	Red Hat
m4.4xlarge	16	64	825	Red Hat
m4.4xlarge	16	64	325	Red Hat
m4.2xlarge	8	32	140	Red Hat
m4.2xlarge	8	32	140	Red Hat
m4.2xlarge	8	32	140	Red Hat
m4.10xlarge	40	160	4190	Red Hat
m4.10xlarge	40	160	4190	Red Hat
m4.xlarge	4	16	150	Red Hat
m4.2xlarge	8	32	140	Red Hat
m4.2xlarge	8	32	140	Red Hat
m4.2xlarge	8	32	140	Red Hat
m4.4xlarge	16	64	325	Red Hat
m4.xlarge	4	16	140	Red Hat
m4.xlarge	4	16	140	Red Hat
m4.2xlarge	8	32	4190	Red Hat
m4.xlarge	4	16	150	Red Hat
m4.2xlarge	8	32	740	Red Hat
m4.2xlarge	8	32	740	Red Hat
m4.2xlarge	8	32	740	Red Hat
m4.2xlarge	8	32	740	Red Hat
m4.2xlarge	8	32	740	Red Hat
m4.2xlarge	8	32	740	Red Hat
m4.2xlarge	8	32	140	Red Hat
m4.2xlarge	8	32	140	Red Hat
m4.2xlarge	8	32	140	Red Hat
m4.4xlarge	16	64	325	Red Hat
m4.4xlarge	16	64	325	Red Hat

m4.10xlarge	40	160	4190	Red Hat
m4.10xlarge	40	160	4190	Red Hat
m4.xlarge	4	16	150	Red Hat
m4.xlarge	4	16	150	Red Hat
m4.xlarge	4	16	150	Red Hat
m4.xlarge	4	16	150	Red Hat
m4.large	4	16	175	Red Hat
m4.4xlarge	16	64	400	Red Hat
m4.4xlarge	16	64	400	Red Hat
m4.4xlarge	16	64	400	Red Hat
m4.2xlarge	8	32	325	Red Hat
m4.2xlarge	8	32	325	Red Hat
m4.2xlarge	8	32	140	Red Hat
m4.2xlarge	8	32	140	Red Hat
m4.2xlarge	8	32	140	Red Hat
m4.xlarge	4	16	140	Red Hat
m4.xlarge	4	16	140	Red Hat
m4.xlarge	4	16	140	Red Hat
m4.xlarge	4	16	140	Red Hat
m4.xlarge	4	16	350	Red Hat
m4.4xlarge	16	64	140	Red Hat
m4.xlarge	4	16	140	Red Hat
m4.4xlarge	16	64	640	Red Hat
m4.xlarge	4	16	1550	Red Hat
m4.xlarge	4	16	440	Red Hat
m4.xlarge	4	16	440	Red Hat
m4.xlarge	4	16	140	Red Hat
m4.large	2	8	140	Red Hat
m4.large	2	8	150	Red Hat
m4.xlarge	4	16	175	Red Hat
m4.4xlarge	16	64	2225	Red Hat
m4.4xlarge	16	64	2225	Red Hat
m4.4xlarge	16	64	2225	Red Hat
m4.xlarge	4	16	300	Windows
m4.2xlarge	8	32	350	Windows
m4.xlarge	4	16	700	Windows
m5.2xlarge	8	32	300	Windows
m4.2xlarge	8	32	5350	Windows
m4.xlarge	4	16	300	Windows
m4.xlarge	4	16	300	Windows
m4.xlarge	4	16	300	Windows
m4.2xlarge	8	32	140	Red Hat
m4.2xlarge	8	32	140	Red Hat
m4.2xlarge	8	32	140	Red Hat
m4.4xlarge	16	64	325	Red Hat

m4.4xlarge	16	64	325	Red Hat
m4.xlarge	4	16	140	Red Hat
m4.xlarge	4	16	140	Red Hat
m4.4xlarge	16	64	4190	Red Hat
m4.xlarge	4	16	150	Red Hat
t2.small	1	3	10	Red Hat

Description
New Non-Production Checkpoint Firewall
Old Non-Production Checkpoint Firewall 1
Old Non-Production Checkpoint Smart Mgmt
New Non-Production Checkpoint Smart Mgmt
REI Jump Server 1
Non-Production F5 LTM Load Balancer 1
Beta Elastic Search Server 1
Beta Elastic Search Server 2
Beta Elastic Search Server 3
Beta Elastic Search Server 4
Beta Elastic Search Server 5
Beta Elastic Search Server 6
Beta JBOSS EAP Server 1
Beta JBOSS EAP Server 2
Beta Kafka Server 1
Beta Kafka Server 2
Beta Kafka Server 3
Beta PostgreSQL Database Server 1
Beta PostgreSQL Database Server 2
Beta Content Management Server 1
Development Elastic Search Server 1
Development Elastic Search Server 2
Development Elastic Search Server 3
Development JBOSS EAP Server 1
Development Kafka Server 1
Development Kafka Server 2
Development PostgreSQL Database Server 1
Development Content Management Server 1
Load Elastic Search Server 1
Load Elastic Search Server 2
Load Elastic Search Server 3
Load Elastic Search Server 4
Load Elastic Search Server 5
Load Elastic Search Server 6
Load Kafka Server 1
Load Kafka Server 2
Load Kafka Server 3
Load JBOSS EAP Server 1
Load JBOSS EAP Server 2

Load PostgreSQL Database Server 1
Load PostgreSQL Database Server 2
Load Vertica Server1
Load Vertica Server2
Load Vertica Server3
Load Content Management Server 1
Load Ambari Server
Load Hadoop Server1
Load Hadoop Server2
Load Hadoop Server3

Non-Production Hyperic Application Server 1
Non-Production Hyperic Database Server 1
Non-Production Informatica Server 1
Non-Production Informatica Server 2
Non-Production Informatica Server 3
Non-Production Jmeter Server 1
Non-Production Jmeter Server 2
Non-Production Jmeter Server 3
Non-Production Jmeter Server 4
Non-Production Log Manager Server 1
Non-Production Operations Server 1
Non-Production Mail Server 1
Non-Production Splunk Server 1
Non-Production Version Control Server 1
Non-Production Vertica Server 1
Non-Production Vertica Server 2
Non-Production Vertica Server 3
IPv6 Proxy
Non-Production Red Hat Directory Server 1 (LDAP)
Non-Production Hadoop Horton works Ambari Server
Non-Production Hadoop Server 1
Non-Production Hadoop Server 2
Non-Production Hadoop Server 3
Windows Active Directory Server 1
Non-Production Symantec Antivirus Server 1
Non-Production Jenkins Server 1
Non-Production Nessus Scanner Server 1
Non-Production Arcserve Backup Server 1
Non-Production Unified Functional Testing Server 1
Non-Production Unified Functional Testing Server 2
Non-Production Unified Functional Testing Server 3

Non-Production Elastic Search Server 1
Non-Production Elastic Search Server 2
Non-Production Elastic Search Server 3
Test JBOSS EAP Server 1

Test JBOSS EAP Server 2
Non-Production Kafka Server 1
Non-Production Kafka Server 2
Test PostgreSQL Database Server 1
Test Content Management Server 1
Rescure Instance for RHEL 7

FPDS Production Servers

Instance Type	vCPU	Memory	EBS	OS
c4.4xlarge	16	32	100 GB	Checkpoint
c4.4xlarge	16	32	100 GB	Checkpoint
c5n.4xlarge	16	42	100 GB	Checkpoint
c5n.4xlarge	16	42	100 GB	Checkpoint
m4.2xlarge	8	32	1500 GB	Checkpoint
m5.2xlarge	8	32	1500 GB	Checkpoint
m4.large	2	8	150 GB	Red Hat
m4.large	2	8	150 GB	Red Hat
m4.large	2	8	150 GB	Red Hat
m4.large	2	8	150 GB	Red Hat
m4.2xlarge	8	32	700 GB	Windows
m4.2xlarge	8	32	700 GB	Windows
m4.xlarge	4	16	140 GB	Red Hat
m4.xlarge	4	16	650 GB	Red Hat
m4.xlarge	4	16	650 GB	Red Hat
m4.xlarge	4	16	440 GB	Red Hat
c4.4xlarge	16	32	160 GB	F5 LTM
c4.4xlarge	16	32	160 GB	F5 LTM
m4.xlarge	4	16	300 GB	Windows
m4.2xlarge	8	32	300 GB	Windows
m4.2xlarge	8	32	5300 GB	Windows
m4.2xlarge	8	32	300 GB	Windows
m4.10xlarge	40	160	1140 GB	Red Hat
m4.2xlarge	8	32	300 GB	Windows
m4.xlarge	4	16	150 GB	Red Hat
m4.xlarge	4	16	2200 GB	Red Hat
m4.4xlarge	16	64	2200 GB	Red Hat
m4.4xlarge	16	64	2200 GB	Red Hat
m4.4xlarge	16	64	2200 GB	Red Hat
m4.4xlarge	16	64	2200 GB	Red Hat
m4.10xlarge	40	160	1175 GB	Red Hat
m4.10xlarge	40	160	1175 GB	Red Hat
m4.10xlarge	40	160	1175 GB	Red Hat
m4.10xlarge	40	160	840 GB	Red Hat
m4.10xlarge	40	160	325 GB	Red Hat
m4.10xlarge	40	160	325 GB	Red Hat
m4.10xlarge	40	160	140 GB	Red Hat
m4.10xlarge	40	160	140 GB	Red Hat

m4.4xlarge	16	64	140 GB	Red Hat
m4.4xlarge	16	64	640 GB	Red Hat
m4.4xlarge	16	64	640 GB	Red Hat
m4.4xlarge	16	64	640 GB	Red Hat
m4.4xlarge	16	64	640 GB	Red Hat
m4.4xlarge	16	64	640 GB	Red Hat
m4.4xlarge	16	64	640 GB	Red Hat
m4.4xlarge	16	64	640 GB	Red Hat
m4.4xlarge	16	64	640 GB	Red Hat
m4.4xlarge	16	64	640 GB	Red Hat
m4.4xlarge	16	64	640 GB	Red Hat
m4.xlarge	4	16	140 GB	Red Hat
m4.xlarge	4	16	140 GB	Red Hat
m4.2xlarge	8	32	140 GB	Red Hat
m4.2xlarge	8	32	140 GB	Red Hat
m4.4xlarge	16	64	1325 GB	Red Hat
m4.4xlarge	16	64	1325 GB	Red Hat
m4.2xlarge	8	32	150 GB	Red Hat
m4.xlarge	4	16	1175 GB	Red Hat
m4.2xlarge	8	32	140 GB	Red Hat
m4.2xlarge	8	32	325 GB	Red Hat
m4.10xlarge	40	160	4250 GB	Red Hat
m4.10xlarge	40	160	6250 GB	Red Hat
m4.large	2	8	30 GB	Red Hat
m4.large	2	8	140 GB	Red Hat
t2.2xlarge	8	32	300 GB	Windows
t2.2xlarge	8	32	300 GB	Windows

Description
Production Checkpoint Firewall 1 (Old)
Production Checkpoint Firewall 2 (Old)
Production Checkpoint Firewall 1
Production Checkpoint Firewall 2
Production Checkpoint Firewall Management Server
Production Checkpoint Firewall Management Server
IPv6 Proxy
IPv6 Proxy
IPv6 Proxy
IPv6 Proxy
Production Jump Server 1
Production Jump Server 2
Production Mail Server
Production Content Management Server 1
Production Content Management Server 2
Production Content Management Server 3
Production F5 LTM Load Balancer 1
Production F5 LTM Load Balancer 2
Production Windows Active Directory Server 1
Production Windows Active Directory Server 2
Production Arcserve Backup Server 1
Production Symantec Antivirus Server 1
Production Splunk log Collection and Analysis Server
Production Nessus Scanner Server 1
Production Hadoop Horton works Ambari Server
Production Hadoop Server 1
Production Hadoop Server 2
Production Hadoop Server 3
Production Hadoop Server 4
Production Hadoop Server 5
Production Vertica Server 1
Production Vertica Server 2
Production Vertica Server 3
Production JBOSS EAP Server 1
Production JBOSS EAP Server 2
Production JBOSS EAP Server 3
Production Informatica Server 1
Production Informatica Server 2

Production Informatica Server 3
Production Elastic Search Server 1
Production Elastic Search Server 2
Production Elastic Search Server 3
Production Elastic Search Server 4
Production Elastic Search Server 5
Production Elastic Search Server 6
Production Elastic Search Server 7
Production Elastic Search Server 8
Production Elastic Search Server 9
Production Elastic Search Server 10
Production Search API Server 1
Production Search API Server 2
Production Search API Server 3
Production Search API Server 4
Production Operations Server 1
Production Operations Server 2
Production Red Hat Directory Server 1 (LDAP)
Production Log Manager Server 1
Production Hyperic Application Server 1
Production Hyperic Database Server 1
Production PostgreSQL Database Server 1
Production PostgreSQL Database Server 2
Rescure Instance for RHEL 7
Rescure Instance for RHEL 6

REI Team Jump Server 2
REI Team Jump Server 4
Counts:-

FPDS COOP Servers

Instance Type	vCPU	Memory	EBS (GB)	OS
c4.4xlarge	16	30	500	Checkpoint
m4.xlarge	4	16	650	Red Hat
c4.4xlarge	16	30	100	F5 LTM
m4.xlarge	4	16	300	Windows
m4.2xlarge	8	32	1175	Red Hat
m4.2xlarge	8	32	1175	Red Hat
m4.2xlarge	8	32	**1175**	Red Hat
m4.10xlarge	40	160	837	Red Hat
m4.10xlarge	40	160	837	Red Hat
m4.4xlarge	16	64	640	Red Hat
m4.4xlarge	16	64	640	Red Hat
m4.4xlarge	16	64	640	Red Hat
m4.xlarge	4	16	140	Red Hat
m4.xlarge	4	16	140	Red Hat
m4.2xlarge	8	32	550	Red Hat
m4.xlarge	4	16	150	Red Hat
m4.4xlarge	16	32	4236	Red Hat
m4.4xlarge	16	32	4236	Red Hat

Description
COOP Checkpoint Firewall 1
COOP Content Management Server 1
COOP F5 Load Balancer 1
Windows Active Directory Server 1, DNS
COOP Vertica Server 1
COOP Vertica Server 2
COOP Vertica Server 3
COOP JBoss EAP Sever 1
COOP JBoss EAP Sever 2
COOP Elastic Search Server 1
COOP Elastic Search Server 2
COOP Elastic Search Server 3
COOP Search API Server 1
COOP Search API Server 2
COOP Operations Server 1
COOP Red Hat Directory Server 1
COOP PostgreSQL Database Server 1
COOP PostgreSQL Database Server 2

FPDS Non-Production Servers

Instance Type	vCPU	Memory	EBS (GB)	OS
c5.4xlarge	16	32	100	Checkpoint
c4.4xlarge	16	32	100	Checkpoint
m4.xlarge	4	16	500	Checkpoint
m5.xlarge	2	8	600	Checkpoint
t2.2xlarge	8	32	200	Windows
c4.4xlarge	16	32	100	F5 LTM
m4.2xlarge	8	32	740	Red Hat
m4.2xlarge	8	32	740	Red Hat
m4.2xlarge	8	32	740	Red Hat
m4.2xlarge	8	32	740	Red Hat
m4.2xlarge	8	32	740	Red Hat
m4.2xlarge	8	32	740	Red Hat
m4.4xlarge	16	64	825	Red Hat
m4.4xlarge	16	64	325	Red Hat
m4.2xlarge	8	32	140	Red Hat
m4.2xlarge	8	32	140	Red Hat
m4.2xlarge	8	32	140	Red Hat
m4.10xlarge	40	160	4190	Red Hat
m4.10xlarge	40	160	4190	Red Hat
m4.xlarge	4	16	150	Red Hat
m4.2xlarge	8	32	140	Red Hat
m4.2xlarge	8	32	140	Red Hat
m4.2xlarge	8	32	140	Red Hat
m4.4xlarge	16	64	325	Red Hat
m4.xlarge	4	16	140	Red Hat
m4.xlarge	4	16	140	Red Hat
m4.2xlarge	8	32	4190	Red Hat
m4.xlarge	4	16	150	Red Hat
m4.2xlarge	8	32	740	Red Hat
m4.2xlarge	8	32	740	Red Hat
m4.2xlarge	8	32	740	Red Hat
m4.2xlarge	8	32	740	Red Hat
m4.2xlarge	8	32	740	Red Hat
m4.2xlarge	8	32	740	Red Hat
m4.2xlarge	8	32	140	Red Hat
m4.2xlarge	8	32	140	Red Hat
m4.2xlarge	8	32	140	Red Hat
m4.4xlarge	16	64	325	Red Hat
m4.4xlarge	16	64	325	Red Hat

m4.10xlarge	40	160	4190	Red Hat
m4.10xlarge	40	160	4190	Red Hat
m4.xlarge	4	16	150	Red Hat
m4.xlarge	4	16	150	Red Hat
m4.xlarge	4	16	150	Red Hat
m4.xlarge	4	16	150	Red Hat
m4.large	4	16	175	Red Hat
m4.4xlarge	16	64	400	Red Hat
m4.4xlarge	16	64	400	Red Hat
m4.4xlarge	16	64	400	Red Hat
m4.2xlarge	8	32	325	Red Hat
m4.2xlarge	8	32	325	Red Hat
m4.2xlarge	8	32	140	Red Hat
m4.2xlarge	8	32	140	Red Hat
m4.2xlarge	8	32	140	Red Hat
m4.xlarge	4	16	140	Red Hat
m4.xlarge	4	16	140	Red Hat
m4.xlarge	4	16	140	Red Hat
m4.xlarge	4	16	140	Red Hat
m4.xlarge	4	16	350	Red Hat
m4.4xlarge	16	64	140	Red Hat
m4.xlarge	4	16	140	Red Hat
m4.4xlarge	16	64	640	Red Hat
m4.xlarge	4	16	1550	Red Hat
m4.xlarge	4	16	440	Red Hat
m4.xlarge	4	16	440	Red Hat
m4.xlarge	4	16	140	Red Hat
m4.large	2	8	140	Red Hat
m4.large	2	8	150	Red Hat
m4.xlarge	4	16	175	Red Hat
m4.4xlarge	16	64	2225	Red Hat
m4.4xlarge	16	64	2225	Red Hat
m4.4xlarge	16	64	2225	Red Hat
m4.xlarge	4	16	300	Windows
m4.2xlarge	8	32	350	Windows
m4.xlarge	4	16	700	Windows
m5.2xlarge	8	32	300	Windows
m4.2xlarge	8	32	5350	Windows
m4.xlarge	4	16	300	Windows
m4.xlarge	4	16	300	Windows
m4.xlarge	4	16	300	Windows
m4.2xlarge	8	32	140	Red Hat
m4.2xlarge	8	32	140	Red Hat
m4.2xlarge	8	32	140	Red Hat
m4.4xlarge	16	64	325	Red Hat

m4.4xlarge	16	64	325	Red Hat
m4.xlarge	4	16	140	Red Hat
m4.xlarge	4	16	140	Red Hat
m4.4xlarge	16	64	4190	Red Hat
m4.xlarge	4	16	150	Red Hat
t2.small	1	3	10	Red Hat

Description
New Non-Production Checkpoint Firewall
Old Non-Production Checkpoint Firewall 1
Old Non-Production Checkpoint Smart Mgmt
New Non-Production Checkpoint Smart Mgmt
REI Jump Server 1
Non-Production F5 LTM Load Balancer 1
Beta Elastic Search Server 1
Beta Elastic Search Server 2
Beta Elastic Search Server 3
Beta Elastic Search Server 4
Beta Elastic Search Server 5
Beta Elastic Search Server 6
Beta JBOSS EAP Server 1
Beta JBOSS EAP Server 2
Beta Kafka Server 1
Beta Kafka Server 2
Beta Kafka Server 3
Beta PostgreSQL Database Server 1
Beta PostgreSQL Database Server 2
Beta Content Management Server 1
Development Elastic Search Server 1
Development Elastic Search Server 2
Development Elastic Search Server 3
Development JBOSS EAP Server 1
Development Kafka Server 1
Development Kafka Server 2
Development PostgreSQL Database Server 1
Development Content Management Server 1
Load Elastic Search Server 1
Load Elastic Search Server 2
Load Elastic Search Server 3
Load Elastic Search Server 4
Load Elastic Search Server 5
Load Elastic Search Server 6
Load Kafka Server 1
Load Kafka Server 2
Load Kafka Server 3
Load JBOSS EAP Server 1
Load JBOSS EAP Server 2

Load PostgreSQL Database Server 1
Load PostgreSQL Database Server 2
Load Vertica Server1
Load Vertica Server2
Load Vertica Server3
Load Content Management Server 1
Load Ambari Server
Load Hadoop Server1
Load Hadoop Server2
Load Hadoop Server3

Non-Production Hyperic Application Server 1
Non-Production Hyperic Database Server 1
Non-Production Informatica Server 1
Non-Production Informatica Server 2
Non-Production Informatica Server 3
Non-Production Jmeter Server 1
Non-Production Jmeter Server 2
Non-Production Jmeter Server 3
Non-Production Jmeter Server 4
Non-Production Log Manager Server 1
Non-Production Operations Server 1
Non-Production Mail Server 1
Non-Production Splunk Server 1
Non-Production Version Control Server 1
Non-Production Vertica Server 1
Non-Production Vertica Server 2
Non-Production Vertica Server 3
IPv6 Proxy
Non-Production Red Hat Directory Server 1 (LDAP)
Non-Production Hadoop Horton works Ambari Server
Non-Production Hadoop Server 1
Non-Production Hadoop Server 2
Non-Production Hadoop Server 3
Windows Active Directory Server 1
Non-Production Symantec Antivirus Server 1
Non-Production Jenkins Server 1
Non-Production Nessus Scanner Server 1
Non-Production Arcserve Backup Server 1
Non-Production Unified Functional Testing Server 1
Non-Production Unified Functional Testing Server 2
Non-Production Unified Functional Testing Server 3

Non-Production Elastic Search Server 1
Non-Production Elastic Search Server 2
Non-Production Elastic Search Server 3
Test JBOSS EAP Server 1

Test JBOSS EAP Server 2
Non-Production Kafka Server 1
Non-Production Kafka Server 2
Test PostgreSQL Database Server 1
Test Content Management Server 1
Rescure Instance for RHEL 7

FPDS Production Servers

Instance Type	vCPU	Memory	EBS	OS
c4.4xlarge	16	32	100 GB	Checkpoint
c4.4xlarge	16	32	100 GB	Checkpoint
c5n.4xlarge	16	42	100 GB	Checkpoint
c5n.4xlarge	16	42	100 GB	Checkpoint
m4.2xlarge	8	32	1500 GB	Checkpoint
m5.2xlarge	8	32	1500 GB	Checkpoint
m4.large	2	8	150 GB	Red Hat
m4.large	2	8	150 GB	Red Hat
m4.large	2	8	150 GB	Red Hat
m4.large	2	8	150 GB	Red Hat
m4.2xlarge	8	32	700 GB	Windows
m4.2xlarge	8	32	700 GB	Windows
m4.xlarge	4	16	140 GB	Red Hat
m4.xlarge	4	16	650 GB	Red Hat
m4.xlarge	4	16	650 GB	Red Hat
m4.xlarge	4	16	440 GB	Red Hat
c4.4xlarge	16	32	160 GB	F5 LTM
c4.4xlarge	16	32	160 GB	F5 LTM
m4.xlarge	4	16	300 GB	Windows
m4.2xlarge	8	32	300 GB	Windows
m4.2xlarge	8	32	5300 GB	Windows
m4.2xlarge	8	32	300 GB	Windows
m4.10xlarge	40	160	1140 GB	Red Hat
m4.2xlarge	8	32	300 GB	Windows
m4.xlarge	4	16	150 GB	Red Hat
m4.xlarge	4	16	2200 GB	Red Hat
m4.4xlarge	16	64	2200 GB	Red Hat
m4.4xlarge	16	64	2200 GB	Red Hat
m4.4xlarge	16	64	2200 GB	Red Hat
m4.4xlarge	16	64	2200 GB	Red Hat
m4.10xlarge	40	160	1175 GB	Red Hat
m4.10xlarge	40	160	1175 GB	Red Hat
m4.10xlarge	40	160	1175 GB	Red Hat
m4.10xlarge	40	160	840 GB	Red Hat
m4.10xlarge	40	160	325 GB	Red Hat
m4.10xlarge	40	160	325 GB	Red Hat
m4.10xlarge	40	160	140 GB	Red Hat
m4.10xlarge	40	160	140 GB	Red Hat

m4.4xlarge	16	64	140 GB	Red Hat
m4.4xlarge	16	64	640 GB	Red Hat
m4.4xlarge	16	64	640 GB	Red Hat
m4.4xlarge	16	64	640 GB	Red Hat
m4.4xlarge	16	64	640 GB	Red Hat
m4.4xlarge	16	64	640 GB	Red Hat
m4.4xlarge	16	64	640 GB	Red Hat
m4.4xlarge	16	64	640 GB	Red Hat
m4.4xlarge	16	64	640 GB	Red Hat
m4.4xlarge	16	64	640 GB	Red Hat
m4.4xlarge	16	64	640 GB	Red Hat
m4.xlarge	4	16	140 GB	Red Hat
m4.xlarge	4	16	140 GB	Red Hat
m4.2xlarge	8	32	140 GB	Red Hat
m4.2xlarge	8	32	140 GB	Red Hat
m4.4xlarge	16	64	1325 GB	Red Hat
m4.4xlarge	16	64	1325 GB	Red Hat
m4.2xlarge	8	32	150 GB	Red Hat
m4.xlarge	4	16	1175 GB	Red Hat
m4.2xlarge	8	32	140 GB	Red Hat
m4.2xlarge	8	32	325 GB	Red Hat
m4.10xlarge	40	160	4250 GB	Red Hat
m4.10xlarge	40	160	6250 GB	Red Hat
m4.large	2	8	30 GB	Red Hat
m4.large	2	8	140 GB	Red Hat
t2.2xlarge	8	32	300 GB	Windows
t2.2xlarge	8	32	300 GB	Windows

Description
Production Checkpoint Firewall 1 (Old)
Production Checkpoint Firewall 2 (Old)
Production Checkpoint Firewall 1
Production Checkpoint Firewall 2
Production Checkpoint Firewall Management Server
Production Checkpoint Firewall Management Server
IPv6 Proxy
IPv6 Proxy
IPv6 Proxy
IPv6 Proxy
Production Jump Server 1
Production Jump Server 2
Production Mail Server
Production Content Management Server 1
Production Content Management Server 2
Production Content Management Server 3
Production F5 LTM Load Balancer 1
Production F5 LTM Load Balancer 2
Production Windows Active Directory Server 1
Production Windows Active Directory Server 2
Production Arcserve Backup Server 1
Production Symantec Antivirus Server 1
Production Splunk log Collection and Analysis Server
Production Nessus Scanner Server 1
Production Hadoop Horton works Ambari Server
Production Hadoop Server 1
Production Hadoop Server 2
Production Hadoop Server 3
Production Hadoop Server 4
Production Hadoop Server 5
Production Vertica Server 1
Production Vertica Server 2
Production Vertica Server 3
Production JBOSS EAP Server 1
Production JBOSS EAP Server 2
Production JBOSS EAP Server 3
Production Informatica Server 1
Production Informatica Server 2

Production Informatica Server 3
Production Elastic Search Server 1
Production Elastic Search Server 2
Production Elastic Search Server 3
Production Elastic Search Server 4
Production Elastic Search Server 5
Production Elastic Search Server 6
Production Elastic Search Server 7
Production Elastic Search Server 8
Production Elastic Search Server 9
Production Elastic Search Server 10
Production Search API Server 1
Production Search API Server 2
Production Search API Server 3
Production Search API Server 4
Production Operations Server 1
Production Operations Server 2
Production Red Hat Directory Server 1 (LDAP)
Production Log Manager Server 1
Production Hyperic Application Server 1
Production Hyperic Database Server 1
Production PostgreSQL Database Server 1
Production PostgreSQL Database Server 2
Rescure Instance for RHEL 7
Rescure Instance for RHEL 6

REI Team Jump Server 2
REI Team Jump Server 4
Counts:-

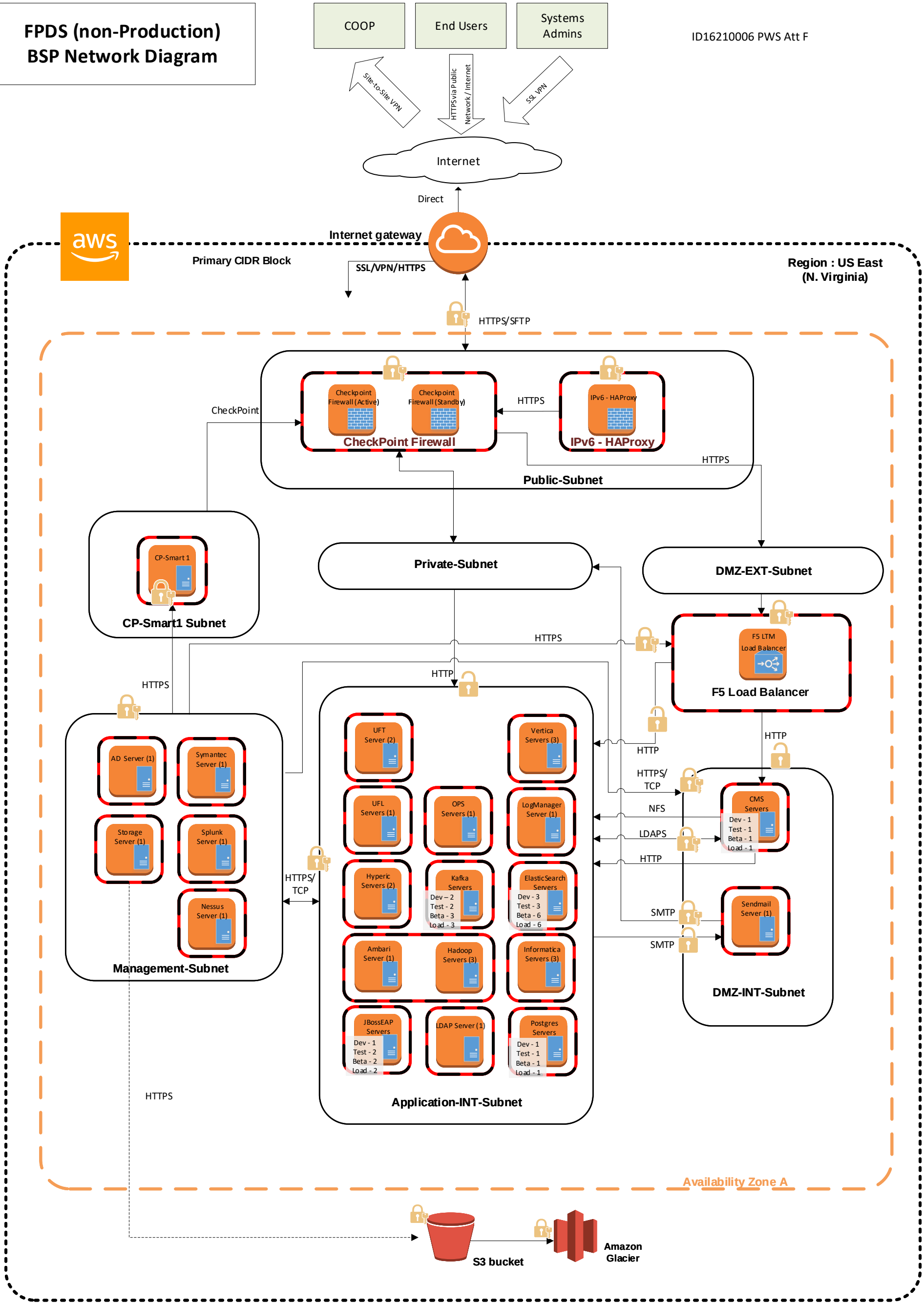
FPDS COOP Servers

Instance Type	vCPU	Memory	EBS (GB)	OS
c4.4xlarge	16	30	500	Checkpoint
m4.xlarge	4	16	650	Red Hat
c4.4xlarge	16	30	100	F5 LTM
m4.xlarge	4	16	300	Windows
m4.2xlarge	8	32	1175	Red Hat
m4.2xlarge	8	32	1175	Red Hat
m4.2xlarge	8	32	**1175**	Red Hat
m4.10xlarge	40	160	837	Red Hat
m4.10xlarge	40	160	837	Red Hat
m4.4xlarge	16	64	640	Red Hat
m4.4xlarge	16	64	640	Red Hat
m4.4xlarge	16	64	640	Red Hat
m4.xlarge	4	16	140	Red Hat
m4.xlarge	4	16	140	Red Hat
m4.2xlarge	8	32	550	Red Hat
m4.xlarge	4	16	150	Red Hat
m4.4xlarge	16	32	4236	Red Hat
m4.4xlarge	16	32	4236	Red Hat

Description
COOP Checkpoint Firewall 1
COOP Content Management Server 1
COOP F5 Load Balancer 1
Windows Active Directory Server 1, DNS
COOP Vertica Server 1
COOP Vertica Server 2
COOP Vertica Server 3
COOP JBoss EAP Sever 1
COOP JBoss EAP Sever 2
COOP Elastic Search Server 1
COOP Elastic Search Server 2
COOP Elastic Search Server 3
COOP Search API Server 1
COOP Search API Server 2
COOP Operations Server 1
COOP Red Hat Directory Server 1
COOP PostgreSQL Database Server 1
COOP PostgreSQL Database Server 2

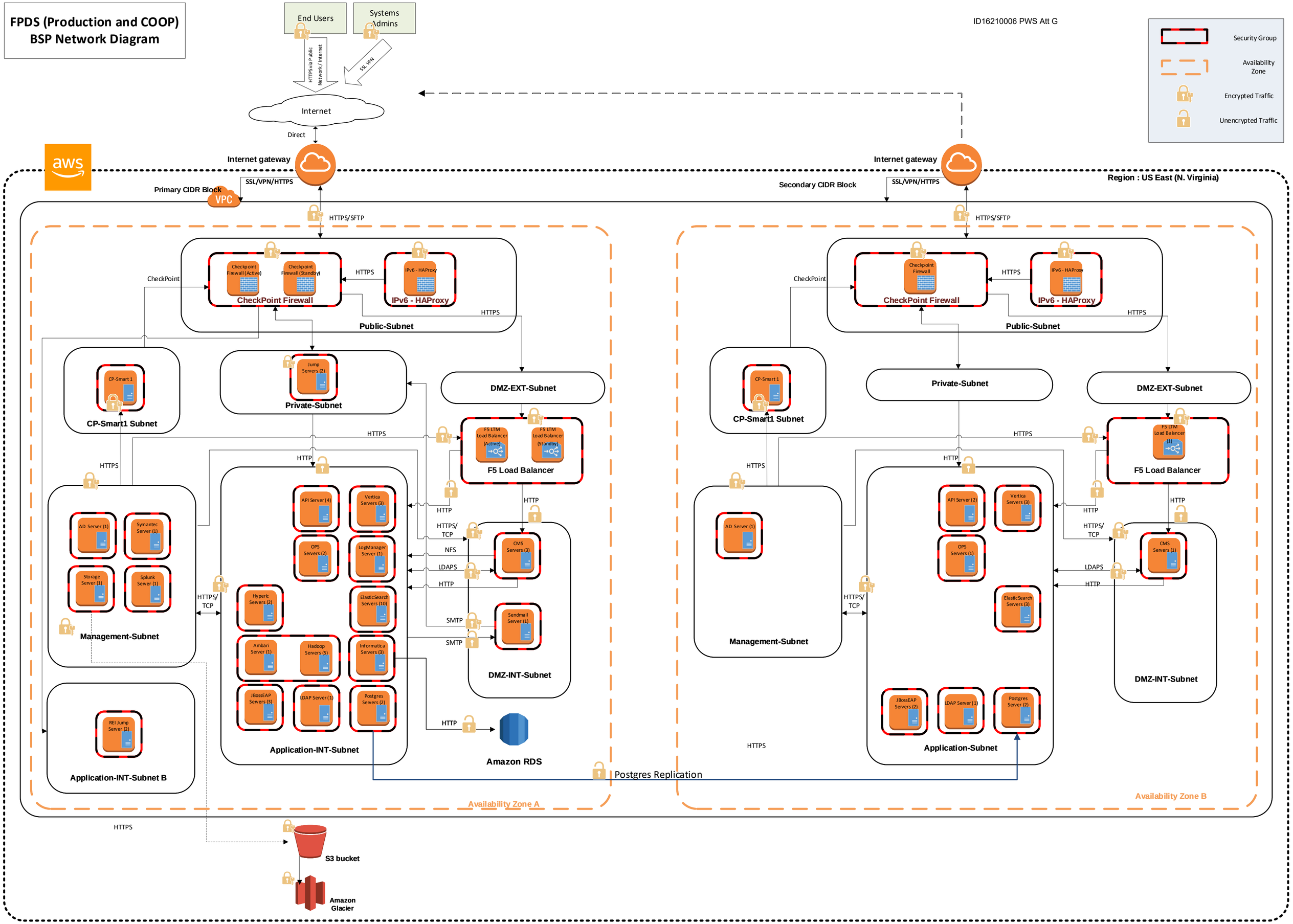
FPDS (non-Production) BSP Network Diagram

ID16210006 PWS Att F



FPDS (Production and COOP) BSP Network Diagram

ID16210006 PWS Att G



USASpending METRICS REPO					
Performance Measures	**Metric**	**Oct-14**	**Nov-14**	**Dec-14**	**Jan-15**
Green Highlighted Cells = Externally Reported					
Availability	**System Availability (Monthly) (100% - system downtime percent)**				
Frequency and Depth\	**Trend usage and effectiveness of website (# of site visits)**				
Frequency and Depth	**USA Spending Mobile Users (% of Mobile Users)**				
Help Desk	**Respond to comments received (# of days)**				
Help Desk	**Resolve help desk tickets (# of days)**				

RT - FY 2015

Feb-15	Mar-15	Apr-15	May-15	Jun-15	Jul-15	Aug-15	Sep-15

	Monthly =
	Total =
	FY17 YTD Total =
System Availability (Monthly)	
Number of Registered Users (Total)	
# of Registered Civilian Gov't Users (Total)	
# of Registered DOD Gov't Users (Total)	
# of Registered Public Users (Total)	
Number of Hits (Monthly)	
Number of Searches (Monthly)	
# of Standard Reports (Monthly)	
# of Standard Reports Run - Public (Monthly)	
# of Standard Reports Run - Civilian Gov't (Monthly)	
# of Standard Reports Run - DoD Gov't (Monthly)	
# of Ad Hoc Reports (Monthly)	
# of Ad Hoc Reports Run - Public (Monthly)	
# of Ad Hoc Reports Run - Civilian Gov't (Monthly)	
# of Ad Hoc Reports Run - DoD Gov't (Monthly)	
# of EZ Searches Performed (Monthly)	
# of Visit (Monthly)	
# of Unique Visitors (Monthly)	
# of Visits per Visitor (Monthly)	
Number of Eligible Records (FY15 YTD Total)	
# of Actions Reported - Civilian (FY15 YTD Total)	
% of Actions - Civilian (FY15 YTD Total)	
$ Obligated - Civilian (FY15 YTD Total)	
% of $ Obligated - Civilian (FY15 YTD Total)	
# of Actions Reported - DoD (FY15 YTD Total)	
% of Actions - DoD (FY15 YTD Total)	
$ Obligated - DoD (FY15 YTD Total)	
% of $ Obligated - DoD (FY15 YTD Total)	
# of Tier 2 Help Desk Incidents Escalated (Total)	
# of Tier 2 Incidents Escalated (Monthly)	
# of Tier 2 Technical Incidents Resolved (Monthly)	
Tier 2 Technical Resolution Rate in Days (Monthly)	

Monthly Result
DEFINITION
Number occuring between the first day and the last day of the month
Cumulative total on the last day of the month, i.e. a snapshot.
Cumulative total for the current fiscal year as of the last day of the month, i.e. a running FY total.
Percent of time FPDS-NG was available (100% minus unscheduled downtime) during that month.
Sum of the total registered civilian government, DoD, and public users on the last day of the month.
Total number of registered civilian government users on the last day of the month.
Total number of registered government users from DoD on the last day of the month.
Total number of registered public users on the last day of the month.
Number of hits received on FPDS-NG during that month.
NG during that month.
Sum of all the Standard Reports run by any type of users during that month.
Number of Standard Reports run by public users during that month.
Number of Standard Reports run by civilian government users during that month.
Number of Standard Reports run by DoD government users users during that month.
Sum of all the Ad Hoc Reports run by any type of users during that month.
Number of Ad Hoc Reports run by public users during that month.
Number of Ad Hoc run by civilian government users during that month.
Number of Ad Hoc run by DoD government users users during that month.
Number of EZ Searches Performed during that month.
Number of visits (or user sessions) to FPDS-NG during that month.
Number of unique visitors to FPDS-NG during that month.
Average number of visits per visitor to FPDS during that month.
month, i.e. a running total.
last day of the month, i.e. a running total.
Percent of the number of Civilian actions divided by the Total for the fiscal year.
the last day of the month, i.e. a running dollar value total.
Percent of the dollar value obligated by Civilian agency actions reported during the fiscal year as of the last day of the month, i.e. a percent representing the running dollar value total.
Cumulative number of actions reported by Civilian agency users reported during the fiscal year as of the last day of the month, i.e. a running total.
Percent of the number of Civilian actions divided by the Total for the fiscal year.
Cumulative amount of dollars obligated by Civilian agency actions reported during the fiscal year as of the last day of the month, i.e. a running dollar value total.
Percent of the dollar value obligated by Civilian agency actions reported during the fiscal year as of the last day of the month, i.e. a percent representing the running dollar value total.
Cumulative total of the number of tickets escalated to IBM Tier 2 for help desk support pulled on the last day of the month.
Number of Tier 2 Technical incidents escalated from Tier 1 or Tier 2 Functional during the month.
Number of Tier 2 tickets escalated to IBM for help desk support resolved during the month.
Average number of days it took for a Tier 2 Technical incident to be resolved during the month.

EXAMPLE
0
0
0
0

USASpending METRICS REPO					
Performance Measures	**Metric**	**Oct-14**	**Nov-14**	**Dec-14**	**Jan-15**
Green Highlighted Cells = Externally Reported					
Availability	**System Availability (Monthly) (100% - system downtime percent)**				
Frequency and Depth\	**Trend usage and effectiveness of website (# of site visits)**				
Frequency and Depth	**USA Spending Mobile Users (% of Mobile Users)**				
Help Desk	**Respond to comments received (# of days)**				
Help Desk	**Resolve help desk tickets (# of days)**				

RT - FY 2015

Feb-15	Mar-15	Apr-15	May-15	Jun-15	Jul-15	Aug-15	Sep-15

	Monthly =
	Total =
	FY17 YTD Total =
System Availability (Monthly)	
Number of Registered Users (Total)	
# of Registered Civilian Gov't Users (Total)	
# of Registered DOD Gov't Users (Total)	
# of Registered Public Users (Total)	
Number of Hits (Monthly)	
Number of Searches (Monthly)	
# of Standard Reports (Monthly)	
# of Standard Reports Run - Public (Monthly)	
# of Standard Reports Run - Civilian Gov't (Monthly)	
# of Standard Reports Run - DoD Gov't (Monthly)	
# of Ad Hoc Reports (Monthly)	
# of Ad Hoc Reports Run - Public (Monthly)	
# of Ad Hoc Reports Run - Civilian Gov't (Monthly)	
# of Ad Hoc Reports Run - DoD Gov't (Monthly)	
# of EZ Searches Performed (Monthly)	
# of Visit (Monthly)	
# of Unique Visitors (Monthly)	
# of Visits per Visitor (Monthly)	
Number of Eligible Records (FY15 YTD Total)	
# of Actions Reported - Civilian (FY15 YTD Total)	
% of Actions - Civilian (FY15 YTD Total)	
$ Obligated - Civilian (FY15 YTD Total)	
% of $ Obligated - Civilian (FY15 YTD Total)	
# of Actions Reported - DoD (FY15 YTD Total)	
% of Actions - DoD (FY15 YTD Total)	
$ Obligated - DoD (FY15 YTD Total)	
% of $ Obligated - DoD (FY15 YTD Total)	
# of Tier 2 Help Desk Incidents Escalated (Total)	
# of Tier 2 Incidents Escalated (Monthly)	
# of Tier 2 Technical Incidents Resolved (Monthly)	
Tier 2 Technical Resolution Rate in Days (Monthly)	

Monthly Result
DEFINITION
Number occuring between the first day and the last day of the month
Cumulative total on the last day of the month, i.e. a snapshot.
Cumulative total for the current fiscal year as of the last day of the month, i.e. a running FY total.
Percent of time FPDS-NG was available (100% minus unscheduled downtime) during that month.
Sum of the total registered civilian government, DoD, and public users on the last day of the month.
Total number of registered civilian government users on the last day of the month.
Total number of registered government users from DoD on the last day of the month.
Total number of registered public users on the last day of the month.
Number of hits received on FPDS-NG during that month.
NG during that month.
Sum of all the Standard Reports run by any type of users during that month.
Number of Standard Reports run by public users during that month.
Number of Standard Reports run by civilian government users during that month.
Number of Standard Reports run by DoD government users users during that month.
Sum of all the Ad Hoc Reports run by any type of users during that month.
Number of Ad Hoc Reports run by public users during that month.
Number of Ad Hoc run by civilian government users during that month.
Number of Ad Hoc run by DoD government users users during that month.
Number of EZ Searches Performed during that month.
Number of visits (or user sessions) to FPDS-NG during that month.
Number of unique visitors to FPDS-NG during that month.
Average number of visits per visitor to FPDS during that month.
month, i.e. a running total.
last day of the month, i.e. a running total.
Percent of the number of Civilian actions divided by the Total for the fiscal year.
the last day of the month, i.e. a running dollar value total.
Percent of the dollar value obligated by Civilian agency actions reported during the fiscal year as of the last day of the month, i.e. a percent representing the running dollar value total.
Cumulative number of actions reported by Civilian agency users reported during the fiscal year as of the last day of the month, i.e. a running total.
Percent of the number of Civilian actions divided by the Total for the fiscal year.
Cumulative amount of dollars obligated by Civilian agency actions reported during the fiscal year as of the last day of the month, i.e. a running dollar value total.
Percent of the dollar value obligated by Civilian agency actions reported during the fiscal year as of the last day of the month, i.e. a percent representing the running dollar value total.
Cumulative total of the number of tickets escalated to IBM Tier 2 for help desk support pulled on the last day of the month.
Number of Tier 2 Technical incidents escalated from Tier 1 or Tier 2 Functional during the month.
Number of Tier 2 tickets escalated to IBM for help desk support resolved during the month.
Average number of days it took for a Tier 2 Technical incident to be resolved during the month.

EXAMPLE
0
0
0
0

1.1 SAM Integration Environment SLA Measures

1.1.1 Measure #1: Help Desk Outstanding Ticket Age

Performance Requirement:	Help Desk Outstanding Ticket Age
Acceptable Quality Level (AQL):	**Less than 10% of all Tier 2 open tickets open are more than 30 days old**
Data Source:	The Help Desk Tracking Tool
How It Is Measured:	Number of tickets older than 30 days divided by the total ticket number of tickets escalated to Tier 2 in the period.
IBM's Approach for Achieving:	Tickets are reviewed daily by the Help Desk Lead. These are addressed on a first in first out basis. When it is determined that tickets open tickets are growing in age, the Help Desk lead will evaluate root causes and shift focus on the oldest tickets.
Data Accessibility:	GSA providing IBM the ability to have access to the help desk tool data for actual escalation time and date.
Restrictions:	Escalations from Tier 1 to Tier 2 must be at 10% or below. Tickets that have dependencies on Tier 3 or external agencies will not be counted. Reports containing metrics related to this metric will be provided to IBM by the third-party tool owner. System defects and enhancements that prevent closure of the ticket will not be counted since this is not a reflection of the Help Desk effectiveness.
IBM Owner:	Help Desk Lead

Pass Example: Current open ticket count as of the end of the month is 1,000. There are 70 tickets determined to be older than 30 days. Therefore 70/1000 = 7%

1.1.2 Measure #2: Help Desk Ticket Closure Rate

Performance Requirement:	Help Desk Ticket Closure Rate
Acceptable Quality Level (AQL):	**More than 90% of the total tickets escalated to Tier 2 over the last 30 days have been closed**
Data Source:	The Help Desk Tracking Tool
How It Is Measured:	Number of tickets closed in a month divided by the number of tickets escalated to Tier 2
IBM's Approach for Achieving:	The Help Desk Lead will assign resources, so ticket closure rate stays close to the number of those escalated to Tier 2. This is to ensure that open ticket counts do not increase over time.
Data Accessibility:	GSA providing IBM the ability to have access to the help desk tool data for actual escalation time and date.

Restrictions:	Escalations from Tier 1 to Tier 2 must be at 10% or below. Reports containing metrics related to this metric will be provided to IBM by the third-party tool owner.
IBM Owner:	Help Desk Lead

Pass Example: Throughout the course of the month, there were 3,000 help desk tickets escalated to Tier 2 help desk. Within the same period, 2,880 help desk tickets were closed. Therefore 2,880/3,000 = 96%

1.1.3 Measure #3: Help Desk Tickets Closed the Same Day

Performance Requirement:	Help Desk Tickets Closed the Same Day
Acceptable Quality Level (AQL):	**More than 30% of Tier 2 tickets closed within 72 hours**
Data Source:	The Help Desk Tracking Tool
How It Is Measured:	Number of monthly total tickets escalated to Tier 2 that are closed within 72 hours. The time starts when the ticket is placed in the Tier 2 queue and closed when set to 'Pending Customer'
IBM's Approach for Achieving:	Once a ticket is escalated and verified by the Help Desk lead as a properly escalated ticket, it is assigned to a Tier 2 agent. The agent will research the issue, provide a resolution and move the ticket to Pending Customer who has three days to respond before it is closed.
Data Accessibility:	GSA providing IBM the ability to have access to the help desk tool data for actual escalation time and date.
Restriction:	Escalations from Tier 1 to Tier 2 must be at 10% or below. Tickets that have dependencies on Tier 3 or external agencies will not be counted. Reports containing metrics related to this metric will be provided to IBM by the third-party tool owner. System defects and enhancements that prevent closure of the ticket will not be counted since this is not a reflection of the Help Desk effectiveness.
IBM Owner:	Help Desk Lead

Pass Example: Throughout the course of the month, there were 3,000 help desk tickets escalated to Tier 2 help desk. Within the period, there were 1,200 tickets that were closed within 72 hours. Therefore 1,200/3,000 = 40%

1.1.4 Measure #4: Help Desk Average Tier 2 Technical Initial Review Time

Performance Requirement:	Help Desk Average Initial Review Time
Acceptable Quality Level (AQL):	**Less than 3 (business days)**
Data Source:	The Help Desk Tracking Tool

How It Is Measured:	Determined from the time a Tier 2 ticket is escalated to the time is initially reviewed and the user has been contacted. (Business Days). IBM receives a document every week that measures the time it takes for Tier 2 agent to respond to a user after FSD has escalated the item.
IBM's Approach for Achieving:	Once a ticket is escalated to Tier 2 Technical, a Tier 2 agent should assign the ticket to themselves and contact the user immediately.
Data Accessibility:	GSA providing IBM the ability to have access to the help desk tool data for actual escalation time and date.
Restriction:	Escalations from Tier 1 to Tier 2 must be at 10% or below. Tickets that have dependencies on Tier 3 or external agencies will not be counted. Reports containing metrics related to this metric will be provided to IBM by the third-party tool owner. System defects and enhancements that prevent closure of the ticket will not be counted since this is not a reflection of the Help Desk effectiveness.
IBM Owner:	Help Desk Lead

1.1.5 Measure #5: Help Desk Average Tier 2 Close Time

Performance Requirement:	Help Desk Average Tier 2 Close Time
Acceptable Quality Level (AQL):	**Less than 5 (business days)**
Data Source:	The Help Desk Tracking Tool
How It Is Measured:	Determined from the time a Tier 2 ticket is escalated to the time it is closed. (Business Days)
IBM's Approach for Achieving:	Once a ticket is escalated and verified by the Help Desk lead as a properly escalated ticket, it is assigned to a Tier 2 agent. The agent will research the issue, provide a resolution and move the ticket to Pending Customer who has three days to respond before it is closed
Data Accessibility:	GSA providing IBM the ability to have access to the help desk tool data for actual escalation time and date.
Restriction:	Escalations from Tier 1 to Tier 2 must be at 10% or below. Tickets that have dependencies on Tier 3 or external agencies will not be counted. Reports containing metrics related to this metric will be provided to IBM by the third-party tool owner. System defects and enhancements that prevent closure of the ticket will not be counted since this is not a reflection of the Help Desk effectiveness.
IBM Owner:	Help Desk Lead

1.1.6 Measure #6: Help Desk Reopened Tier 2 Technical Tickets

Performance Requirement:	Reopened Tier 2 Technical Tickets
Acceptable Quality Level (AQL):	**Less than 5% Reopened**
Data Source:	The Help Desk Tracking Tool
How It Is Measured:	Tickets that were moved to resolved but reopened by the user because issue was not resolved. Service Now has a tool that allows you to see if any tickets were reopened during a period of time selected.
IBM's Approach for Achieving:	Tier 2 Technical Agents should not close any help desk tickets until they have verified with the user that the issue is resolved.
Data Accessibility:	GSA providing IBM the ability to have access to the help desk tool data for actual escalation time and date.
Restriction:	Escalations from Tier 1 to Tier 2 must be at 10% or below. Tickets that have dependencies on Tier 3 or external agencies will not be counted. Reports containing metrics related to this metric will be provided to IBM by the third-party tool owner. System defects and enhancements that prevent closure of the ticket will not be counted since this is not a reflection of the Help Desk effectiveness.
IBM Owner:	Help Desk Lead

1.1.7 Measure #7: Help Desk Foreign Registrant Tickets

Performance Requirement:	Help Desk Foreign Registrant Tickets
Acceptable Quality Level (AQL):	**Less than 25% of all Tier 2 Tickets are Foreign**
Data Source:	The Help Desk Tracking Tool
How It Is Measured:	Total count of Tier 2 tickets opened regarding foreign registrations
IBM's Approach for Achieving:	IBM maintains effective monitoring of the help desk queue, so issues reported by foreign registrations can be investigated immediately so other foreign entities do not experience the same issues.
Data Accessibility:	GSA providing IBM the ability to have access to the help desk tool data for actual escalation time and date.

Restriction:	Escalations from Tier 1 to Tier 2 must be at 10% or below. Tickets that have dependencies on Tier 3 or external agencies will not be counted. Reports containing metrics related to this metric will be provided to IBM by the third-party tool owner. System defects and enhancements that prevent closure of the ticket will not be counted since this is not a reflection of the Help Desk effectiveness.
IBM Owner:	Help Desk Lead

1.1.8 Measure #8: Reputation – Number of Reputation Incidents

Performance Requirement:	Number of Reputation Incidents
Acceptable Quality Level (AQL):	**Zero**
Data Source:	Stakeholder manual identification
How It Is Measured:	A reputation incident is one in which unapproved content is displayed on a production website, generally referred to as defacement. Defacement incidents are tracked across the environment as a whole (defacement of any website or component is treated the same). This is a yes/no metric. Time to recover from defacement contributes to unavailability calculations.
IBM's Approach for Achieving:	The IBM team continually strives to support GSA and its stakeholders to be successful. Activities outlined in the QCP support the quality efforts which include process controls, auditing, testing defect identification and defect correction. The integrity of all the AOCS systems is highly visible and any disruption or negative event can result in erosion of GSA's reputation.
Data Accessibility:	Incorrect data displayed on the website as result of a system issue where approved specification (data, functional or security) is not met. This is exclusive of extracts which fall under data quality. Data displayed as user entered or interfaced from another system will not be considered.
Restriction:	Agreement to reputation events will involve concurrence from FAS, CIO, COR and the IBM team.
IBM Owner:	All Team Members

1.1.9 Measure #9: Availability – Response Time

Performance Requirement:	Availability of www.sam.gov
Acceptable Quality Level (AQL):	**99.80%**

Data Source:	Rational Performance Test monitoring
FPDS Requirements:	Present a screen to users within 5 seconds Changes to the technical environment which may negatively impact data submission and/or reporting shall not be implemented between July and October
How It Is Measured:	Unavailable if system wide response takes longer than 5 seconds. Measured at the solution edge, net of scheduled maintenance. Calculated as the total hours of site availability per month divided by the total hours of a month. The site is considered unavailable when no external user is able to access the website.
IBM's Approach for Achieving:	The IBM team maintains the software and hardware of SAM. The hosting team continually monitors the servers and application for availability.
Data Accessibility:	Server and application monitoring tools are utilized to observe availability of the system.
Restriction:	Third party data center (hosting vendor) maintains 100% uptime.
IBM Owner:	Hosting & Infrastructure Lead

Example: The AOCS systems were unavailable for 1 hour on 10/5/2013. Since there are 31 days in October and 24 hours in a day, the total possible available hours are 744.

743/744= 99.86% = Pass

1.1.10 Measure #11: Availability - Extracts

Performance Requirement:	Availability of Extracts
Acceptable Quality Level (AQL):	**99.80%**
Data Source:	Stakeholder manual identification
How It Is Measured:	All Extracts will be posted and accessible for the time period of the approved specification. Unavailable if active users are unable to access the posted extracts. Calculated as the total hours of available extracts per month divided by the total hours of a month.
IBM's Approach for Achieving:	The IBM team continually monitors the SAM extracts for availability. Extracts are posted daily and undergo a quality control process of review prior to posting. Posted extracts are audited periodically for availability.
Data Accessibility:	Server and application monitoring tools are utilized to observe availability of the system.
Restriction:	Third party data center (hosting vendor) maintains 100% uptime.
IBM Owner:	Extracts & Interfaces Lead

Example: Extracts were unavailable for 1 hour on 10/5/2013. Since there are 31 days in October and 24 hours in a day, the total possible available hours are 744.

743/744= 99.86% = Pass

1.1.11 Measure #13: Availability – SAM Scheduled Maintenance

Performance Requirement:	Scheduled Maintenance
Acceptable Quality Level (AQL):	**Less than 16 Hours**
Data Source:	Hyperic Monitoring
Requirement:	System downtime (defined as the system is not accessible and operable by the user), will not exceed 8 hours per 12-month period (approximately 99.9% up time) exclusive of scheduled down time. Scheduled down time may occur not more frequently than once each month for a time period of up to 24 hours (noon Saturday to noon Sunday) with no scheduled down time during the month of September.
How It Is Measured:	Total scheduled downtime each month will not exceed 16 hours
IBM's Approach for Achieving:	IBM will request downtime at least 24 hours prior the maintenance window. Upon approval, the scheduled downtime will count towards the total available time for the month. The IBM team will work to minimize downtime by combining activities that require server reboot and therefore needing a scheduled maintenance window.
Data Accessibility:	Server and application monitoring tools are utilized to observe the activities of the system.
Restriction:	Unscheduled maintenance as a result of external agency failure in communication will not count against this metric. An example would be change in an external interface without prior notification resulting in the SAM servers requiring a reboot to resume normal operations. Exceptions must be approved by GSA.
IBM Owner:	Hosting & Infrastructure Lead

1.1.12 Measure #14: Availability – Interface Availability

Performance Requirement:	Availability of Interfaces
Acceptable Quality Level (AQL):	**97.00%**
Data Source:	Hyperic Monitoring
How It Is Measured:	Agency critical interfaces run within an hour of specific execution time. Calculated as the total hours of Interface availability per month divided by the total hours of a month.

IBM's Approach for Achieving:	IBM maintains a Master Interface spreadsheet that lists out those interfaces. Each interface specification outlines the time in which the interface needs to run. If an interface does not run within an hour of the specified time, the monitoring team will report this as a miss and research the reason for the late delivery. The team will continue to implement process improvements to address the root causes
Data Accessibility:	Manual interface monitoring and use of Interface Tracking spreadsheet.
Restriction:	Third party data center (hosting vendor) maintains 100% uptime.
IBM Owner:	Extracts & Interfaces Lead

There are 75 interfaces in total that SAM, maintains which are listed on the Interface Master List. If an interface is determined to not be operational, this is noted on the Interfaces Tracking Spreadsheet.

1.1.13 Measure #17: Business Process – Average Cycle Time

Performance Requirement:	A Record's Average Cycle Time
Acceptable Quality Level (AQL):	**7 Days or less**
Data Source:	Database Query
How It Is Measured:	The average time it takes a user to complete a registration and move from Draft to Active. The start time of a new or updated registration is captured by the system. The date and time in which a registration becomes active is also captured. All of the start times and activated times for a month are used calculate the average by using those records that were actually completed within the reporting period.
IBM's Approach for Achieving:	On a weekly basis, the IBM team provides a metric dashboard that contain the average cycle time. The team will continually look at ways in which reduction in cycle times can be achieved such as working with third party agencies to increase processing speed and performing maintenance on the application to expedite the user registration process.
Data Accessibility:	Database queries using PIT start and activation times.
Restriction:	IGT only registrations will be excluded as they are processed instantaneously. Pending CAGE or IRS will not exceed 7 days.
IBM Owner:	Extracts & Interfaces Lead

1.1.14 Measure #18: Business Process – Interface Jobs - Extracts (Daily)

Performance Requirement:	Interface Job Extracts (Daily)

Acceptable Quality Level (AQL):	**Less than 8 hours**
Data Source:	Database Query
How It Is Measured:	The average time it takes to generate the daily extract file
IBM's Approach for Achieving:	Continuous 24/7 monitoring and sends out the alert emails to the concerned Interface POC's if the interface is taking longer than usual or fixing the bug before it hits the SLA
Data Accessibility:	Automated monitoring emails which sends out every day to the team about the status of the interfaces, documented in Interface monitoring document
Restriction:	Includes only entity profiles within the federal government for many functions, including, procurement, contracts, payments, size determination, and validation
IBM Owner:	Extracts & Interfaces Lead

1.1.15 Measure #19: Business Process – Interface Jobs – Extracts (Monthly)

Performance Requirement:	Interface Job Extracts (Monthly)
Acceptable Quality Level (AQL):	**Less than 24 hours**
Data Source:	Database Query
How It Is Measured:	The average time it takes to generate the monthly extract file
IBM's Approach for Achieving:	Continuous 24/7 monitoring and sends out the alert emails to the concerned Interface POC's if the interface is taking longer than usual or fixing the bug before it hits the SLA
Data Accessibility:	Automated monitoring emails which sends out every day to the team about the status of the interfaces, documented in Interface monitoring document
Restriction:	Includes only entity profiles within the federal government for many functions, including, procurement, contracts, payments, size determination, and validation
IBM Owner:	Extracts & Interfaces Lead

1.1.16 Measure #20: Business Process – Exclusions Created

Performance Requirement:	Exclusions Created via e-mail or upload
Acceptable Quality Level (AQL):	**Less than 24 hours**
Data Source:	Database Query
How It Is Measured:	The average time it takes to generate an exclusion.

IBM's Approach for Achieving:	Continuous 24/7 monitoring and sends out the alert emails to the concerned Interface POC's if the interface is taking longer than usual or fixing the bug before it hits the SLA
Data Accessibility:	Automated monitoring emails which sends out every day to the team about the status of the interfaces, documented in Interface monitoring document
Restriction:	Does not include exclusions entered in via the front end.
IBM Owner:	Extracts & Interfaces Lead

1.1.17 Measure #21: Security - Outages due to security

Performance Requirement:	Outages due to security incidents (unplanned unavailability)
Acceptable Quality Level (AQL):	**No more than 1 outage per month**
Data Source:	Stakeholder manual identification
How It Is Measured:	Number of outages due to incidents (unplanned unavailability). Sam.gov is unavailable due to a security incident.
IBM's Approach for Achieving:	Continuous monitoring and improvements through vulnerability scanning and remediation, monthly patching, ongoing assessment and improvement of security controls through coordination with the ISSO and system owner
Data Accessibility:	Outages that are requested by GSA as a result of a formally defined security incident as outlined in IT Security Procedural Guide: Incident Response (IR) CIO-IT Security-01-02.
Restriction:	None
IBM Owner:	Information Assurance Lead

1.1.18 Measure #22: Security - Security Risks and Controls

Performance Requirement:	Proportion of information security risks for which satisfactory controls have been fully implemented
Acceptable Quality Level (AQL):	**90% deployed IAW approved schedule**
Data Source:	Stakeholder manual identification
How It Is Measured:	Security Related Items Identified on the POA&M have a plan of action and are remediated in the appropriate timeframe.
IBM's Approach for Achieving:	GSA and IBM will follow the Security Plan process of process of scanning and identifying potential vulnerabilities in the.gov applications.

Data Accessibility:	Plan of Action and Milestone (POA&M) report provided by GSA. As defined in the security requirements, all High POA&Ms are to be remediated within 30 days of being identified as a POA&M.
Restriction:	GSA will provide IBM monthly updates to content within the POA&M for SLA reporting. Pending or approved AoRs may override the POA&M requirement and therefore will not be counted. POA&M items may be approved by GSA to be completed in accordance with a scheduled maintenance window or FastPath or Quarterly release that is outside of the 30-day window. These approved items will not be included in the calculation. Exceptions beyond 30 days for remediation due to planned release scheduling must be approved by GSA.
IBM Owner:	Information Assurance Lead

Example: There were 20 POA&Ms identified in a month by GSA. 18 have been addressed within 30 days. 18/20 = 90% = Pass.

1.1.19 Measure #23: Security - Security Reporting Timeliness

Performance Requirement:	Time lag between detection, reporting and acting upon security incidents
Acceptable Quality Level (AQL):	**At least 90% of incidents addressed per response table**
Data Source:	Stakeholder manual identification
How It Is Measured:	Security incidents are responded to in the timeframes identified in current Incident Response Table
IBM's Approach for Achieving:	GSA and IBM will follow the Security Plan process of timely identification and reporting of security incidents. Weekly meetings between the GSA ISSO and IBM Information Assurance Lead will review any open security incidents.
Data Accessibility:	GSA ISSO to maintain and provide agreed upon incident response table.
Restriction:	GSA to provide IBM the Incident Response Table
IBM Owner:	Information Assurance Lead

1.1.20 Measure #24: Data Quality - Data Stewardship Quality Index

Performance Requirement:	Data Stewardship Quality Index
Acceptable Quality Level (AQL):	**Average 99.8% across the relevant time period**
Data Source:	Stakeholder manual identification

How It Is Measured:	Quality of data as presented within extracts as indicated by the number of DUNS numbers with data defects.
IBM's Approach for Achieving:	Each month as the monthly extract files are generated, a quality check is conducted on the outputs against the criteria identified in the AOCS Data Quality plan
Data Accessibility:	Data element errors defined in the approved version of the Operational Data Quality Plan.
Restriction:	This will be measured on the monthly extract files. The daily files use the same data subsets and therefore are affected in the same manner as the monthly files.
IBM Owner:	Extracts & Interfaces Lead

Example Pass Calculation:

Number of records in the file = 600,000

Number of DUNS with defects = 1,000

1,000/600,000 = .17 or 99.83%

Example Data Quality Report (The first row indicates a failed metric):

Date	Total Data Quality Issues	# of DUNS in File	Percent of Issues per DUNS	%
1/1/2015	1,200	500,000	0.24%	99.76%
2/1/2015	1,100	550,000	0.20%	99.80%
3/1/2015	1,000	600,000	0.17%	99.83%
4/1/2015	900	650,000	0.14%	99.86%
5/1/2015	800	700,000	0.11%	99.89%

Example of Data Quality threshold from the Operational Data Quality Plan:

#	Data Element	Validation Description	Showstopper	H/M/L	Threshold %
1	DUNS	Data Is Present - Make sure there are no blank values	Y	H	0.00%
2	DUNS	Length - Make sure all are 9 Characters	Y	H	0.00%
3	DUNS-PLUS4	Length - Make sure all are 4 Characters	Y	H	0.00%

1.1.21 Measure #25: Data Quality - Extract Provision & Reporting Timeliness

Performance Requirement:	Extract Provision Timeliness
Acceptable Quality Level (AQL):	**95% of Daily and Monthly extracts are posed on time within the month.**
Data Source:	Stakeholder manual identification
FPDS Requirements:	Provide capability to return online standard reports within 10 seconds exclusive of network transit time. For all reports, standard and ad hoc, that are less than 10,000 lines and there are no time-outs. For all reports, standard and ad hoc, over than 10,000 lines the time-out rate is not more than 5%.
How It Is Measured:	Total number of failed events across a month that extracts are late relative to the agreed calendar.
IBM's Approach for Achieving:	IBM maintains a master Interface spreadsheet that lists out those interfaces which generate extracts. Each extract interface specification outlines the time in which the file needs to be posted to SAM. If a file is not posted on time, the monitoring team will report this as a miss and research the reason for the late delivery. The team will continue to implement process improvements to address the root causes
Data Accessibility:	Agencies responsible for password access to secure folders.
Restriction:	Only Extracts listed at the time of approval of this document will be considered for this metric
IBM Owner:	Extracts & Interfaces Lead

Example Pass Calculation: 10 files not posted on time = 396-10=386

386/396= 97%

Example Fail Calculation: 25 files not posted on time =396-25=371

371/396=94%

The list of Daily and Monthly Extracts:

#	Extract Name	Daily Tu-Sa	Monthly	Monthly First Sunday	Monthly 15th	Monthly Last Sunday	Once per FY
1	Legacy CCR FOUO 4082	X	X	X			
2	Legacy CCR FOUO 40822	X	X	X			
3	Legacy CCR MPIN	X	X	X			
4	Legacy CCR Proprietary 4082	X	X	X			
5	Legacy CCR Proprietary 40822	X	X	X			
6	Legacy CCR Sensitive 4082	X	X	X			
7	Legacy CCR Sensitive 40822	X	X	X			
8	Legacy CCR Complete 4082	X	X	X			
9	Legacy CCR Complete 40822	X	X	X			
10	Legacy CCR GSA Complete		X			X	
11	Legacy CCR FOIA		X		X		
12	Legacy FedReg Extract	X					
13	SAM Public (Currently NOT being posted due to D&B/GSA discussions)	X	X	X			
14	SAM FOUO	X	X	X			
15	SAM Sensitive	X	X	X			
16	SAM System-Only	X	X	X			
17	SAM MPIN	X	X	X			
18	SAM FSRS	X	X	X			
19	SAM Reps and Certs (NOT being posted until GSA testing is complete)		X	X			
20	SAM Exclusion Public Extract (Full volume daily file)	X					
21	SAM IRS Exclusion Extract (Full volume daily file)	X					
22	Bio-Preferred Fiscal Year Report (Posted once per FY)						X

1.1.22 Measure #26: Data Quality - Extract Provision Consistency

Performance Requirement:	Extract Provision Consistency
Acceptable Quality Level (AQL):	**Less than 12 Extracts Missed per Year**
Data Source:	Stakeholder manual identification and interface monitoring
How It Is Measured:	Number of times on which the **monthly** extracts are not delivered timely due to technical or data quality issues. Any extract not posted within 4 hours of the specification will be considered a miss.
IBM's Approach for Achieving:	Monthly files are generated from the ETL servers and graphs are run throughout the night to produce the extract of the most current data in SAM. The interfaces that run the graphs are monitored for execution throughout the night. Any failure in the graph creation of the extract can cause a delay in posting of the extract in a timely manner. Additionally, GSA will conduct acceptance testing and provide disposition of extract posting. Any failure to post or delay in posting, the IBM team will notify a GSA POC for communication to stakeholders.
Data Accessibility:	Interface tracking spreadsheet is maintained by the IBM data and interface team. Any breach to SLAs will be reported on the monitoring spreadsheet.
Restrictions:	Monthly Extracts listed at the time of approval of this document will be considered for this metric
IBM Owner:	Extracts & Interfaces Lead

There are 18 monthly files that are currently part of the SAM extracts:

Extract Name	Monthly	Monthly First Sunday	Monthly 15th	Monthly Last Sunday	Once per FY
Legacy CCR FOUO 4082	X	X			
Legacy CCR FOUO 40822	X	X			
Legacy CCR MPIN	X	X			
Legacy CCR Proprietary 4082	X	X			
Legacy CCR Proprietary 40822	X	X			
Legacy CCR Sensitive 4082	X	X			
Legacy CCR Sensitive 40822	X	X			
Legacy CCR Complete 4082	X	X			
Legacy CCR Complete 40822	X	X			
Legacy CCR GSA Complete	X			X	
Legacy CCR FOIA	X		X		
SAM Public (Currently NOT being posted due to D&B/GSA discussions)	X	X			
SAM FOUO	X	X			
SAM Sensitive	X	X			
SAM System-Only	X	X			
SAM MPIN	X	X			
SAM FSRS	X	X			
SAM Reps and Certs (NOT being posted until GSA testing is complete)	X	X			

1.1.23 Measure #27: Program Management - Deliverable Timeliness

Performance Requirement:	Deliverable Timeliness
Acceptable Quality Level (AQL):	**100.00%**
Data Source:	Stakeholder manual identification
How It Is Measured:	Percentage of deliverables and scheduled items available and accepted on schedule.
IBM's Approach for Achieving:	Program deliverables are listed in the deliverables tracking spreadsheet within the Connections website. The IBM team will follow the policies documented within the QCP to address the accuracy and timeliness of deliverables.
Data Accessibility:	GSA to acknowledge receipt of deliverables on the same day. Deliverables are posted on the Connections website that can be accessed by anyone with an approved account.
Restriction:	None
IBM Owner:	PMO Lead

Any missed deliverable in a month will result in a failure of this metric.

1.1.24 Measure #28: Program Management - Risk Management

Performance Requirement:	Risk Management
Acceptable Quality Level (AQL):	**There are no unmitigated or unaccepted High-level risks to the program**
Data Source:	Stakeholder manual identification
How It Is Measured:	Risks identified in the monthly risk log delivered within the Monthly Steward Report will have a mitigation strategy for all items marked as high.
IBM's Approach for Achieving:	Items are added to the risk log as issues / risks arise. The team conducts monthly risk reviews and updates the risk log. Only current known risks that are documented for consideration of mitigation will be counted within this metric.
Data Accessibility:	GSA and IBM to meet at least quarterly to review current risk log which is also delivered in the monthly Steward Report.
Restriction:	None
IBM Owner:	PMO Lead

1.1.25 Measure #29: Release Quality - Defects Per Release

Performance Requirement:	Defects Per Release
Acceptable Quality Level (AQL):	**Less than 5 Serious defects per 100 RTC Items**
Data Source:	Rational Team Concert
How It Is Measured:	Less than 5 Serious software defects as a result of the production deployment. (1 Serious defect for every 20 RTC delivered items)
IBM's Approach for Achieving:	Items that can be traced to a requirement such as Defect, Enhancement and O&M make up the RTC count. 5 Serious defects identified within 30 days after the release.
Data Accessibility:	All defects are maintained in the Rational Team Concert (RTC) tool. Items are marked for delivery in the due date field and may be tracked to completion. Once an item is successfully implemented in production, it is closed.
Restrictions	None
IBM Owner:	Program Manager

Pass Example: A release contained 120 items. 5 serious defects were opened in the first 30 days after the release.

Fail Example: A release contained 120 items. 6 serious defects were opened in the first 30 days

1.1.26 Measure #30: Release Quality - Production Scope

Performance Requirement:	Production Releases contain the agreed / scheduled scope
Acceptable Quality Level (AQL):	**95% of requirements scheduled have been delivered**
Data Source:	Stakeholder manual identification
How It Is Measured:	Missed functionality as indicated by the approved requirements specifications not implemented.
IBM's Approach for Achieving:	Approved system specifications added to a release scope prior to end of requirements phase. Requirements that are agreed upon will be developed and delivered to testing for validation. Per the System Engineering plan, approved requirements are designed and developed according to specification and reviewed accordingly. System testing including GAT and UAT will validate proper and complete incorporation of the requirements.
Data Accessibility:	Requirements are maintained in the Rational Team Concert (RTC) Requirements Composer tool. These requirements are linked to individual RTC numbers. Once a requirement is approved for a release, it is tracked to completion within the RTC item.
Restriction:	This is effective for quarterly releases only.
IBM Owner:	Program Manager

During the months when no release is added to production or no new requirements are implemented, the previous score will carry over to the current month.

1.1.27 Measure #31: Release Quality - Production Releases on Schedule

Performance Requirement:	Production Releases are delivered on schedule
Acceptable Quality Level (AQL):	**Delivered on schedule**
Data Source:	Stakeholder manual identification
How It Is Measured:	Release date is met as agreed upon by GSA and IBM.
IBM's Approach for Achieving:	GSA and IBM will work together to develop and work towards a quarterly release scope and plan. Once the release date is set and the items for delivery are agreed upon, the teams will have regularly scheduled meetings to discuss progress of the release. The teams will target to have the release date agreed upon at least 90 days prior to the release. Any change to a release date, due to a dependency on GSA, will not count against IBM as a missed schedule delivery.
Data Accessibility:	Release items are maintained in the Rational Team Concert (RTC) tool. Items are marked for delivery in the due date field and may be tracked to completion. Once an item is successfully implemented in production, it is closed.
Restriction:	This is effective for quarterly releases only. This measure will not be counted due to reasons beyond failure of a passing test disposition or incomplete delivery of agreed upon scope.
IBM Owner:	Program Manager

During the months when no release is added to production, the previous score will carry over to the current month.

SAM Integration Environment Software List
Checkpoint GAIA 80.30
Thales (Gemalto) - Safenet Authentication server(MFA VPN)
Microsoft Internet Information Server (VPN MFA and RDP)
Microsoft Windows Remote Desktop Gateway (Jumpbox MFA)
AWSTATS Web Analytics Software 7.3
F5 BIG-IP 14
Symantec Antivirus 14
Red Hat Linux 8
Microsoft Windows 2016 Data Center
Postfix 3
Arcserve Backup server 17
Windows SQL Server Database 2017 (arcserve, symantec)
LDAP 11
AD Windows Server 2016 Datacenter
ConnectDirect 4.2
Red Hat Linux NFS 4.0.0
Apache Web Server 2.4
JSF 2.x
Primefaces 7.x
Websphere MQ Server 8.0, ApacheMQ Artemis 2.6.3
Clover ETL 5.5 Server, Clover ETL Designer, Jboss EAP 7.2.5, OpenJDK 1.8.0
Erwin Data Modeler SE 2020 R2
PostgreSQL server v11
Active Directory Windows Server 2016 Datacenter
JBOSS-EAP-7.2.6
Splunk 8
Netsparker 5
Nessus 8
Burp suite Professional
McAfee Database Security 4
OpenJDK 1.8.0
Spring Security 5.3.2
Jquery 3.5.1
SFTP
RTP (functional testing)
Katalon Studio (functional testing)
Selenium (functional testing)
Apache JMeter (functional testing)
Hyperic 5.8.6

SAM Integration Environment Software List
Checkpoint GAIA 80.30
Thales (Gemalto) - Safenet Authentication server(MFA VPN)
Microsoft Internet Information Server (VPN MFA and RDP)
Microsoft Windows Remote Desktop Gateway (Jumpbox MFA)
AWSTATS Web Analytics Software 7.3
F5 BIG-IP 14
Symantec Antivirus 14
Red Hat Linux 8
Microsoft Windows 2016 Data Center
Postfix 3
Arcserve Backup server 17
Windows SQL Server Database 2017 (arcserve, symantec)
LDAP 11
AD Windows Server 2016 Datacenter
ConnectDirect 4.2
Red Hat Linux NFS 4.0.0
Apache Web Server 2.4
JSF 2.x
Primefaces 7.x
Websphere MQ Server 8.0, ApacheMQ Artemis 2.6.3
Clover ETL 5.5 Server, Clover ETL Designer, Jboss EAP 7.2.5, OpenJDK 1.8.0
Erwin Data Modeler SE 2020 R2
PostgreSQL server v11
Active Directory Windows Server 2016 Datacenter
JBOSS-EAP-7.2.6
Splunk 8
Netsparker 5
Nessus 8
Burp suite Professional
McAfee Database Security 4
OpenJDK 1.8.0
Spring Security 5.3.2
Jquery 3.5.1
SFTP
RTP (functional testing)
Katalon Studio (functional testing)
Selenium (functional testing)
Apache JMeter (functional testing)
Hyperic 5.8.6

Hostname	Type Server
SAMPR-DMZ-F501	Linux
SAMPR-DMZ-F502	Linux
CHECKPOINT-R80.30-FW-MEMBER A	Linux
CHECKPOINT-R80.30-FW-MEMBER B	Linux
CHECKPOINT-SMART-R80.30	Linux
SAMPRRH6PGS02	Redhat Enterprise
SAMPRRH6FLS01	Redhat Enterprise
SAMPRRH6LGM01	Redhat Enterprise
SAMPRRH6ESB01	Redhat Enterprise
SAMPRRH6ESB02	Redhat Enterprise
SAMPRRH6ESB03	Redhat Enterprise
SAMPRRH6JBA01	Redhat Enterprise
SAMPRRH6JBA02	Redhat Enterprise
SAMPRRH6JBA03	Redhat Enterprise
SAMPRRH6JBA04	Redhat Enterprise
SAMPRRH6JBA05	Redhat Enterprise
SAMPRRH6JBA06	Redhat Enterprise
SAMPRRH6JBA07	Redhat Enterprise
SAMPRRH6JBA08	Redhat Enterprise
SAMPRRH6ELS01	Redhat Enterprise
SAMPRRH6ELS02	Redhat Enterprise
SAMPRRH6ELS03	Redhat Enterprise
SAMPRRH6ELS04	Redhat Enterprise
SAMPRRH6ELS05	Redhat Enterprise
SAMPRRH6LST01	Redhat Enterprise
SAMPRRH6KC01	Redhat Enterprise
SAMPRRH6PGS01	Redhat Enterprise
SAMPRRH6ETL01	Redhat Enterprise
SAMPRRH6ETL02	Redhat Enterprise
SAMCORH6PGS01	Redhat Enterprise
SAMPRRH6SPK01	Redhat Enterprise
SAMPRRH6SMA01	Redhat Enterprise
SAMPRRH6COD01	Redhat Enterprise
SAMPRRH6FTP01	Redhat Enterprise
SAMPRRH6FTP02	Redhat Enterprise
SAMPRRH6MNT01	Redhat Enterprise
SAMPRRH6WBG01	Redhat Enterprise
SAMPRRH6WBG02	Redhat Enterprise
SAMPRRH6WBG03	Redhat Enterprise
SAMPRRH6WBA01	Redhat Enterprise
SAMPRRH6WBA02	Redhat Enterprise
SAMPRRH6WBA03	Redhat Enterprise
SAMPRRH6WBA04	Redhat Enterprise
SAMPRRH6WBA05	Redhat Enterprise
SAMPRRH6WBA06	Redhat Enterprise

SAMPRRH6WBA07	Redhat Enterprise
SAMPRRH6WBA08	Redhat Enterprise
SAMPRRH6WBATST-SAM.GOV	Redhat Enterprise
SAMPRRH6WBATST2-GW.SAM.GOV	Redhat Enterprise
SAMPRRH6MQS01	Redhat Enterprise
SAMPRRH8DIR02-COOP	Redhat Enterprise
SAMPRWINAD01	Microsoft Windows
SAMPRWINAV01	Microsoft Windows
SAMPRWINSQ01	Microsoft Windows
SAMPRWINAD02	Microsoft Windows
SAMPRWINHRD02	Microsoft Windows
SAMPRWINHRD01	Microsoft Windows
SAMPRWINSM01	Microsoft Windows
lgcyprod	Oracle DB
SAMPINRH8WBA01	Web Apache
SAMPINRH8WBA02	Web Apache
SAMPINRH8WBA03	Web Apache
SAMPINRH8WBA04	Web Apache
SAMPINRH8WBA05	Web Apache
SAMPINRH8WBA06	Web Apache
SAMPINRH8WBA07	Web Apache
SAMPINRH8WBA08	Web Apache
SAMPINRH8JBA01	JBOSS App Servers
SAMPINRH8JBA02	JBOSS App Servers
SAMPINRH8JBA03	JBOSS App Servers
SAMPINRH8JBA04	JBOSS App Servers
SAMPINRH8JBA05	JBOSS App Servers
SAMPINRH8JBA06	JBOSS App Servers
SAMPINRH8JBA07	JBOSS App Servers
SAMPINRH8JBA08	JBOSS App Servers
SAMPINRH8API01	API Servers
SAMPINRH8API02	API Servers
SAMPINRH8API03	API Servers
SAMPINRH8API04	API Servers
SAMPINRH8KNC01	Kinesis Consumer
SAMPINRH8KNP02	Kinesis Producer
SAMPINRH8PGS01	Postgres Kinesis Stream

*Some of these servers will be replaced by other instances but there will never be more than this.

Hostname	Type Server
CHECKPOINT-FW-R80.30	Linux
CHECKPOINT-SMART-R80.30	Linux
SAMNPRH8DIR01	Redhat Enterprise
SAMNPRH6RTC04	Redhat Enterprise
SAMNPRH6RTC02	Redhat Enterprise
SAMNPRH6SMA01	Redhat Enterprise
SAMNPWINAD01	Microsoft Windows
SAMNPWINAV01	Microsoft Windows
RTC (RDS)	Oracle DB
SAMNPH6LGM01	Redhat Enterprise

ID16210006 PWS Att M

IT Policy Requirements Guide

CIO-12-2018

Office of the Chief Information Officer

Table of Contents

1.0 Introduction ……2

1.1 Scope……2

1.2 Purpose……2

2.0 Contracting Life Cycle……2

2.1 Contracting Life Cycle Graphic……3

2.2 Contracting Phase Activities for COR ……3

3.0 Non-Security & Non-Privacy IT Policies……..4-10

4.0 Internal GSA Resources……..10

5.0 External GSA Resources……..10

1.0 Introduction

The U.S. General Services Administration (GSA) has implemented various federal policies for providing direction, and constituting uniform rules and accountability for governing the acquisition and usage of information technology (IT). This document identifies GSA information technology policies other than security and privacy policies and provides guidance to help GSA employees and applicable contractors fulfill them. Having one comprehensive Guide identify policies will assist the GSA workforce's understanding and implementation of policies. As policies are updated this guide will be updated.

1.1 Scope

This IT Policy Requirements Guide covers IT policies other than security and privacy because GSA CIO 09-48 IT Security Procedural Guide covers all security and privacy IT policies. As a result of the close association of IT systems and IT governance processes in some cases one may be able to detect a relationship between the listed policies and what could be referred to as explicit IT security policy. However the primary scope of this guide is on IT policies outside of security and privacy.

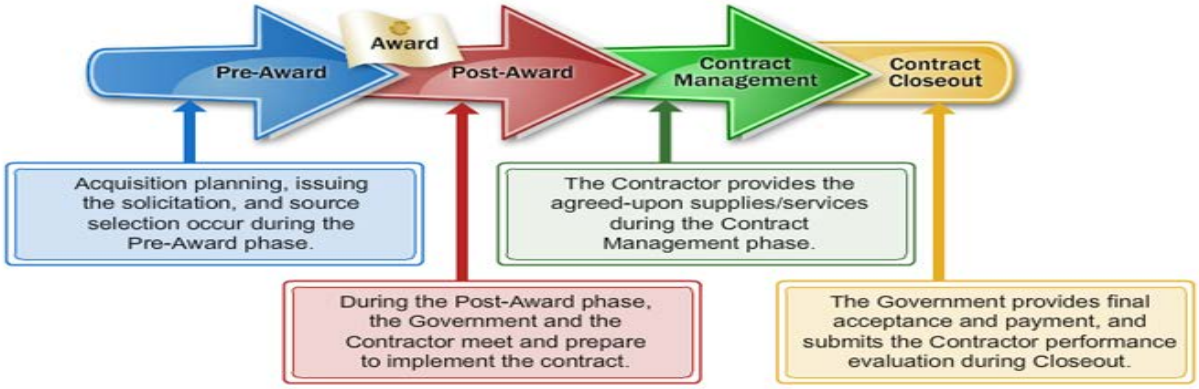
1.2 Purpose

The purpose of this Guide is to identify applicable non-security and non-privacy IT policies and provide guidance on implementing these policies. The applicability of IT policy to the contracting phases is used to help highlight critical requirements that the acquisition professional must adhere to. There is emphasis given to the Contracting Officer's Representative (COR) due to his or her unique viewpoint in contract management. In addition, this guide identifies what IT policies a contractor must comply with when this guide has been incorporated into their contract. Section 3 specifies which policies are applicable for a contractor based on the products or services being acquired in the contract.

2.0 Contracting Life Cycle

Every acquisition, and its resulting contract, follows a four phase contracting life cycle. The Contracting Officer's Representative (COR) has significant supporting involvement in each phase.

2.1 Contracting Life Cycle Graphic



Source: Graphic is from DAU University's "FCR 100 Contracting Officer Level 1" 2017 online course.

2.2 Contracting Phase Activities for COR

The following list *some* primary activities performed by the COR during the four contracting phases. The Contracting Officer (CO) has the actual authority to act as an agent for the Government and can delegate responsibilities to the COR. The COR oversees technical aspects of the contracts and performs most of the administrative functions required to ensure acceptable service or product. The CO relies on the COR to be his or her "eyes and ears" to help manage the contract.

(1.) Pre-Award • **Conducting Market Research** • **Defining Requirements** • **Support determining the Acquisition Strategy**	**(2.) Post-Award** • **Supporting creation of the Management Plan & contract kick off meeting** • **Creating of a COR Checklist** • **Maintaining a COR Contract File** • **Liaison/Communicating Concerns and Information** • **Ongoing Market Research to stay current with market conditions, technology advances, and industry trends**
(3.) Contract Administration • **Monitoring Performance/Providing technical direction** • **Managing Contract Changes** • **Inspecting and accepting supplies and/or services** • **Reviewing invoices and processing payments**	**(4.) Closeout** • **Supporting contract closeout procedures**** • **Providing contract evaluation in CPARS** • **Completing contract file** ****NOTE: Final invoice & payment, deobligation of funds, etc..**

3.0 Non-Security & Non-Privacy IT Policies

The chart below identifies which policies apply to GSA employees and the contractors. To determine if a policy applies, first check if there is a green check mark in the column with the heading, "*Who has primary responsibilities?*". If there is a checkmark for an employee or contractor, then identify if the policy must be followed based on the scope of the policy as detailed in the column with the heading, *"When does it apply?"*.

Policy	Who has primary responsibilities?		When does it apply?	Which contracting phase does it apply?
	GSA	Contractor		
CIO IL-16-03 GSA Open Source Software (OSS) Policy This Instructional Letter (IL) establishes GSA policies for OAuth 2.0 integration of GSA.gov accounts with third party services including but not limited to Websites, Software as a Service (SaaS), mobile applications, and Google Apps Scripts.	✅ See 5. Responsibilities a. b. c. d. e. f.	❌	When there is a development requirement for new or existing software, component or functionality	- Pre-Award - Contract Administration
CIO 2101.1 GSA Enterprise Information Technology Management (ITM) Policy This policy reinforces several existing IT management processes; integrates GSA IT in all implementation, procurement, workforce, and IT-related budget matters; and strengthens our partnerships across GSA.	✅ See 3. Applicability c. See 4. Responsibilities a. (1), (2), (3)(a)(b) b. (1),(2),(3),(4)	❌	When engaging with business lines, reviewing business plans, and/or conducting reviews (acquisition, budget, or post-implementation)	- Pre-Award - Contract Administration - Closeout
CIO 2102.1 Information Technology (IT) Integration Policy Establishes GSA's privacy policies and procedures, provides guidance and direction on implementing program requirements, defines privacy related contracting requirements, and assigns responsibilities to ensure compliance with the Privacy Act of 1974.	✅ See 5. Scope and applicability a. b. c.	❌	When acquiring any: 1.) new internal GSA IT solution 2.) major enhancement to existing project that has criteria of either: a.) over $150k b.) cloud acquisition c.) BPA d.) RFI & market research e.) or high-priority IT acquisitions	-Pre-Award -Post-Award -Contract Administration -Closeout

3.0 continued

Policy	Who has primary responsibilities?		When does it apply?	Which contracting phase does it apply?
	GSA	Contractor		
CIO 2104.1A CIO CHGE 1 GSA Information Technology IT General Rules of Behavior This Order sets forth the General Services Administration's (GSA's) policy on IT General Rules of Behavior.	✅ See 4. Applicability	✅ See 4. Applicability	When accessing GSA IT resources to conduct business on behalf of, or with, GSA or GSA supported Government organizations, and to all GSA IT resources which process or store GSA data, whether leased or owned.	- Contract Administration
CIO 2105.1C CHGE 1 GSA Section 508: Managing Information and Communications Technology (ICT) for Individuals with Disabilities This Order provides direction and guidance for ensuring information and communications technology allow persons with disabilities to have access to information and data that is comparable to the access of individuals without disabilities.	✅ See 5. Responsibilities a. Heads of Services and Staff Offices (HSSO) (1), (2), (3) (4)(a)(b)(c)(d) (e)(f)(g)	❌	When developing, procuring, maintaining, or using information and communications technology	- Pre-Award - Contract Administration
CIO 2105.2 P GSA Section 508 Procedures Handbook This Order issues and transmits Handbook (HB), GSA Section 508 Procedures. Section 508 prohibits Federal agencies from procuring, developing, maintaining, or using EIT that is not accessible to people with disabilities, subject to an undue burden defense. If it is properly determined by the agency that meeting the Section 508 standards would impose an undue burden, GSA must provide individuals with disabilities with information and data involved by an alternative means of access that allows the individual to use the information and data.	✅ See 3. Applicability	✅ See 3. Applicability	When developing, procuring, maintaining, or using electronic and information technology	- Pre-Award - Contract Administration

3.0 continued

Policy	Who has primary responsibilities?		When does it apply?	Which contracting phase does it apply?
	GSA	Contractor		
CIO 2108.1 Software License Management GSA is consolidating software license management and establishing a software license management program. This Order establishes software license management roles, responsibilities, and procedures.	✅ See 3. Scope and applicability a. b. c. d. See 4. Responsibilities a. (1)(2) (3) (4)(5)(6)(7) b.(1)(2)	✅ See 3. Scope and applicability a. b. c. d. See 4. Responsibilities a. (1)(2) (3) (4)(5)(6)(7) b.(1)(2)	When there is a requirement to acquire software	- Pre-Award - Contract Administration - Closeout
CIO 2110.4 GSA Enterprise Architecture Policy This Order establishes agency-wide policy, principles, roles and responsibilities for the establishment and implementation of the General Services Administration (GSA) Enterprise Architecture (EA).	✅ See 4. Applicability a. b. c. See 5. Roles and responsibilities a. b. c. d. e. f.	❌	When building EA or when there is a requirement to purchase new software	- Pre-Award - Contract Administration
CIO 2130.2 Enterprise IT Governance This policy provides direction and guidance on GSA Enterprise IT Governance (EIG). EIG is a structured decision-making framework for identifying, selecting, prioritizing, and tracking all IT investments and initiatives for the GSA enterprise. EIG integrates new business-driven approaches to investment evaluation and selection with existing agency activities and programs (e.g., Spend Tracker and legacy PBS IT governance).	✅ See 3. Applicability	❌	When EIG approval is needed	- Pre-Award

3.0 continued

Policy	Who has primary responsibilities?		When does it apply?	Which contracting phase does it apply?
	GSA	Contractor		
CIO 2135.2B GSA Information Technology (IT) Capital Planning and Investment Control This Order establishes agency-wide policies, roles and responsibilities for GSA's IT Capital Planning and Investment Control process (CPIC). CPIC is an integrated management process for the continuous selection, control, and evaluation of IT investments over their life cycles and is focused on achieving desired outcomes in support of GSA's missions, goals, and objectives.	✅ See 4. Applicability See 8. CPIC responsibilities a.b.c.d. e.(1)(2)(3)(4)(5)(6)(7) f.Program/ Project Manager 1)(2)(3)(4)(5)(6)(7)(8)	❌	When evaluating IT investments over their life cycles	- Pre-Award - Post-Award - Contract Administration - Closeout
CIO 2140.4 Information Technology (IT) Solutions Life Cycle (SLC) Policy This Order sets forth policy for planning and managing IT solutions developed for or operated by GSA. This policy has been developed to ensure the Solutions Life Cycle (SLC) discipline used is consistent with SLC guiding principles, acquisition planning requirements, and capital planning and investment control requirements. The term SLC replaces the term Software Development Life Cycle (SDLC) which was used in the past.	✅ See 5. Applicability and scope a. b. c. d. e. f.	❌	This policy applies to acquisition development, maintenance, enhancement, operation, and disposal of IT systems and solutions of any size, complexity, or significance that are part of the agency's' IT portfolio as defined in CIO 2135.2B GSA Information Technology (IT) Capital Planning and Investment Control	- Pre-Award - Post-Award - Contract Administration - Closeout
CIO 2142.1 P GSA Information and Data Quality Handbook This order issues and transmits Handbook (HB), General Services Administration (GSA) Information and Data Quality Guidelines.	✅ See 2. Applicability	❌	When acquisition will result in a new asset or data update to an existing asset	- Contract Administration

3.0 continued

Policy	Who has primary responsibilities?		When does it apply?	Which contracting phase does it apply?
	GSA	Contractor		
CIO 2141.2 General Services Administration (GSA) Web Domain Names This GSA Order sets forth GSA's internal guidance to assist organizations desiring to obtain unique website identifications. This Order provides domain name guidance for GSA staff organizations, including service, geographical, and operational areas.	✅ See 4. Coverage	❌	Applicable if an acquisition involves the need for a new domain name	- Pre-Award
CIO 2160.1F CHGE 2 GSA information Technology (IT) Standards Profile To ensure acquisition and use of standard information technologies and proper maintenance of the IT Standards Profile. The IT Standards Profile is the official GSA repository of all approved software applications. It is managed by GSA IT and can be found at ea.gsa.gov.	✅ See 2. Applicability a. b. c. d. e. See 5. Responsibilities a. b. c. d. e. f. g. See 6. Compliance a. b. (1)(2)(3)(4) c. d. (1)(2)	❌	When acquiring or using information technologies in the conduct of GSA business	- Pre-Award
CIO 2160.2B CHGE 1 GSA Electronic Messaging and Related Services This Order updates GSA's directive on electronic messaging due to the move from a server-based messaging system to cloud-based e-mail and collaboration tools and additional federal requirements for managing electronic mail records. This directive addresses security, appropriate use, and recordkeeping of the GSA Enterprise Messaging Services (GEMS) in a cloud-based environment.	✅ See 3. Applicability	✅ See 3. Applicability	All authorized users who are granted access to GEMS and to all communications sent or received via GEMS	- Pre-Award

3.0 continued

Policy	Who has primary responsibilities?		When does it apply?	Which contracting phase does it apply?
	GSA	Contractor		
CIO 2160.4A Provisioning of Information Technology (IT) Devices This Order provides direction and guidance on the deployment of computer workstations, mobile devices, and printers for agency and designated contractor personnel.	✅ See 4. Applicability a. See 5. Roles and responsibilities a.(1)(2) b.(1)(2)	✅ See 4. Applicability a.	When writing SOW. Compliance with policy should be addressed in Statements of Work (SOWs) for contractors.	- Pre-Award - Contract Administration - Closeout
CIO 2164.1 Internal Clearance Process for GSA Data Assets This Order provides the internal clearance process that the General Services Administration (GSA) must follow before releasing GSA data assets. GSA IT's Office of Enterprise Information & Data Management (IDM) established this process in collaboration with the Office of General Counsel (OGC), the Freedom of Information Act (FOIA) Division, the Privacy Officer in GSA IT, and the Executive Secretariat Division. The established clearance process ensures that the privacy, security, and confidentiality of GSA's critical data assets are protected from unauthorized access, release, and dissemination.	✅ See 4. Applicability	❌	Before releasing GSA data assets	- Contract Administration
CIO P 2165.2 GSA Telecommunications Policy This policy establishes the policy for General Services Administration (GSA) authorized users for utilization of GSA-provided telecommunications equipment, systems and services (hereafter, GSA telecommunications).	✅ See 2. Applicability	✅ See 2. Applicability	When creating any agreement (e.g. MOU) that results in that process or handle of any GSA-owned information, data, or IT system equipment	- Pre-Award

3.0 continued

Policy	Who has primary responsibilities?		When does it apply?	Which contracting phase does it apply?
	GSA	Contractor		
CIO 7000.3 Information Technology Standards for Internal GSA Workplaces This Order transmits the information technology (IT) standards for all new workplace projects, including new construction or alterations to existing space, for all GSA offices.	✅ See 5. Scope and applicability	✅ See 5. Scope and applicability	When there is a requirement to purchase IT equipment for an internal GSA workplace	- Pre-Award
CIO 9297.1 GSA Data Release Policy This Order provides GSA's policy on releasing information relating to GSA employees, contractors, and others on whom GSA maintains information described in this document.	✅ See 4. Applicability	❌	When releasing information to the public as through FOIA or other official requests and who collect, maintain, use, manage, or come in contact with personally identifiable or sensitive information owned by GSA	- Contract Administration - Contract Closeout

4.0 Internal GSA Resources

- GSA Acquisition Policy
  https://insite.gsa.gov/portal/content/510990

- GSA IT Policy Management
  https://insite.gsa.gov/portal/content/626370

- GSA IT Vendor Management
  https://insite.gsa.gov/portal/category/535534

5.0 External GSA Resources

- GSA Directives Library
  https://www.gsa.gov/directives-library

IT Security Procedural Guide:

Security and Privacy Requirements for IT Acquisition Efforts

CIO-IT Security-09-48

Revision 4

June 15, 2021

Office of the Chief Information Security Officer

IMPORTANT!

This guide defines security and privacy requirements for GSA IT acquisition contracts involving externally hosted contractor information systems that do not connect to the GSA network; information systems hosted in GSA facilities that directly connect to the GSA network; cloud information systems; or mobile applications. The security and privacy requirements are appropriately formatted to allow the respective security and privacy contract requirements to be placed in-line within a statement of work for each system type. Alternatively, this entire document can be incorporated into the statement of work or contract.

NOTE: Throughout this guide there are highlighted SELECT statements. The requirements office, in coordination with the contracting officer, will complete the selections prior to their incorporation into a contract or statement of work.

VERSION HISTORY/CHANGE RECORD

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
Revision 1 – November 6, 2009				
1	Bo Berlas	Minor Changes to GSA 800-53 R3 Control Tailoring workbook in Appendix A	GSA 800-53 Control Tailoring Workbook Update	17
Revision 2 – November 7, 2014				
1	John Sitcharing/ Blanche Heard	Minor changes to verbiage regarding Penetration Testing	Update Penetration Testing verbiage	9
2	John Sitcharing/ Blanche Heard	CISO mandated change in Penetration Testing requirement/ naming conventions based on consolidation efforts	CISO Mandate	Entire document
Revision 3 – February 2, 2017				
1	Bo Berlas	Added Essential Security controls to Section 2	Security Controls Update	9
2	Bo Berlas	Added sections 3-5	Updated to Provide Requirements for Internal Systems, Cloud Systems, and Mobile Applications	22-55
Revision 4 – June 15, 2021				
1	Bryon Feliksa/ John Klemens	Incorporated security references from MV 16-01 and additional references. Added a section on LiSaaS, Privacy controls, and updated Privacy and other sections to align with GSA policy and procedures.	Incorporate MV 16-01 and consolidate GSA Cybersecurity and Privacy Guidance.	Throughout

APPROVAL

IT Security Procedural Guide 09-48, *"Security and Privacy Requirements for IT Acquisition Efforts,"* Revision 4, is hereby approved for distribution.

X

Kurt Garbars
CISO

This guide will be available on the OCIO Webpage and GSA.gov when revised.

Table of Contents

1 Introduction....1

1.1 Scope....1
1.2 Purpose....2

2 External Information Systems – IT Security and Privacy Requirements....3

2.1 Required Policies and Regulations for GSA Contracts....3
2.2 GSA Security Compliance Requirements....4
2.3 Essential Security Controls....5
2.4 Assessment and Authorization (A&A) Activities....9
2.5 Reporting and Continuous Monitoring....11
2.6 GSA Privacy Requirements....15
2.7 Additional Stipulations....17

3 Internal Information Systems - IT Security and Privacy Requirements....19

3.1 Required Policies and Regulations for GSA Contracts....19
3.2 GSA Security Compliance Requirements....20
3.3 Essential Security Controls....21
3.4 Assessment and Authorization (A&A) Activities....26
3.5 Reporting and Continuous Monitoring....28
3.6 GSA Privacy Requirements....32
3.7 Additional Stipulations....33

4 Low Impact Software as a Service (LiSaaS) – IT Security and Privacy Requirements....36

4.1 Assessment of the System....36
4.2 Authorization of the System....37
4.3 Reporting and Continuous Monitoring....37
4.4 Protection of Information....37
4.5 Data Ownership and Unrestricted Rights to Data....37
4.6 Personally Identifiable Information....38
4.7 Data Availability....38
4.8 Data Release....38
4.9 Confidentiality and Nondisclosure....39
4.10 Section 508 Compliancy....39
4.11 Additional Stipulations....39
4.12 Terms of Service....41
4.13 References....41

5 Cloud Information Systems – IT Security and Privacy Requirements....42

5.1 Assessment and Authorization....42
5.2 Assessment of the System....42
5.3 Authorization of the System....44
5.4 Reporting and Continuous Monitoring....46
5.5 Personnel Security Requirements....47
5.6 Sensitive Information Storage....47
5.7 Protection of Information....48
5.7.1 Unrestricted Rights to Data....48

5.7.2 Personally Identifiable Information 48
5.7.3 Data Availability 48
5.7.4 Data Release 48
5.8 Data Ownership 49
5.9 Confidentiality and Nondisclosure 49
5.10 GSA Non-Disclosure Agreement 49
5.11 Additional Stipulations 50
5.12 References 52

6 Mobile Application - IT Security and Privacy Requirements 53

6.1 General Mobile Application Guidelines 53
6.2 Mobile Device Security 53
6.3 Application Sources 54
6.4 Terms of Service (ToS) 55
6.5 GSA Privacy Requirements 55
6.6 GSA App Development, Assessment, Authorization and Deployment 56
6.7 Intellectual Property 58
6.8 Confidentiality and Nondisclosure 58
6.9 GSA Non-Disclosure Agreement 59
6.10 Personnel Security Requirements 59
6.11 Additional Stipulations 60

Appendix A: GSA Tailoring of NIST 800-53 Controls 63

1 Introduction

The U.S. General Services Administration (GSA) must provide information security for the information systems that support the operations and assets of the agency, including those provided or managed by GSA, another agency, contractor, or other source. The Federal Information Security Modernization Act of 2014 (FISMA of 2014) describes Federal agency security and privacy responsibilities as including "information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency." This includes services which are either fully or partially provided; including other agency hosted, outsourced, and cloud computing solutions. Agency information security programs apply to all organizations (sources) which possess or use Federal information – or which operate, use, or have access to Federal information systems (whether automated or manual) – on behalf of a Federal agency, information systems used or operated by an agency or other organization on behalf of an agency.

Office of Management and Budget (OMB) Memorandum M-14-04 asserts that agencies are responsible for ensuring information technology acquisitions comply with the information technology security requirements in FISMA of 2014, OMB's implementing policies including OMB Circular A-130 and guidance and standards from the National Institute of Standards and Technology (NIST).

1.1 Scope

This guide provides security and privacy requirements for the GSA information system types outlined below:

- **External Information Systems.** External information systems reside in contractor facilities and typically do not connect to the GSA network. External information systems may be government owned and contractor operated or contractor owned and operated on behalf of GSA or the Federal Government (when GSA is the managing agency).
- **Internal Information Systems.** Internal information systems reside on premise in GSA facilities AND directly connect to the GSA network. Internal systems are operated on behalf of GSA or the Federal Government (when GSA is the managing agency).
- **Low Impact Software as a Service (LiSaaS) Systems.** LiSaaS systems must adhere to GSA IT Security Procedural Guide 17-75, "*Security Reviews for Low Impact Software as a Service (SaaS) Solutions*." LiSaaS systems are cloud applications that are implemented for a limited duration, considered low impact and would cause limited harm to GSA, and cost less than $100,000 to deploy.
- **Cloud Information Systems**. Includes Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or SaaS. Requires FedRAMP.
- **Mobile Application.** A mobile application, most commonly referred to as an app, is a type of application software designed to run on a mobile device, such as a smartphone or tablet computer.

1.2 Purpose

The purpose of this document is to define and establish consistent security and privacy requirements for GSA IT acquisition contracts involving externally hosted information systems that do not connect to the GSA network; information systems hosted in GSA facilities that directly connect to the GSA network; LiSaaS systems, cloud information systems; or mobile applications. The security and privacy requirements are appropriately formatted to allow the respective security and privacy contract language to be placed in-line within a statement of work for each system type. The security and privacy requirements identified in this guide will ensure compliance with the appropriate provisions of FISMA of 2014, OMB Circular A-130, and NIST Special Publication (SP) 800-53, Revision 4.

2 External Information Systems – IT Security and Privacy Requirements

2.1 Required Policies and Regulations for GSA Contracts

Federal Laws and Regulations:

The contractor shall comply with all applicable Federal Laws and Regulations.

- 40 U.S.C. 11331, "*Responsibilities for Federal Information Systems Standards*"
- FISMA of 2014, "*The Federal Information Security Modernization Act of 2014*"
- HSPD 12, "*Homeland Security Presidential Directive 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*"
- OMB Circular No. A-130, "*Managing Information as a Strategic Resource*"
- OMB M-08-23, "*Securing the Federal Government's Domain Name System Infrastructure (Submission of Draft Agency Plans Due by September 5, 2008)*"
- OMB M 14-03, "*Enhancing the Security of Federal Information and Information Systems*"
- OMB M-10-23, "*Guidance for Agency Use of Third-Party Websites and Applications*"
- OMB M-15-13, "*Policy to Require Secure Connections across Federal Websites and Web Services*"
- OMB M-17-12, "*Preparing for and Responding to a Breach of Personally Identifiable Information*"
- Privacy Act of 1974, "*5 USC, § 552a*"
- OMB Memoranda, location of current fiscal year guidance on Federal Information Security and Privacy Management Requirements, including FISMA reporting

Federal Standards and Guidance:

The contractor shall comply with all applicable Federal Information Processing Standards (FIPS). NIST Special Publications (800 Series) are guidance, unless required by a FIPS publication, in which case usage is mandatory.

- FIPS PUB 199, "*Standards for Security Categorization of Federal Information and Information Systems*"
- FIPS PUB 200, "*Minimum Security Requirements for Federal Information and Information Systems*"
- FIPS PUB 140-2, "*Security Requirements for Cryptographic Modules*"
- NIST SP 800-18, Revision 1, "*Guide for Developing Security Plans for Federal Information Systems*"
- NIST SP 800-30, Revision 1, "*Guide for Conducting Risk Assessments*"
- NIST SP 800-34, Revision 1, "*Contingency Planning Guide for Federal Information Systems*"
- NIST SP 800-37, Revision 1, "*Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Lifecycle Approach*"
- NIST SP 800-47, "*Security Guide for Interconnecting Information Technology Systems*"
- NIST SP 800-53, Revision 4, "*Security and Privacy Controls for Federal Information Systems and Organizations*"

- NIST SP 800-53A, Revision 4, *"Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*"
- NIST SP 800-63-3, "*Digital Identity Guidelines*"
- NIST SP 800-122, "*Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*"
- NIST SP 800-137, "*Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*"

GSA Policies:

The contractor shall comply with the following GSA Directives/Policies.

- GSA Order CIO 1878.1, "*GSA Privacy Act Program*"
- GSA Order CIO 1878.2, "*Conducting Privacy Impact Assessments (PIAs) in GSA*"
- GSA Order CIO 2100.1, "*GSA Information Technology (IT) Security Policy*"
- GSA Order CIO 9297.2, "*GSA Information Breach Notification Policy*"

The GSA policies listed in this paragraph must be followed, if applicable.

- GSA Order CIO 2103.1, "*Controlled Unclassified Information (CUI) Policy*"
- GSA Order CIO 2104.1, "*GSA Information Technology (IT) General Rules of Behavior*"
- GSA Order CIO 2182.2, "*Mandatory Use of Personal Identity Verification (PIV) Credentials*"

GSA Procedural Guides:

GSA IT Procedural Guides are guidance, unless required by a GSA Directive/Policy, in which case usage is mandatory.

Note: GSA's Procedural Guides are updated frequently; to make sure you have the most recent version of publicly available procedural guides, visit GSA.gov. If a non-publicly available guide is needed, contact the contracting officer who will coordinate with the GSA Office of the Chief Information Security Officer to determine if it can be made available.

2.2 GSA Security Compliance Requirements

FIPS PUB 200, *"Minimum Security Requirements for Federal Information and Information Systems*," is a mandatory federal standard that defines the minimum security requirements for federal information and information systems in seventeen security-related areas. Information systems supporting GSA must meet the minimum security and privacy requirements through the use of security controls in accordance with NIST Special Publication 800-53, Revision 4 (hereafter described as NIST 800-53), *"Security and Privacy Controls for Federal Information Systems and Organizations."*

To comply with the Federal standard, GSA must determine the security category of the information and information system in accordance with FIPS PUB 199, *"Standards for Security Categorization of Federal Information and Information Systems,"* and then the contractor shall

apply the appropriately tailored set of Low, Moderate, or High impact baseline security controls in NIST 800-53, as determined by GSA. NIST 800-53 controls requiring organization-defined parameters (i.e., password change frequency) shall be consistent with GSA specifications. The GSA-specified control parameters and supplemental guidance defining more specifically the requirements per FIPS PUB 199 impact level are available in the GSA Control Tailoring Workbook referenced in Appendix A of this document.

The Contractor shall use GSA technical guidelines, NIST guidelines, Center for Internet Security (CIS) guidelines (Level 1), or industry best practice guidelines in hardening their systems.

2.3 Essential Security Controls

All NIST 800-53 controls must be implemented as per the applicable FIPS PUB 199 Low, Moderate, or High baseline. The following table identifies essential security controls from the respective baselines to highlight their importance and ensure they are implemented. The Contractor shall make the proposed system and security architecture of the information system available to the Security Engineering Division, in the Office of the Chief Information Security Officer for review and approval before commencement of system build (architecture, infrastructure, and code).

Control ID	Control Title	Baseline	GSA Implementation Guidance
AC-2	Account Management	L, M, H	
AC-17 (3)	Remote Access | Managed Access Control Points	M, H	All remote accesses from internal users/systems to the external information system must be routed through GSA's managed network access control points, subjecting them to security monitoring.
AU-2	Audit Events	L, M, H	Information systems shall implement audit configuration requirements as documented in applicable GSA IT Security Technical Hardening Guides (i.e., hardening and technology implementation guides); for web applications see GSA IT Security Procedural Guide 07-35, Section 2.8.10, What to Log. For technologies where a Technical Guide and Standard does not exist, events from an industry source such as vendor guidance or Center for Internet Security benchmark, recommended by the GSA S/SO or Contractor to be approved and accepted by the GSA AO shall be used.
CM-6	Configuration Settings	L, M, H	Information systems, including vendor owned/operated systems on behalf of GSA, shall configure their systems in agreement with GSA technical guidelines, NIST guidelines, Center for Internet Security guidelines (Level 1), or industry best practice guidelines, as deemed appropriate.

Control ID	Control Title	Baseline	GSA Implementation Guidance
CP-7	Alternative Processing Site	M, H	FIPS PUB 199 Moderate and High impact systems must implement processing across geographically-disparate locations to ensure fault tolerance. Amazon Web Services based architectures must implement a multi-region strategy (multiple availability zones in a single region are not sufficient).
CP-8	Telecom Services	M, H	FIP PUB 199 Moderate and High impact information systems must implement alternate telecom services to support resumption when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.
IA-2 (1)	Identification and Authentication (Organizational Users) | Network Access to Privileged Accounts	L, M, H	All information systems shall implement multi-factor authentication for privileged accounts.
IA-2 (2)	Identification and Authentication (Organizational Users) | Network Access to Non-Privileged Accounts	M, H	FIPS PUB 199 Moderate and High impact information systems must implement multi-factor authentication for non-privileged accounts.
IA-7	Cryptographic Module Authentication	L, M, H	The information system shall implement FIPS PUB 140-2 compliant encryption modules for authentication functions. Reference: https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules
MP-4	Media Storage	M, H	Digital media including magnetic tapes, external/removable hard drives, flash/thumb drives, diskettes, compact disks and digital video disks shall be encrypted using a FIPS PUB 140-2 certified encryption module.
MP-5	Media Transport	M, H	Digital media including magnetic tapes, external/removable hard drives, flash/thumb drives and digital video disks shall be encrypted using a FIPS PUB 140-2 certified encryption module during transport outside of controlled areas.

Control ID	Control Title	Baseline	GSA Implementation Guidance
PL-8	Information Security Architecture	M, H	All information system security architectures must be formally reviewed and approved by the Office of the Chief Information Security Officer, Security Engineering Division during the system develop/design stages of the SDLC and prior to Security Assessment and Authorization.
RA-5	Vulnerability Scanning	L, M, H	All systems must complete weekly operating system (OS) and monthly web application vulnerability scans. The most recent vulnerability scanning results shall be provided to GSA together with the quarterly POA&M submission.
SA-22	Unsupported System Components	GSA Required	All systems must be comprised of software and hardware components that are fully supported in terms of security patching for the anticipated life of the system; software must be on GSA's Enterprise Architecture IT Standards List.
SC-8 / SC-8(1)	Transmission Confidentiality and Integrity / Transmission Confidentiality and Integrity | Cryptographic or Alternate Physical Protection	M, H	Implemented encryption algorithms and cryptographic modules shall be FIPS-approved and FIPS PUB 140-2 validated, respectively. ○ Digital signature encryption algorithms - Reference: https://csrc.nist.gov/Projects/Cryptographic-Algorithm-Validation-Program/Validation/Validation-List/DSA ○ Block cypher encryption algorithms - Reference: https://csrc.nist.gov/Projects/Cryptographic-Algorithm-Validation-Program/Block-Ciphers ○ Secure hashing algorithms – Reference: https://csrc.nist.gov/Projects/Cryptographic-Algorithm-Validation-Program/Secure-Hashing Internet accessible Websites shall implement HTTPS Only and HTTP Strict Transport Security (HSTS), reference OMB Memorandum M-15-13. SSL/TLS implementations shall align with GSA IT Security Procedural Guide 14-69, *"SSL/TLS Implementation."*
SC-13	Cryptographic Protection	L, M, H	Implemented encryption algorithms and cryptographic modules shall be FIPS-approved and FIPS PUB 140-2 validated, respectively. ○ Digital signature encryption algorithms - Reference: https://csrc.nist.gov/Projects/Cryptographic-Algorithm-Validation-Program/Validation/Validation-List/DSA ○ Block cypher encryption algorithms - Reference: https://csrc.nist.gov/Projects/Cryptographic-Algorithm-Validation-Program/Block-Ciphers ○ Secure hashing algorithms – Reference: https://csrc.nist.gov/Projects/Cryptographic-Algorithm-Validation-Program/Secure-Hashing

Control ID	Control Title	Baseline	GSA Implementation Guidance
SC-17	PKI Certificates	M, H	Implement appropriate creation, use, and signing of crypto certs in agreement with GSA IT Security Procedural Guide 14-69, *"SSL/TLS Implementation,"* and NIST Special Publications 800-32, NIST 800-63.
SC-18	Mobile Code	M, H	
SC-22	Architecture and Provisioning for Name / Address Resolution Service	L, M, H	Information systems shall be Domain Name System Security Extensions (DNSSEC) compliant. Reference OMB Memorandum M-08-23, which requires all Federal Government departments and agencies that have registered and are operating second level .gov to be DNSSEC.
SC-28 (1)	Protection of Information at Rest | Cryptographic Protection	GSA Required – For systems with Personally Identifiable Information Only	Systems bearing PII must implement protect information at rest. At a minimum, fields bearing PII data must be encrypted with field level encryption. Encryption algorithms shall be FIPS-approved; implemented encryption modules shall be FIPS PUB 140-2 validated.
SI-2	Flaw Remediation	L, M, H	All projects and systems must be adequately tested for flaws; all Critical, High, and Moderate risk findings must be remediated prior to go-live. Post go-live, all critical and high vulnerabilities identified must be mitigated within 30 days and all moderate vulnerabilities mitigated within 90 days.
SI-3	Malicious Code Protection	L, M, H	
SI-4	Information System Monitoring	L, M, H	
SI-10	Information Input Validation	M, H	All system accepting input from end users must validate the input in accordance to industry best practices and published guidelines, including GSA IT Security Procedural Guide 07-35, *"Web Application Security,"* and OWASP Top 10 Web Application Security Vulnerabilities.
AR-2	Privacy Impact and Risk Assessment	See note below	The contractor shall conduct a Privacy Threshold Analysis (PTA) and, if applicable, a Privacy Impact Assessment (PIA) identifying the categories of information and addressing potential risks to PII. The contractor also shall coordinate with the GSA Privacy Office concerning these documents.
AR-8	Accounting of Disclosures	See note below	The contractor shall keep an accurate accounting of disclosures of information held in any system of records under its control.

Control ID	Control Title	Baseline	GSA Implementation Guidance
TR-2	System of Records Notices and Privacy Act Statements	See note below.	The contractor shall coordinate with the GSA Privacy Office to ensure System of Records Notices (SORNs) and Privacy Act notices on forms that collect Personally Identifiable Information (PII) are established and kept current.
UL-1	Internal Use	See note below	The contractor shall ensure that PII is shared internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices.
UL-2	Information Sharing with Third Parties	See note below	The contractor shall coordinate with the GSA Privacy Office to ensure PII is shared in accordance with GSA requirements and agreements with third parties.

Note: Privacy controls are not associated with a baseline. Controls are applicable/not applicable based on PII data being collected, stored, or transmitted.

2.4 Assessment and Authorization (A&A) Activities

The implementation of a new Federal Government IT system requires a formal approval process known as Assessment and Authorization (A&A). NIST Special Publication 800-37, Revision 1 (hereafter described as NIST 800-37) and GSA IT Security Procedural Guide 06-30, "*Managing Enterprise Risk,*" provide guidelines for performing the A&A process. The Contractor system/application must have a valid assessment and authorization, known as an Authority to Operate (ATO) (signed by the Federal government) before going into operation and processing GSA information. The failure to obtain and maintain a valid ATO will result in the termination of the contract. The system must have a new A&A conducted (signed by the Federal government) at least every three (3) years or at the discretion of the Authorizing Official when there is a significant change to the system's security posture or via continuous monitoring based on GSA CIO IT Security 12-66, "*Information Security Continuous Monitoring Strategy*" that is reviewed and accepted by the GSA CISO.

Assessing the System

1. The Contractor shall comply with Assessment and Authorization (A&A) requirements as mandated by Federal laws and policies, including making available any documentation, physical access, and logical access needed to support this requirement. The Level of Effort for the A&A is based on the System's NIST Federal Information Processing Standard (FIPS) Publication 199 categorization. The contractor shall create, maintain and update the following A&A documentation:

    - System Security Plan (SSP) completed in agreement with NIST Special Publication 800-18, Revision 1, *"Guide for Developing Security Plans for Federal Information Systems."* The SSP shall include as appendices required policies and procedures across 17 control families mandated per FIPS PUB 200, Rules of Behavior, and Interconnection Agreements (in agreement with NIST Special Publication 800-47,

"Security Guide for Interconnecting Information Technology Systems"). The SSP shall include; as an appendix, a completed GSA Control Tailoring Workbook identified in Appendix A of this guide. The column in the workbook titled "GSA Defined Values," shall be used to document all contractor implemented settings that are different from the GSA defined setting and where the GSA defined setting allows a contractor determined setting.

- Contingency Plan (including Disaster Recovery Plan) completed in agreement with NIST Special Publication 800-34.
- Contingency Plan Test Report completed in agreement with GSA IT Security Procedural Guide 06-29, *"Contingency Planning."*
- Incident Response Plan completed in agreement with NIST Special Publication 800-61, "Computer Security Incident Handling Guide" and GSA IT Security Procedural Guide 01-02, "*Incident Response*."
- Incident Response Test Report completed in agreement NIST Special Publication 800-61, "Computer Security Incident Handling Guide" and GSA IT Security Procedural Guide 01-02, "*Incident Response*."
- Configuration Management Plan completed in agreement with GSA IT Security Procedural Guide 01-05, "*Configuration Management*."
- Plan of Actions & Milestones completed in agreement with GSA IT Security Procedural Guide 09-44, *"Plan of Action and Milestones (POA&M)."*
- Penetration Test Reports documenting the results of vulnerability analysis and exploitability of identified vulnerabilities. Note: Penetration testing is required for all FIPS PUB 199 Low impact and Moderate impact Internet accessible information systems, and all FIPS PUB 199 High impact information systems are required to complete an independent penetration test and provide an Independent Penetration Test Report documenting the results of the exercise as part of the A&A package. Reference GSA IT Security Procedural Guide 06-30, *"Managing Enterprise Risk"* and GSA IT Security Procedural Guide 11-51, *"Conducting Penetration Test Exercises"* for penetration testing guidance.

2. Information systems must be assessed and authorized every three (3) years or whenever there is a significant change to the system's security posture in accordance with NIST Special Publication 800-37, Revision 1, *"Guide for the Security Certification and Accreditation of Federal Information Systems,"* and CIO IT Security 06-30, "*Managing Enterprise Risk*" or via continuous monitoring based on GSA CIO IT Security 12-66, "*Information Security Continuous Monitoring Strategy*" that is reviewed and accepted by the GSA CISO.

3. At the Moderate impact level and higher, the **<SELECT: contractor or Government>** is responsible for providing an independent Security Assessment/Risk Assessment in accordance with GSA IT Security Procedural Guide 06-30, *"Managing Enterprise Risk."*

4. If the Government is responsible for providing a Security Assessment/Risk Assessment and Penetration Test, the Contractor shall allow GSA employees (or GSA designated third party contractors) to conduct A&A activities to include control reviews in

accordance with NIST 800-53/NIST 800-53A and GSA IT Security Procedural Guide 06-30, *"Managing Enterprise Risk."* Review activities include but are not limited to operating system vulnerability scanning, web application scanning, and database scanning of applicable systems that support the processing, transportation, storage, or security of GSA information. This includes the general support system infrastructure.

5. Identified gaps between required NIST 800-53 controls and the contractor's implementation as documented in the Security Assessment/Risk Assessment report shall be tracked for mitigation in a Plan of Action and Milestones (POA&M) document completed in accordance with GSA IT Security Procedural Guide 09-44, *"Plan of Action and Milestones (POA&M)."* Depending on the severity of the gaps, the Government may require them to be remediated before an Authorization to Operate is issued.
6. The Contractor is responsible for mitigating all security risks found during the A&A and continuous monitoring activities. All high-risk vulnerabilities must be mitigated within 30 days and all moderate risk vulnerabilities must be mitigated within 90 days from the date vulnerabilities are formally identified. The Government will determine the risk rating of vulnerabilities.

Authorization of the System

1. Upon receipt of the documentation (Security Authorization Package (SAP)) described in GSA IT Security Procedural Guide 06-30, *"Managing Enterprise Risk"* and NIST Special Publication 800-37 as documented above, the GSA Authorizing Official (AO) for the system (in coordination with the GSA Chief Information Security Officer (CISO), system Program Manager (PM), Information System Security Manager (ISSM), and Information System Security Officer (ISSO) will render an authorization decision to:
    - Authorize system operation w/out any restrictions or limitations on its operation;
    - Authorize system operation w/restriction or limitation on its operation, or;
    - Not authorize for operation.
2. The Contractor shall provide access to the Federal Government, or their designee acting as their agent, when requested, in order to verify compliance with the requirements for an Information Technology security program. At its option, the Government may choose to conduct on site surveys. The Contractor shall make appropriate personnel available for interviews and documentation during this review. If documentation is considered proprietary or sensitive, these documents may be reviewed on-site under the hosting Contractor's supervision.

2.5 Reporting and Continuous Monitoring

Maintenance of the security authorization to operate will be through continuous monitoring of security controls of the external system and its environment of operation to determine if the security controls in the information system continue to be effective over time in light of changes that occur in the system and environment. Through continuous monitoring, security

controls and supporting deliverables are updated and submitted to GSA per the schedules below. The submitted deliverables (or lack thereof) provide a current understanding of the security state and risk posture of the information systems. They allow GSA AOs to make credible risk-based decisions regarding the continued operations of the information systems and initiate appropriate responses as needed when changes occur.

Deliverables to be provided to the GSA COR/ISSO/ISSM Quarterly

1. Vulnerability Scanning
   Reference: NIST 800-53 control RA-5
   Provide the most recent Web Application and Operating System vulnerability scan reports.

2. Plan of Action & Milestones (POA&M) Update
   Reference: NIST 800-53 control CA-5
   Provide POA&M updates in accordance with requirements and the schedule set forth in GSA CIO IT Security Procedural Guide 09-44, "*Plan of Action and Milestones (POA&M).*"

Deliverables to be provided to the GSA COR/ISSO/ISSM Annually

1. Updated A&A documentation including the System Security Plan and Contingency Plan
   a. System Security Plan
      Reference: NIST 800-53 control PL-2
      Review and update the System Security Plan annually to ensure the plan is current and accurately describes implemented system controls and reflects changes to the contractor system and its environment of operation. The System Security Plan must be in accordance with NIST 800-18, Revision 1, *"Guide for Developing Security Plans."*
   b. Contingency Plan
      Reference: NIST 800-53 control CP-2
      Provide an annual update to the contingency plan completed in accordance with NIST 800-34, *"Contingency Planning Guide."*

2. User Certification/Authorization Review Documents
   Reference: NIST 800-53 control AC-2
   Provide the results of the annual review and validation of system users' accounts to ensure the continued need for system access. The user certification and authorization documents will illustrate the organization establishes, activates, modifies, reviews, disables, and removes information system accounts in accordance with documented account management procedures.

3. Separation of Duties Matrix
   Reference: NIST 800-53 control AC-5

Develop and furnish a separation of duties matrix reflecting proper segregation of duties for IT system maintenance, management, and development processes. The separation of duties matrix will be updated or reviewed on an annual basis.

4. Information Security Awareness and Training Records
   Reference: NIST 800-53 control AT-4
   Provide the results of security awareness (AT-2) and role-based information security technical training (AT-3). AT-2 requires basic security awareness training for employees and contractors that support the operation of the contractor system. AT-3 requires information security technical training to information system security roles. Training shall be consistent with the requirements contained in C.F.R. Part 5 Subpart C (5 C.F.R 930.301) and conducted at least annually.

5. Annual FISMA Self-Assessment
   Reference: NIST 800-53 control CA-2
   Deliver the results of the annual FISMA self-assessment conducted per GSA IT Security Procedural Guide 04-26, "*Federal Information Security Modernization Act (FISMA) Implementation."* Based on the controls selected for self-assessment, the GSA OCISO will provide the appropriate test cases for completion.

6. System(s) Baseline Configuration Standard Document
   Reference: NIST 800-53 control CM-2/CM-2(1)
   Provide a well-defined, documented, and up-to-date specification to which the information system is built.

7. System Configuration Settings Verification
   Reference: NIST 800-53 control CM-6/CM-6(1)
   Establish and document mandatory configuration settings for information technology products employed within the information system that reflect the most restrictive mode consistent with operational requirements. Configuration settings are the configurable security-related parameters of information technology products that compose the information system. Systems should be configured in agreement with GSA technical guidelines, NIST guidelines, Center for Internet Security guidelines (Level 1), or industry best practice guidelines in hardening their systems, as deemed appropriate by the Authorizing Official.

   Provide the most recent operating system Configuration Settings Compliance scan report.

8. Configuration Management Plan
   Reference: NIST 800-53 control CM-9
   Provide an annual update to the Configuration Management Plan for the information system.

9. Contingency Plan Test Report
   Reference: NIST 800-53 control CP-4
   Provide a contingency plan test report completed in accordance with GSA IT Security Procedural Guide 06-29, *"Contingency Planning."* A continuity test shall be

conducted annually prior to mid-July of each year. The continuity test can be a table top test while the system is at the FIPS PUB 199 Low Impact level. The table top test must include Federal and hosting Contractor representatives. Functional exercises must be completed once every three years for FIPS PUB 199 Moderate impact systems and annually for FIPS PUB 199 High impact systems.

10. Incident Response Test Report
    Reference: NIST 800-53 control IR-3
    Provide an incident response plan test report documenting results of incident reporting process per GSA IT Security Procedural Guide 01-02, *"Incident Response."*

11. Information System Interconnection Agreements
    Reference: NIST 800-53 control CA-3
    Provide Interconnection Security Agreements (ISA) and supporting Memoranda of Agreement/Understanding (MOA/U), completed in accordance with NIST 800-47, *"Security Guide for Connecting Information Technology Systems,"* for existing and new interconnections. Per NIST 800-47, an interconnection is the direct connection of two or more IT systems for the purpose of sharing data and other information resources through a pipe, such as ISDN, T1, T3, DS3, VPN, etc. ISAs shall be submitted as appendices as part of the annual System Security Plan submission. ISAs shall include, if applicable, any changes since the last submission; updated ISAs are required at least every three years.

12. Rules of Behavior
    Reference: NIST 800-53 control PL-4
    Define and establish Rules of Behavior for information system users. Rules of Behavior shall be submitted as an appendix to the System Security Plan.

13. Penetration Testing Report
    Reference: NIST 800-53 control CA-8
    All Internet accessible systems, and all FIPS PUB 199 High impact systems are required to complete an independent penetration test and provide a Penetration Test Report documenting the results of the exercise as part of their A&A package. Annual penetration tests are required for these same systems in accordance with GSA Order CIO 2100.1 and CIO-IT Security-11-51, "*Conducting Penetration Test Exercises.*"

14. Personnel Screening and Security
    Reference: NIST 800-53 control PS-3, NIST 800-53 control PS-7
    Furnish documentation reflecting favorable adjudication of background investigations for all personnel (including subcontractors) supporting the system. Contractors shall comply with GSA Order CIO 2100.1, *"GSA Information Technology (IT) Security Policy"* and GSA Order, CIO P 2181.1, "*Homeland Security Presidential Directive-12 (HSPD-12) Personal Identity Verification and Credentialing Handbook*." GSA separates the risk levels for personnel working on Federal computer systems into three categories: Low Risk, Moderate Risk, and High Risk.

- Those contract personnel (hereafter known as "Applicant") determined to be in a Low Risk position will require a National Agency Check with Written Inquiries (NACI) investigation.
- Those Applicants determined to be in a Moderate Risk position will require either a Limited Background Investigation (LBI) or a Minimum Background Investigation (MBI) based on the Contracting Officer's (CO) determination.
- Those Applicants determined to be in a High Risk position will require a Background Investigation (BI).

Applicants will not be reinvestigated if a prior favorable adjudication is on file with FPS or GSA, there has been less than a one year break in service, and the position is identified at the same or lower risk level.

Once a favorable FBI Criminal History Check (Fingerprint Check) has been returned, Applicants may receive a GSA identity credential (if required) and initial access to GSA information systems. The HSPD-12 Handbook contains procedures for obtaining identity credentials and access to GSA information systems as well as procedures to be followed in case of unfavorable adjudications.

Deliverables to be provided to the GSA COR/ISSO/ISSM Biennially

1. Policies and Procedures
   Develop and maintain current the following policies and procedures:
   a. Access Control Policy and Procedures (NIST 800-53 AC-1)
   b. Security Awareness and Training Policy and Procedures (NIST 800-53 AT-1)
   c. Audit and Accountability Policy and Procedures (NIST 800-53 AU-1)
   d. Identification and Authentication Policy and Procedures (NIST 800-53 IA-1)
   e. Incident Response Policy and Procedures (NIST 800-53 IR-1, reporting timeframes are documented in GSA IT Security Procedural Guide 01-02, "*Incident Response*"
   f. System Maintenance Policy and Procedures (NIST 800-53 MA-1)
   g. Media Protection Policy and Procedures (NIST 800-53 MP-1)
   h. Physical and Environmental Policy and Procedures (NIST 800-53 PE-1)
   i. Personnel Security Policy and Procedures (NIST 800-53 PS-1)
   j. System and Information Integrity Policy and Procedures (NIST 800-53 SI-1)
   k. System and Communication Protection Policy and Procedures (NIST 800-53 SC-1)
   l. Key Management Policy (NIST 800-53 SC-12)

2.6 GSA Privacy Requirements

Personally identifiable information (PII) **<SELECT: is or is not>** in the scope of the acquisition and PII **<SELECT: is or is not>** expected to be stored, processed, or transmitted in the vendor's information system. The collection, maintenance or dissemination of any PII that is subject to the Privacy Act and/or the E-Government Act will be handled in full accordance with all GSA rules of conduct and in accordance with GSA Privacy Program requirements.

The contractor shall prepare a Privacy Threshold Analysis (PTA) to confirm and document PII is not in scope, or to determine which categories of information will be stored, processed, or transmitted by the system. The PTA must be completed before development begins and whenever a change with a privacy impact (e.g., a new category of information is collected) is made to an existing system. PTAs are required as part of GSA's process to determine whether a Privacy Impact Assessment (PIA) and/or a System of Records Notice (SORN) is required, and if any other privacy requirements apply to the information system. Instructions for the PTA and PIA forms can be found at https://www.gsa.gov/reference/gsa-privacy-program/privacy-impact-assessments-pia.

PII (should it come into scope) will require the following guidelines be adhered to.

- The vendor's information system must be authorized at least at the FIPS PUB 199 Moderate level.
- For any system that collects, maintains or disseminates PII, a PIA must be completed by the contractor and provided to the GSA Privacy Office for review along with the other authorization to operate (ATO) documents.
- If the system retrieves information using PII, the Privacy Act applies and it must have a system of records notice (SORN) published in the Federal Register.
- If PII is collected from individuals by the system, a Privacy Act Statement (i.e., Privacy Notice) must be provided to users prior to their use of the application on what data is being collected and why, as well as the authority for the collection and the impact of not providing some or all of it. The Privacy Act Statement must be available to the individual directly on the form used to collect the information. Providing a link back to the Statement from the form is acceptable.

Provided below is a template for an acceptable Privacy Act Statement, when bracketed sections are completed. A completed example is available at https://www.gsa.gov/reference/gsa-privacy-program/privacy-act-statement-for-design-research.

Privacy Act Statement

This (insert voluntary or mandatory) collection of personal information in authorized by (insert legal authority). We collect (developer insert categories of PII collected, e.g., name, email, etc.). Your personal information is collected so we can (developer insert purpose of collection and what effect on the individual, if any, not providing any or all of the information may have). Your personal information is stored in (developer insert GSA system name). GSA may use this information pursuant to its published Privacy Act system of records notice (insert link to applicable GSA Privacy Act SORN).

Note: Systems that access data a user creates must assume a user may include privacy data/PII in the system unless the data creation is restricted to data controlled by the system.

All contractor staff who have significant privacy information responsibilities must complete GSA's specialized Privacy 201 Training. This includes contractors who work with PII as part of their work duties (e.g.; Human Resource staff, Finance staff, and managers/supervisors).

2.7 Additional Stipulations

1. Deliverables shall be labeled Sensitive But Unclassified (SBU) or contractor selected designation per document sensitivity. External transmission/dissemination of SBU to or from a Government computer must be encrypted. Certified encryption modules must be used in accordance with FIPS PUB 140-2, *"Security Requirements for Cryptographic Modules."*
2. The Contractor shall certify applications are fully functional and operate correctly as intended on systems using the United States Government Configuration Baseline (USGCB). This includes Internet Explorer configured to operate on Windows. The standard installation, operation, maintenance, update, and/or patching of software shall not alter the configuration settings from the approved USGCB configuration. The information technology should also use the Windows Installer Service for installation to the default "program files" directory and should be able to silently install and uninstall. Applications designed for normal end users shall run in the standard user context without elevated system administration privileges. The contractor shall use Security Content Automation Protocol (SCAP) validated tools with USGCB Scanner capability to certify their products operate correctly with USGCB configurations and do not alter USGCB settings.
3. The Contractor shall cooperate in good faith in defining non-disclosure agreements that other third parties must sign when acting as the Federal government's agent.
4. The Government has the right to perform manual or automated audits, scans, reviews, or other inspections of the vendor's IT environment being used to provide or facilitate services for the Government. The Contractor shall be responsible for the following privacy and security safeguards:
    a. The Contractor shall not publish or disclose in any manner, without the Contracting Officer's written consent, the details of any safeguards either designed or developed by the Contractor under this contract or otherwise provided by the Government. Exception - Disclosure to a Consumer Agency for purposes of A&A verification or to the MAX.Gov portal. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours of the request. Access to support incident investigations, shall be provided as soon as possible but not longer than 72 hours after request.

        The program of inspection shall include, but is not limited to:

        - Authenticated and unauthenticated operating system/network vulnerability scans
        - Authenticated and unauthenticated web application vulnerability scans

- Authenticated and unauthenticated database application vulnerability scans
- Automated scans can be performed by Government personnel, or agents acting on behalf of the Government, using Government operated equipment, and Government specified tools. If the vendor chooses to run its own automated scans or audits, results from these scans may at the Government's discretion, be accepted in lieu of Government performed vulnerability scans. In these cases, scanning tools and their configuration shall be approved by the Government. In addition, the results of vendor-conducted scans shall be provided in full to the Government.

b. If new or unanticipated threats or hazards are discovered by either the Government or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.

5. The Contractor shall comply with Section 1634 of Public Law 115-91 that prohibits use of any hardware, software, or services developed or provided, in whole or in part, by— (1) Kaspersky Lab (or any successor entity); (2) any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or (3) any entity of which Kaspersky Lab has majority ownership.

3 Internal Information Systems - IT Security and Privacy Requirements

3.1 Required Policies and Regulations for GSA Contracts

Federal Laws and Regulations:

The contractor shall comply with all applicable Federal Laws and Regulations.

- 40 U.S.C. 11331, "*Responsibilities for Federal Information Systems Standards*"
- FISMA of 2014, "*The Federal Information Security Modernization Act of 2014*"
- HSPD 12, "*Homeland Security Presidential Directive 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*"
- OMB Circular No. A-130, "*Managing Information as a Strategic Resource*"
- OMB M-08-23, "*Securing the Federal Government's Domain Name System Infrastructure (Submission of Draft Agency Plans Due by September 5, 2008)*"
- OMB M 14-03, "*Enhancing the Security of Federal Information and Information Systems*"
- OMB M-10-23, "*Guidance for Agency Use of Third-Party Websites and Applications*"
- OMB M-15-13, "*Policy to Require Secure Connections across Federal Websites and Web Services*"
- OMB M-17-12, "*Preparing for and Responding to a Breach of Personally Identifiable Information*"
- Privacy Act of 1974, "*5 USC, § 552a*"
- OMB Memoranda, location of current fiscal year guidance on Federal Information Security and Privacy Management Requirements, including FISMA reporting

Federal Standards and Guidance:

The contractor shall comply with all applicable Federal Information Processing Standards (FIPS). NIST Special Publications (800 Series) are guidance, unless required by a FIPS publication, in which case usage is mandatory.

- FIPS PUB 199, "*Standards for Security Categorization of Federal Information and Information Systems*"
- FIPS PUB 200, "*Minimum Security Requirements for Federal Information and Information Systems*"
- FIPS PUB 140-2, "*Security Requirements for Cryptographic Modules*"
- NIST SP 800-18, Revision 1, "*Guide for Developing Security Plans for Federal Information Systems*"
- NIST SP 800-30, Revision 1, "*Guide for Conducting Risk Assessments*"
- NIST SP 800-34, Revision 1, "*Contingency Planning Guide for Federal Information Systems*"
- NIST SP 800-37, Revision 1, "*Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Lifecycle Approach*"
- NIST SP 800-47, "*Security Guide for Interconnecting Information Technology Systems*"
- NIST SP 800-53, Revision 4, "*Security and Privacy Controls for Federal Information Systems and Organizations*"

- NIST SP 800-53A, Revision 4, *"Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans"*
- NIST SP 800-63-3, "*Digital Identity Guidelines*"
- NIST SP 800-122, "*Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*"
- NIST SP 800-137, "*Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*"

GSA Policies:

The contractor shall comply with the following GSA Directives/Policies.

- GSA Order CIO 1878.1, "*GSA Privacy Act Program*"
- GSA Order CIO 1878.2, "*Conducting Privacy Impact Assessments (PIAs) in GSA*"
- GSA Order CIO 2100.1, "*GSA Information Technology (IT) Security Policy*"
- GSA Order CIO 9297.2, "*GSA Information Breach Notification Policy*"

The contractor shall comply with the following GSA policies listed below when inside a GSA building or inside a GSA firewall.

- GSA Order CIO 2100.3, "*Mandatory Information Technology (IT) Security Training Requirement for Agency and Contractor Employees with Significant Security Responsibilities*"
- GSA Order 9732.1 ADM P, "*Suitability and Personnel Security*"

The GSA policies listed in this paragraph must be followed, if applicable.

- GSA Order CIO 2103.1, "*Controlled Unclassified Information (CUI) Policy*"
- GSA Order CIO 2104.1, "*GSA Information Technology (IT) General Rules of Behavior*"
- GSA Order CIO 2182.2, "*Mandatory Use of Personal Identity Verification (PIV) Credentials*"

GSA Procedural Guides:

GSA IT Procedural Guides are guidance, unless required by a GSA Directive/Policy, in which case usage is mandatory.

Note: GSA's Procedural Guides are updated frequently; to make sure you have the most recent version of publicly available procedural guides, visit GSA.gov. If a non-publicly available guide is needed, contact the contracting officer who will coordinate with GSA Office of the Chief Information Security Officer to determine if it can be made available.

3.2 GSA Security Compliance Requirements

FIPS PUB 200, *"Minimum Security Requirements for Federal Information and Information Systems,"* is a mandatory federal standard that defines the minimum security requirements for federal information and information systems in seventeen security-related areas. Information

systems supporting GSA must meet the minimum security and privacy requirements through the use of the security controls in accordance with NIST Special Publication 800-53, Revision 4 (hereafter described as NIST 800-53), *"Security and Privacy Controls for Federal Information Systems and Organizations."*

To comply with the federal standard, GSA must determine the security category of the information and information system in accordance with FIPS PUB 199, *"Standards for Security Categorization of Federal Information and Information Systems,"* and then the contractor shall apply the appropriately tailored set of Low, Moderate, or High impact baseline security controls in NIST 800-53, as determined by GSA. NIST 800-53 controls requiring organization-defined parameters (i.e., password change frequency) shall be consistent with GSA specifications. The GSA-specified control parameters and supplemental guidance defining more specifically the requirements per FIPS PUB 199 impact level are available in the GSA Control Tailoring Workbook referenced in Appendix A of this document.

The Contractor shall use GSA technical guidelines, NIST guidelines, Center for Internet Security (CIS) guidelines (Level 1), or industry best practice guidelines in hardening their systems. Where a GSA security hardening benchmark exists, it must be used. GSA security hardening benchmarks may be exceeded but not lowered. GSA benchmarks are available on the GSA Intranet and will be provided by GSA upon request.

3.3 Essential Security Controls

All NIST 800-53 controls must be implemented as per the applicable FIPS PUB 199 Low, Moderate, or High baseline. The following table identifies essential security controls from the respective baselines to highlight their importance; ensure they are implemented; and identify integration requirements with GSA's IT and IT Security environment (if any). Contractor systems shall ensure these essential security controls are implemented. Further, the Contractor shall make the proposed system and security architecture of the information system available to the Security Engineering Division, in the Office of the Chief Information Security Officer for review and approval before commencement of system build (architecture, infrastructure, and code).

Control ID	Control Title	Baseline	GSA Implementation Guidance
AC-2	Account Management	L, M, H	Account management systems must leverage or integrate seamlessly with an existing GSA Access and Identity Management Solution such as GAMS, PIV-based authentication, or other GSA-supported Single-Sign-On solution.
AC-17 (3)	Remote Access | Managed Access Control Points	M, H	All remote accesses to the internal information system must be routed through GSA's managed network access control points, subjecting them to security monitoring.

Control ID	Control Title	Baseline	GSA Implementation Guidance
AU-2	Audit Events	L, M, H	Information systems shall implement audit configuration requirements as documented in applicable GSA IT Security Technical Hardening Guides (i.e., hardening and technology implementation guides); for web applications see GSA IT Security Procedural Guide 07-35, Section 2.8.10, What to Log. For technologies where a Technical Guide and Standard does not exist, events from an industry source such as vendor guidance or Center for Internet Security (CIS) benchmark, recommended by the GSA S/SO or Contractor to be approved by the GSA AO shall be used. Internal Information systems shall transmit OS audit log events to GSA's Enterprise Logging Platform (ELP) when possible. OS audit logs not able to be transmitted o the ELP, web application, database, and other logs will be will be retained by the system owner.
CM-6	Configuration Settings	L, M, H	Information systems shall implement GSA benchmarks for system hardening. GSA benchmarks may be exceeded but not lowered. Where a GSA benchmark does NOT exist, GSA technical guidelines, NIST guidelines, Center for Internet Security guidelines (Level 1), or industry best practice guidelines, as deemed appropriate, may be used. Further, all workstations and servers connected to the GSA network shall have BigFix and have agents installed.
CP-7	Alternative Processing Site	M, H	FIPS PUB 199 Moderate and High impact systems must implement processing across geographically-disparate locations to ensure fault tolerance. Amazon Web Services based architectures must implement a multi-region strategy (multiple availability zones in a single region are not sufficient).
CP-8	Telecom Services	M, H	FIP PUB 199 Moderate and High impact information systems must implement alternate telecom services to support resumption when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.
IA-2 (1)	Identification and Authentication (Organizational Users) | Network Access to Privileged Accounts	L, M, H	Information systems shall implement multi-factor authentication for privileged accounts. Information systems shall technically integrate with a GSA supported enterprise identification and authentication solution (e.g., SAML 2.0 with SSO integration (following 2FA with HSPD-12 PIV card)).

Control ID	Control Title	Baseline	GSA Implementation Guidance
IA-2 (2)	Identification and Authentication (Organizational Users) | Network Access to Non-Privileged Accounts	M, H	Information systems at the FIPS PUB 199 Moderate and High impact levels must implement multi-factor authentication for non-privileged accounts. Information systems shall technically integrate with a GSA supported enterprise identification and authentication solution (e.g., SAML 2.0 with SSO integration (following 2FA with HSPD-12 PIV card)).
IA-7	Cryptographic Module Authentication	L, M, H	The information system shall implement FIPS PUB 140-2 compliant encryption modules for authentication functions. Reference: https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules
MP-4	Media Storage	M, H	Digital media including magnetic tapes, external/removable hard drives, flash/thumb drives, diskettes, compact disks and digital video disks shall be encrypted using a FIPS PUB 140-2 certified encryption module.
MP-5	Media Transport	M, H	Digital media including magnetic tapes, external/removable hard drives, flash/thumb drives and digital video disks shall be encrypted using a FIPS PUB 140-2 certified encryption module during transport outside of controlled areas.
PL-8	Information Security Architecture	M, H	All information system security architectures must be formally reviewed and approved by the Office of the Chief Information Security Officer, Security Engineering Division during the system develop/design stages of the SDLC and prior to Security Assessment and Authorization.
RA-5	Vulnerability Scanning	L, M, H	All systems must integrate with the GSA vulnerability scanning tool set managed by the Security Operations Division in the Office of the Chief Information Security Officer. Information systems shall coordinate integration with the scanning program by contacting SecOps@gsa.gov.
SA-22	Unsupported System Components	GSA Required	All systems must be comprised of software and hardware components that are fully supported in terms of security patching for the anticipated life of the system; software must be on GSA's Enterprise Architecture IT Standards List.

Control ID	Control Title	Baseline	GSA Implementation Guidance
SC-8/ SC-8(1)	Transmission Confidentiality and Integration	M, H	Implemented encryption algorithms and cryptographic modules shall be FIPS-approved and FIPS PUB 140-2 validated, respectively. ○ Digital signature encryption algorithms - Reference: https://csrc.nist.gov/Projects/Cryptographic-Algorithm-Validation-Program/Validation/Validation-List/DSA ○ Block cypher encryption algorithms - Reference: https://csrc.nist.gov/Projects/Cryptographic-Algorithm-Validation-Program/Block-Ciphers ○ Secure hashing algorithms – Reference: https://csrc.nist.gov/Projects/Cryptographic-Algorithm-Validation-Program/Secure-Hashing Internet accessible Websites shall implement HTTPS Only and HTTP Strict Transport Security (HSTS), reference OMB Memorandum M-15-13. SSL/TLS implementations shall align with GSA IT Security Procedural Guide 14-69, *"SSL/TLS Implementation."*
SC-13	Cryptographic Protection	L, M, H	Implemented encryption algorithms and cryptographic modules shall be FIPS-approved and FIPS PUB 140-2 validated, respectively. ○ Digital signature encryption algorithms - Reference: https://csrc.nist.gov/Projects/Cryptographic-Algorithm-Validation-Program/Validation/Validation-List/DSA ○ Block cypher encryption algorithms - Reference: https://csrc.nist.gov/Projects/Cryptographic-Algorithm-Validation-Program/Block-Ciphers ○ Secure hashing algorithms – Reference: https://csrc.nist.gov/Projects/Cryptographic-Algorithm-Validation-Program/Secure-Hashing
SC-17	PKI Certificates	M, H	Implement appropriate creation, use, and signing of crypto certs in agreement with GSA IT Security Procedural Guide 14-69, *"SSL/TLS Implementation,"* and NIST Special Publications 800-32, NIST 800-63.
SC-18	Mobile Code	M, H	iOS and Android app creation, usage restrictions. Mobile applications shall undergo assessment and authorization practices as documented in GSA IT Security Procedural Guide 12-67, *"Securing Mobile Devices and Applications."*
SC-22	Architecture and Provisioning for Name / Address Resolution Service	L, M, H	Information systems shall be Domain Name System Security Extensions (DNSSEC) compliant. Reference OMB Memorandum M-08-23, which requires all Federal Government departments and agencies that have registered and are operating second level .gov to be DNSSEC.

Control ID	Control Title	Baseline	GSA Implementation Guidance
SC-28 (1)	Protection of Information at Rest | Cryptographic Protection	GSA Required – For systems with Personally Identifiable Information Only	Systems bearing PII must implement protect information at rest. At a minimum, fields bearing PII data must be encrypted with field level encryption. Encryption algorithms shall be FIPS-approved; implemented encryption modules shall be FIPS PUB 140-2 validated.
SI-2	Flaw Remediation	L, M, H	All projects and systems must be adequately tested for flaws; all Critical, High, and Moderate risk findings must be remediated prior to go-live. Post go-live, all critical and high vulnerabilities identified must be mitigated within 30 days and all moderate vulnerabilities mitigated within 90 days.
SI-3	Malicious Code Protection	L, M, H	All internal information systems must incorporate Bit9 and FireEye HX agents on supported operating systems. These agents will be provided.
SI-4	Information System Monitoring	L, M, H	All information systems must be monitored internally and across ingress/egress points for potentially malicious activity. In addition, all internal information systems must incorporate Bit9 and FireEye HX agents on supported operating systems. These agents will be provided.
SI-10	Information Input Validation	M, H	All system accepting input from end users must validate the input in accordance to industry best practices and published guidelines, including GSA IT Security Procedural Guide 07-35, *"Web Application Security,"* and OWASP Top 10 Web Application Security Vulnerabilities.
AR-2	Privacy Impact and Risk Assessment	See note below	The contractor shall conduct a Privacy Threshold Analysis (PTA) and, if applicable, a Privacy Impact Assessment (PIA) identifying the categories of information and addressing potential risks to PII. The contractor also shall coordinate with the GSA Privacy Office concerning these documents.
AR-8	Accounting of Disclosures	See note below	The contractor shall keep an accurate accounting of disclosures of information held in any system of records under its control.
TR-2	System of Records Notices and Privacy Act Statements	See note below	The contractor shall coordinate with the GSA Privacy Office to ensure System of Records Notices (SORNs) and Privacy Act notices on forms that collect Personally Identifiable Information (PII) are established and kept current.
UL-1	Internal Use	See note below	The contractor shall ensure that PII is shared internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices.

Control ID	Control Title	Baseline	GSA Implementation Guidance
UL-2	Information Sharing with Third Parties	See note below	The contractor shall coordinate with the GSA Privacy Office to ensure PII is shared in accordance with GSA requirements and agreements with third parties.

Note: Privacy controls are not associated with a baseline. Controls are applicable/not applicable based on PII data being collected, stored, or transmitted.

3.4 Assessment and Authorization (A&A) Activities

The implementation of a new Federal Government IT system requires a formal approval process known as Assessment and Authorization (A&A). NIST Special Publication 800-37, Revision 1 (hereafter described as NIST 800-37) and GSA IT Security Procedural Guide 06-30, "*Managing Enterprise Risk,"* provide guidelines for performing the A&A process. The Contractor system/application must have a valid assessment and authorization, known as an Authority to Operate (ATO) (signed by the Federal government) before going into operation and processing GSA information. The failure to obtain and maintain a valid ATO will result in the termination of the contract. The system must have a new A&A conducted (signed by the Federal government) at least every three (3) years or at the discretion of the Authorizing Official when there is a significant change to the system's security posture or via continuous monitoring based on GSA IT Security Procedural Guide 12-66, "*Information Security Continuous Monitoring Strategy*" that is reviewed and accepted by the GSA CISO.

Assessing the System

1. The Contractor shall comply with Assessment and Authorization (A&A) requirements as mandated by Federal laws and policies, including making available any documentation, physical access, and logical access needed to support this requirement. The Level of Effort for the A&A is based on the System's NIST Federal Information Processing Standard (FIPS) Publication 199 categorization. The contractor shall create, maintain and update the following A&A documentation:
    - System Security Plan (SSP) completed in agreement with NIST Special Publication 800-18, Revision 1, *"Guide for Developing Security Plans for Federal Information Systems.*" The SSP shall include as appendices required policies and procedures across 17 control families mandated per FIPS PUB 200, Rules of Behavior, and Interconnection Agreements (in agreement with NIST Special Publication 800-47, *"Security Guide for Interconnecting Information Technology Systems"*). The SSP shall include; as an appendix, a completed GSA Control Tailoring Workbook identified in Appendix A of this guide. The column in the workbook titled "GSA Defined Values," shall be used to document all contractor implemented settings that are different from the GSA defined setting and where the GSA defined setting allows a contractor determined setting.
    - Contingency Plan (including Disaster Recovery Plan) completed in agreement with NIST Special Publication 800-34.

- Contingency Plan Test Report completed in agreement with GSA IT Security Procedural Guide 06-29, *"Contingency Planning.*"
- Plan of Actions & Milestones completed in agreement with GSA IT Security Procedural Guide 09-44, *"Plan of Action and Milestones (POA&M)*."
- Penetration Test Reports documenting the results of vulnerability analysis and exploitability of identified vulnerabilities. Note: Penetration testing is required for all FIPS PUB 199 Low impact and Moderate impact Internet accessible information systems, and all FIPS PUB 199 High impact information systems are required to complete an independent penetration test and provide an Independent Penetration Test Report documenting the results of the exercise as part of the A&A package. Reference GSA IT Security Procedural Guide 06-30, *"Managing Enterprise Risk"* and GSA IT Security Procedural Guide 11-51, *"Conducting Penetration Test Exercises"* for penetration testing guidance.

2. Information systems must be assessed and authorized every three (3) years or whenever there is a significant change to the system's security posture in accordance with NIST Special Publication 800-37 Revision 1, "*Guide for the Security Certification and Accreditation of Federal Information Systems,*" and GSA IT Security 06-30, "*Managing Enterprise Risk*" or via continuous monitoring based on GSA CIO IT Security 12-66, "*Information Security Continuous Monitoring Strategy*" that is reviewed and accepted by the GSA CISO.
3. At the Moderate impact level and higher, the **<SELECT: contractor or Government>** is responsible for providing an independent Security Assessment/Risk Assessment in accordance with GSA IT Security Procedural Guide 06-30, *"Managing Enterprise Risk*."
4. If the Government is responsible for providing a Security Assessment/Risk Assessment and Penetration Test, the Contractor shall allow GSA employees (or GSA designated third party contractors) to conduct A&A activities to include control reviews in accordance with NIST 800-53/NIST 800-53A and GSA IT Security Procedural Guide 06-30, *"Managing Enterprise Risk*." Review activities include but are not limited to operating system vulnerability scanning, web application scanning, and database scanning of applicable systems that support the processing, transportation, storage, or security of GSA information. This includes the general support system infrastructure.
5. Identified gaps between required NIST 800-53 controls and the contractor's implementation as documented in the Security Assessment/Risk Assessment report shall be tracked for mitigation in a Plan of Action and Milestones (POA&M) document completed in accordance with GSA IT Security Procedural Guide 09-44, *"Plan of Action and Milestones (POA&M)."* Depending on the severity of the gaps, the Government may require them to be remediated before an Authorization to Operate is issued.
6. The Contractor is responsible for mitigating all security risks found during the A&A and continuous monitoring activities. All high-risk vulnerabilities must be mitigated within 30 days and all moderate risk vulnerabilities must be mitigated within 90 days from the date vulnerabilities are formally identified. The Government will determine the risk rating of vulnerabilities.

Authorization of the System

1. Upon receipt of the documentation (Security Assessment Package, (SAP)) described in GSA IT Security Procedural Guide 06-30, *"Managing Enterprise Risk."* and NIST Special Publication 800-37 as documented above, the GSA Authorizing Official (AO) for the system (in coordination with the GSA Chief Information Security Officer (CISO), system Program Manager (PM), Information System Security Manager (ISSM), and Information System Security Officer (ISSO)) will render an authorization decision to:
    - Authorize system operation w/out any restrictions or limitations on its operation;
    - Authorize system operation w/ restriction or limitation on its operation, or
    - Not authorize for operation.
2. The Contractor shall provide access to the Federal Government, or their designee acting as their agent, when requested, in order to verify compliance with the requirements for an Information Technology security program. At its option, the Government may choose to conduct on site surveys. The Contractor shall make appropriate personnel available for interviews and documentation during this review. If documentation is considered proprietary or sensitive, these documents may be reviewed on-site under the hosting Contractor's supervision.

3.5 Reporting and Continuous Monitoring

Maintenance of the security authorization to operate will be through continuous monitoring of security controls of the contractors system and its environment of operation to determine if the security controls in the information system continue to be effective over time in light of changes that occur in the system and environment. Through continuous monitoring, security controls and supporting deliverables are updated and submitted to GSA per the schedules below. The submitted deliverables (or lack thereof) provide a current understanding of the security state and risk posture of the information systems. They allow GSA AOs to make credible risk-based decisions regarding the continued operations of the information systems and initiate appropriate responses as needed when changes occur.

Deliverables to be provided to the GSA COR/ISSO/ISSM Quarterly

1. Plan of Action & Milestones (POA&M) Update
   Reference: NIST 800-53 control CA-5
   Provide POA&M updates in accordance with requirements and the schedule set forth in GSA CIO IT Security Procedural Guide 09-44, "*Plan of Action and Milestones (POA&M).*"

Deliverables to be provided to the GSA COR/ISSO/ISSM Annually

1. Updated A&A documentation including the System Security Plan and Contingency Plan
    a. System Security Plan

Reference: NIST 800-53 control PL-2
Review and update the System Security Plan annually to ensure the plan is current and accurately describes implemented system controls and reflects changes to the contractor system and its environment of operation. The System Security Plan must be in accordance with NIST 800-18, Revision 1, *"Guide for Developing Security Plans."*

b. Contingency Plan
Reference: NIST 800-53 control CP-2
Provide an annual update to the contingency plan completed in accordance with NIST 800-34, *"Contingency Planning Guide."*

2. User Certification/Authorization Review Documents
Reference: NIST 800-53 control AC-2
Provide the results of the annual review and validation of system users' accounts to ensure the continued need for system access. The user certification and authorization documents will illustrate the organization establishes, activates, modifies, reviews, disables, and removes information system accounts in accordance with documented account management procedures.

3. Separation of Duties Matrix
Reference: NIST 800-53 control AC-5
Develop and furnish a separation of duties matrix reflecting proper segregation of duties for IT system maintenance, management, and development processes. The separation of duties matrix will be updated or reviewed on an annual basis.

4. Information Security Awareness and Training Records
Reference: NIST 800-53 control AT-4
Provide the results of security awareness (AT-2) and role-based information security technical training (AT-3). AT-2 requires basic security awareness training for employees and contractors that support the operation of the contractor system. AT-3 requires information security technical training to information system security roles. Training shall be consistent with the requirements contained in C.F.R. Part 5 Subpart C (5 C.F.R 930.301) and conducted at least annually.

5. Annual FISMA Self-Assessment
Reference: NIST 800-53 control CA-2
Deliver the results of the annual FISMA self-assessment conducted per GSA IT Security Procedural Guide 04-26, "*Federal Information Security Modernization Act (FISMA) Implementation."* Based on the controls selected for self-assessment, the GSA OCISO will provide the appropriate test cases for completion.

6. System(s) Baseline Configuration Standard Document
Reference: NIST 800-53 control CM-2/CM-2(1)
Provide a well-defined, documented, and up-to-date specification to which the information system is built.

7. System Configuration Settings

Reference: NIST 800-53 control CM-6
Establish and document mandatory configuration settings for information technology products employed within the information system that reflect the most restrictive mode consistent with operational requirements. Configuration settings are the configurable security-related parameters of information technology products that compose the information system. Systems shall implement GSA benchmarks for system hardening. GSA benchmarks may be exceeded but not lowered. Where a GSA benchmark does NOT exist, GSA technical guidelines, NIST guidelines, Center for Internet Security guidelines (Level 1), or industry best practice guidelines, as deemed appropriate, may be used.

All workstations and servers connected to the GSA network integrate with BigFix and have agents installed. Provide the most recent operating system Configuration Settings Compliance scan report.

8. Configuration Management Plan
   Reference: NIST 800-53 control CM-9
   Provide an annual update to the Configuration Management Plan for the information system.

9. Contingency Plan Test Report
   Reference: NIST 800-53 control CP-4
   Provide a contingency plan test report completed in accordance with GSA IT Security Procedural Guide 06-29, *"Contingency Planning."* A continuity test shall be conducted annually prior to mid-July of each year. The continuity test can be a table top test while the system is at the FIPS PUB 199 Low Impact level. The table top test must include Federal and hosting Contractor representatives. Functional exercises must be completed once every three years for FIPS PUB 199 Moderate impact systems and annually for FIPS PUB 199 High impact systems.

10. Incident Response Test Report
    Reference: NIST 800-53 control IR-3
    Provide an incident response plan test report documenting results of incident reporting process per GSA IT Security Procedural Guide 01-02, *"Incident Response*."

11. Information System Interconnection Agreements
    Reference: NIST 800-53 control CA-3
    Provide Interconnection Security Agreements (ISA) and supporting Memoranda of Agreement/Understanding (MOA/U), completed in accordance with NIST 800-47, *"Security Guide for Connecting Information Technology Systems,"* for existing and new interconnections. Per NIST 800-47, an interconnection is the direct connection of two or more IT systems for the purpose of sharing data and other information resources through a pipe, such as ISDN, T1, T3, DS3, VPN, etc. ISAs shall be submitted as appendices as part of the annual System Security Plan submission. ISAs shall include, if applicable, any changes since the last submission; updated ISAs are required at least every three years.

12. Rules of Behavior
    Reference: NIST 800-53 control PL-4
    Define and establish Rules of Behavior for information system users. Rules of Behavior shall be submitted as an appendix to the System Security Plan.

13. Penetration Testing Report
    Reference: NIST 800-53 control CA-8
    All Internet accessible systems, and all FIPS PUB 199 High impact systems are required to complete an independent penetration test and provide a Penetration Test Report documenting the results of the exercise as part of their A&A package. Annual penetration tests are required for these same systems in accordance with GSA Order CIO 2100.1 and CIO-IT Security-11-51, "*Conducting Penetration Test Exercises.*"

14. Personnel Screening and Security
    Reference: NIST 800-53 control PS-3, NIST 800-53 control PS-7
    Furnish documentation reflecting favorable adjudication of background investigations for all personnel (including subcontractors) supporting the system. Contractors shall comply with GSA Order CIO 2100.1, "*GSA Information Technology (IT) Security Policy"* and GSA Order CIO P 2181.1, "*Homeland Security Presidential Directive-12 (HSPD-12) Personal Identity Verification and Credentialing Handbook."* GSA separates the risk levels for personnel working on Federal computer systems into three categories: Low Risk, Moderate Risk, and High Risk.

    - Those contract personnel (hereafter known as "Applicant") determined to be in a Low Risk position will require a National Agency Check with Written Inquiries (NACI) investigation.
    - Those Applicants determined to be in a Moderate Risk position will require either a Limited Background Investigation (LBI) or a Minimum Background Investigation (MBI) based on the Contracting Officer's (CO) determination.
    - Those Applicants determined to be in a High Risk position will require a Background Investigation (BI).

    Applicants will not be reinvestigated if a prior favorable adjudication is on file with FPS or GSA, there has been less than a one year break in service, and the position is identified at the same or lower risk level.

    Once a favorable FBI Criminal History Check (Fingerprint Check) has been returned, Applicants may receive a GSA identity credential (if required) and initial access to GSA information systems. The HSPD-12 Handbook contains procedures for obtaining identity credentials and access to GSA information systems as well as procedures to be followed in case of unfavorable adjudications.

Deliverables to be provided to the GSA COR/ISSO/ISSM Biennially

1. Policies and Procedures
   Develop and maintain current the following policies and procedures:
   a. Access Control Policy and Procedures (NIST 800-53 AC-1)
   b. Security Awareness and Training Policy and Procedures (NIST 800-53 AT-1)
   c. Audit and Accountability Policy and Procedures (NIST 800-53 AU-1)
   d. Identification and Authentication Policy and Procedures (NIST 800-53 IA-1)
   e. Incident Response Policy and Procedures (NIST 800-53 IR-1, reporting timeframes are documented in GSA IT Security Procedural Guide 01-02, "*Incident Response*"
   f. System Maintenance Policy and Procedures (NIST 800-53 MA-1)
   g. Media Protection Policy and Procedures (NIST 800-53 MP-1)
   h. Physical and Environmental Policy and Procedures (NIST 800-53 PE-1)
   i. Personnel Security Policy and Procedures (NIST 800-53 PS-1)
   j. System and Information Integrity Policy and Procedures (NIST 800-53 SI-1)
   k. System and Communication Protection Policy and Procedures (NIST 800-53 SC-1)
   l. Key Management Policy (NIST 800-53 SC-12)

3.6 GSA Privacy Requirements

Personally identifiable information (PII) **<SELECT: is or is not>** in the scope of the acquisition and PII **<SELECT: is or is not>** expected to be stored, processed, or transmitted in the vendor's information system. The collection, maintenance or dissemination of any PII that is subject to the Privacy Act and/or the E-Government Act will be handled in full accordance with all GSA rules of conduct and in accordance with GSA Privacy Program requirements.

The contractor shall prepare a Privacy Threshold Analysis (PTA) to confirm and document PII is not in scope, or to determine which categories of information will be stored, processed, or transmitted by the system. The PTA must be completed before development begins and whenever a change with privacy impact (e.g., a new category of information is collected) is made to an existing system. PTAs are required as part of GSA's process to determine whether a Privacy Impact Assessment (PIA) and/or a System of Records Notice (SORN) is required, and if any other privacy requirements apply to the information system. Instructions for the PTA and PIA forms can be found at https://www.gsa.gov/reference/gsa-privacy-program/privacy-impact-assessments-pia.

PII (should it come into scope) will require the following guidelines be adhered to.

- The vendor's information system must be authorized at least at the FIPS PUB 199 Moderate level.
- For any system that collects, maintains or disseminates PII, a PIA must be completed by the contractor and provided to the GSA Privacy Office for review along with the other authorization to operate (ATO) documents.

- If the system retrieves information using PII, the Privacy Act applies and it must have a system of records notice (SORN) published in the Federal Register.
- If PII is collected from individuals by the system, a Privacy Act Statement (i.e., Privacy Notice) must be provided to users prior to their use of the application on what data is being collected and why, as well as the authority for the collection and the impact of not providing some or all of it. The Privacy Act Statement must be available to the individual directly on the form used to collect the information. Providing a link back to the Statement from the form is acceptable.

Provided below is a template for an acceptable Privacy Act Statement, when bracketed sections are completed. A completed example is available at https://www.gsa.gov/reference/gsa-privacy-program/privacy-act-statement-for-design-research.

Privacy Act Statement

This (insert voluntary or mandatory) collection of personal information in authorized by (insert legal authority). We collect (developer insert categories of PII collected, e.g. name, email, etc.). Your personal information is collected so we can (developer insert purpose of collection and what effect on the individual, if any, not providing any or all of the information may have). Your personal information is stored in (developer insert GSA system name). GSA may use this information pursuant to its published Privacy Act system of records notice (insert link to applicable GSA Privacy Act SORN).

Note: Systems that access data a user creates must assume a user may include privacy data/PII in the system unless the data creation is restricted to data controlled by the system.

All contractor staff who have significant privacy information responsibilities must complete GSA's specialized Privacy 201 Training. This includes contractors who work with PII as part of their work duties (e.g.; Human Resource staff, Finance staff, and managers/supervisors).

3.7 Additional Stipulations

1. Deliverables shall be labeled Sensitive But Unclassified (SBU) or contractor selected designation per document sensitivity. External transmission/dissemination of SBU to or from a Government computer must be encrypted. Certified encryption modules must be used in accordance with FIPS PUB 140-2, *"Security Requirements for Cryptographic Modules."*
2. The Contractor shall certify applications are fully functional and operate correctly as intended on systems using the United States Government Configuration Baseline (USGCB). This includes Internet Explorer configured to operate on Windows. The standard installation, operation, maintenance, update, and/or patching of software shall not alter the configuration settings from the approved USGCB configuration. The information technology should also use the Windows Installer Service for installation to the default "program files" directory and should be able to silently install and uninstall. Applications designed for normal end users shall run in the standard user context

without elevated system administration privileges. The contractor shall use Security Content Automation Protocol (SCAP) validated tools with USGCB Scanner capability to certify their products operate correctly with USGCB configurations and do not alter USGCB settings.

3. The Contractor shall cooperate in good faith in defining non-disclosure agreements that other third parties must sign when acting as the Federal government's agent.
4. The Government has the right to perform manual or automated audits, scans, reviews, or other inspections of the vendor's IT environment being used to provide or facilitate services for the Government. The Contractor shall be responsible for the following privacy and security safeguards:
    a. The Contractor shall not publish or disclose in any manner, without the Contracting Officer's written consent, the details of any safeguards either designed or developed by the Contractor under this contract or otherwise provided by the Government. Exception - Disclosure to a Consumer Agency for purposes of A&A verification or to the MAX.Gov portal. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours of the request. Access to support incident investigations, shall be provided as soon as possible but not longer than 72 hours after request.

        The program of inspection shall include, but is not limited to:

        - Authenticated and unauthenticated operating system/network vulnerability scans.
        - Authenticated and unauthenticated web application vulnerability scans
        - Authenticated and unauthenticated database application vulnerability scans.
        - Automated scans can be performed by Government personnel, or agents acting on behalf of the Government, using Government operated equipment, and Government specified tools. If the vendor chooses to run its own automated scans or audits, results from these scans may at the Government's discretion, be accepted in lieu of Government performed vulnerability scans. In these cases, scanning tools and their configuration shall be approved by the Government. In addition, the results of vendor-conducted scans shall be provided in full to the Government.

    b. If new or unanticipated threats or hazards are discovered by either the Government or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.

5. The Contractor shall comply with Section 1634 of Public Law 115-91 that prohibits use of any hardware, software, or services developed or provided, in whole or in part, by— (1) Kaspersky Lab (or any successor entity); (2) any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or (3) any entity of which Kaspersky Lab has majority ownership.

4 Low Impact Software as a Service (LiSaaS) – IT Security and Privacy Requirements

To be considered for award, the contractor must comply with GSA IT's Low-Impact SaaS (LiSaaS) review. The successful vendor will need to ensure any software-as-a-service provided under this contract meets GSA security and privacy requirements prior to invoicing the government for services received under this contract. This includes working with GSA to ensure the Software-as-a-Service (SaaS) passes the current Low-impact-software-as-a-service (LiSaaS) approval process, as outlined in GSA IT Security Procedural Guide 17-75, "*Security Reviews for Low Impact Software as a Service (SaaS) Solutions*." The review process is made up of two main parts: Voluntary Product Accessibility Template (VPAT) for 508 accessibility and security scanning/process reviews. Once this process is complete and the software-as-a-service tool is approved for use by GSA, the CSP will have one year to achieve a FedRAMP authorization. This will either require the software as a service to undergo the FedRAMP Tailored approval process or the standard FedRAMP process for low impact systems. Without a LiSaaS approval, GSA will not be able to use the tool for the base year of the contract, and without FedRAMP approval, GSA will be unable to use the product for the option years of the contract.

The contractor's agreement to the LiSaaS and FedRAMP requirements are required. If the contractor does not agree, no contract award will be made.

If at any time, the vendor is either unwilling or unable to meet any of the process requirements, GSA may choose to cancel the contract and terminate any outstanding orders.

4.1 Assessment of the System

Maintenance of the security authorization to operate will be through continuous monitoring of security controls of the contractors system and its environment of operation to determine if the security controls in the information system continue to be effective over time in light of changes that occur in the system and environment. Through continuous monitoring, security controls and supporting deliverables are updated and submitted to GSA per the schedules below. The submitted deliverables (or lack thereof) provide a current understanding of the security state and risk posture of the information systems. They allow GSA AOs to make credible risk-based decisions regarding the continued operations of the information systems and initiate appropriate responses as needed when changes occur.

The contractor shall provide evidence in support of meeting the requirements for the review activities stated in GSA IT Security Procedural Guide 17-75 and as listed below.

- Unique IDs for each person using the SaaS. Two factor authentication should be used.
- System and security parameters deferred to customers, default settings must be changed.
- Encryption of authentication credentials during transmission.
- Results of web application vulnerability scans.
- Results of operating system vulnerability scans.

- Vendor's flaw remediation process.
- Results of one of the following audits/certifications:
  - Service Organization Control (SOC) 2/Statements on Standards for Attestation Engagements (SSAE) 18
  - SysTrust/WebTrust
  - ISO/IEC 27001
  - Payment Card Industry Data Security Standard (PCI DSS)

4.2 Authorization of the System

The LiSaaS ATO will be valid for no longer than one (1) year. The contractor shall maintain its LiSaaS ATO while pursuing a FedRAMP ATO (i.e., FedRAMP Tailored or the standard FedRAMP process for low impact systems) for its SaaS offering. Without a LiSaaS approval, GSA will not be able to use the tool for the base year of the contract, and without FedRAMP approval, GSA will be unable to use the product for the option years of the contract. If at any time, the vendor is either unwilling or unable to meet any of the process requirements, GSA may choose to cancel the contract and terminate any outstanding orders.

4.3 Reporting and Continuous Monitoring

In support of continuous monitoring the vendor shall maintain its audit report/certification, perform web application and operating system scans, and remediate flaws per the vendor's flaw remediation process. The vendor shall report if its audit report/certification renews or expires and if any of the other required activities cannot be supported.

4.4 Protection of Information

The contractor shall be responsible for properly protecting all information used, gathered, disclosed, or developed as a result of work under this contract. The contractor shall also protect all Government data, etc. by treating the information as sensitive. All information gathered or created under this contract should be considered as confidential information. It is anticipated that this information will be gathered, created and stored within the primary work location. If contractor personnel must remove any information from the primary work area they should protect it to the same extent they would their proprietary data and/or company trade secrets. The use of any information that is subject to the Privacy Act will be utilized in full accordance with all rules of conduct as applicable to Privacy Act Information. Personnel shall adhere to the Privacy Act, Title 5 of the U. S. Code, Section 552a and applicable agency rules and regulations.

4.5 Data Ownership and Unrestricted Rights to Data

All Government data collected in the system is the property of the Federal Government. The Government will retain unrestricted rights to government data. The ordering activity retains All data collected by the system shall be provided by the Contractor (system provider) as requested during the contract period and at the completion of the contract period.

Government data rights of software deliverables shall be in accordance with FAR 52. 227-19 Commercial Computer Software License and/or FAR 52. 227-14 Rights in Data - General. Ownership of data entered into any and all systems, system documentation, all deliverables produced in the performance of this contract, and other related system information shall reside with the Government.

The Contractor shall place the following copyright notice on all materials, documents, deliverables, etc. developed during the performance of this contract:

For purposes of clarity, the intent of the government is for intellectual property to be vested in the federal government for work paid for by the federal government. All documents, graphics, and code created under this contract are the intellectual property of the federal government including, but not limited to, plans, reports, schedules, software code, software designs, graphics, etc. In the event that the federal government implements under this contract open-source software and pays for the cost of the implementation of open-source software, the final changes and edits to the code and configuration (such as work to integrate plug-ins) are the intellectual property of the federal government.

4.6 Personally Identifiable Information

Personally identifiable information (PII) data **is not** in the scope of the acquisition and PII data **is not** expected to be stored in the vendor's SaaS solution. The contractor shall prepare a Privacy Threshold Analysis (PTA) to either document PII is not in scope, or determine which caetgories of information will be stored, processed, or transmitted by the system. The use of any information that is subject to the Privacy Act will be utilized in full accordance with all rules of conduct as applicable to Privacy Act Information.

Privacy data (should it come into scope) will require that the vendor’s SaaS solution be FedRAMP authorized at least at the FIPS PUB 199 Moderate level.

4.7 Data Availability

The data must be available to the Government upon request within one business day or within the timeframe negotiated with the Contractor, and shall not be used for any other purpose other than that specified herein. The contractor shall provide requested data at no additional cost to the government.

4.8 Data Release

Contractor will not disclose Customer Data to any government or third party or access or use Customer Data; except in each case as necessary to maintain the SaaS solution or to provide the SaaS solution to Customer in accordance with this contract, or as necessary to comply with the law or a valid and binding order of a governmental or regulatory body (such as a subpoena or court order). Unless it would be in violation of a court order or other legal requirement, Contractor will give Government reasonable notice of any such legal requirement or order, to allow Government to seek a protective order or other appropriate remedy.

4.9 Confidentiality and Nondisclosure

Personnel (contractor/subcontractor employee)working on any of the described tasks, may at Government request, be required to sign formal non-disclosure and/or conflict of interest agreements to guarantee the protection and integrity of Government information and documents. The Contractor shall submit to the COR a completed confidentiality and non-disclosure agreement form for each individual contractor/subcontractor.

Additionally, any information made available to the Contractor by the Government shall be used only for the purpose of carrying out the provisions of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of the contract. In performance of this contract, the Contractor assumes responsibility for protection of the confidentiality of Government records and shall ensure that all work performed by its subcontractors shall be under the supervision of the Contractor or the Contractor's responsible employees. Each officer or employee of the Contractor or any of its subcontractors to whom any Government record may be made available or disclosed shall be notified in writing by the Contractor that information disclosed to such officer or employee can be used only for that purpose and to the extent authorized herein. Further disclosure of any such information, by any means, for a purpose or to an extent unauthorized herein, may subject the offender to criminal sanctions imposed by 18 U. S. C. §§ 1030.

4.10 Section 508 Compliancy

The Contractor(s) shall provide accessibility based on Section 508 of the Rehabilitation Act of 1973 (29 U. S. C. 794d). All electronic and information technology (EIT) delivered must meet the applicable accessibility standards at 36 CFR 1194, unless an agency exception to this requirement exists. The 36 CFR 1194 implements Section 508 of the Rehabilitation Act of 1973, as amended. All deliverables will be Section 508 compliant, and will be reviewed for compliance by the government which reserves the right to reject the deliverable(s) until remediation of deficiencies has been successfully completed by the Contractor. Complete technical descriptions are provided on the following website: http://www.section508.gov.

Where appropriate, the Contractor(s) shall indicate whether each product or service is compliant or noncompliant with the accessibility standards at 36 CFR 1194. Further, the quote must indicate where full details of compliance can be found (e. g., vendor's website or other exact location).

4.11 Additional Stipulations

1. Deliverables shall be labeled Sensitive But Unclassified (SBU) or contractor selected designation per document sensitivity. External transmission/dissemination of SBU to or from a Government computer must be encrypted. Certified encryption modules must be used in accordance with FIPS PUB 140-2, "*Security Requirements for Cryptographic Modules*."
2. The contractor shall cooperate in good faith in defining non-disclosure agreements that

other third parties must sign when acting as the Federal government's agent.

3. The Government has the right to perform manual or automated audits, scans, reviews, or other inspections of the vendor's IT environment being used to provide or facilitate services for the Government. The Contractor shall be responsible for the following privacy and security safeguards:

    a. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours of the request. Access to support incident investigations, shall be provided as soon as possible but not longer than 72 hours after request.

    b. Physical Access Considerations – If the SaaS provider is operated within an IaaS that is FedRAMP authorized (e. g., AWS); physical access to the physical datacenter environment will be governed by the terms of access allowed by the underlying infrastructure provider as defined in the FedRAMP A&A authorization package.

    c. The program of inspection shall include, but is not limited to:

        - Authenticated and unauthenticated operating system/network vulnerability scans
        - Authenticated and unauthenticated web application vulnerability scans
        - Authenticated and unauthenticated database application vulnerability scans
        - Automated scans can be performed by Government personnel, or agents acting on behalf of the Government, using Government operated equipment, and Government specified tools. If the vendor chooses to run its own automated scans or audits, results from these scans may at the Government's discretion, be accepted in lieu of Government performed vulnerability scans. In these cases, scanning tools and their configuration shall be approved by the Government. In addition, the results of vendor-conducted scans shall be provided in full to the Government.

    d. If new or unanticipated threats or hazards are discovered by either the Government or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.

4. The Contractor shall comply with Section 1634 of Public Law 115-91 that prohibits use of any hardware, software, or services developed or provided, in whole or in part, by— (1) Kaspersky Lab (or any successor entity); (2) any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or (3) any entity of which Kaspersky Lab has majority ownership.

4.12 Terms of Service

Many terms found in commercial ToS or End User License Agreements (EULA) are not acceptable when the Government is the end user. Office of Chief Information Officer (OCIO) requires that software and services within the GSA Enterprise have approved ToS or EULA.

The Contractor's SaaS will undergo a formal review by GSA as part of the review/approval process. The Contractor's ToS shall be found to be acceptable to the government or a modified ToS negotiated as part of the approval review, prior to final authorization.

4.13 References

GSA IT Security Procedural Guide 17-75, *"Security Reviews for Low Impact Software as a Service (SaaS) Solutions"*

FIPS PUB 199, *"Standards for Security Categorization of Federal Information and Information Systems"*

Guide to Understanding FedRAMP

5 Cloud Information Systems – IT Security and Privacy Requirements

The contractor shall implement the controls contained within the FedRAMP Cloud Computing Security Requirements Baseline and FedRAMP Continuous Monitoring Requirements for **<SELECT Low, Moderate, or High>** impact systems (as defined in FIPS PUB 199). These documents define requirements for compliance to meet minimum Federal information security and privacy requirements for **<SELECT Low, Moderate, or High>** impact systems. The FedRAMP baseline controls are based on NIST Special Publication 800-53, Revision 4, *"Security and Privacy Controls for Federal Information Systems and Organizations"* (as amended), and also includes a set of additional controls for use within systems providing cloud services to the federal government.

The contractor shall generally, substantially, and in good faith follow FedRAMP guidelines and Security guidance. In situations where there are no procedural guides, the contractor shall use generally accepted industry best practices for IT security.

GSA may choose to cancel the contract and terminate any outstanding orders if the contractor has its FedRAMP authorization (Joint Authorization Board [JAB] Provisional or Agency) revoked and the deficiencies are greater than agency risk tolerance thresholds.

5.1 Assessment and Authorization

5.2 Assessment of the System

1. The contractor shall comply with FedRAMP requirements as mandated by Federal laws and policies, including making available any documentation, physical access, and logical access needed to support this requirement. The Level of Effort for the A&A is based on the System's FIPS PUB 199 categorization. The contractor shall create, maintain and update the following documentation using FedRAMP requirements and templates, which are available at https://www.fedramp.gov/:
    - Privacy Impact Assessment (PIA)
    - FedRAMP Test Procedures and Results
    - Security Assessment Report (SAR)
    - System Security Plan (SSP)
    - Contingency Plan (CP)
    - Contingency Plan (CP) Test Results
    - Plan of Action and Milestones (POA&M)
    - Continuous Monitoring Plan (CMP)
    - FedRAMP Control Tailoring Workbook
    - Control Implementation Summary Table
    - Results of Penetration Testing
    - Software Code Review

- Interconnection Agreements/Service Level Agreements/Memorandum of Agreements

2. Information systems must be assessed by an accredited FedRAMP Third Party Assessment Organization (3PAO) initially and whenever there is a significant change to the system's security posture in accordance with the FedRAMP Continuous Monitoring Plan.
3. The Government reserves the right to perform Security Assessment and Penetration Testing (of its instance). If the Government exercises this right, the contractor shall allow Government employees (or designated third parties) to conduct Security Assessment and Penetration Testing activities to include control reviews in accordance with FedRAMP requirements. Penetration shall be supported by mutually agreed upon Rules of Engagement (RoE). Review activities include but are not limited to manual penetration testing; automated scanning of operating systems, web applications; wireless scanning; network device scanning to include routers, switches, and firewall, and IDS/IPS; databases and other applicable systems, including general support structure, that support the processing, transportation, storage, or security of Government information for vulnerabilities.
4. The contractor shall provide access to the Federal Government, or their designee acting as their agent, when requested, in order to verify compliance with the requirements for an Information Technology security program. The Government reserves the right to conduct on-site inspections. The contractor shall make appropriate personnel available for interviews and provide all necessary documentation during this review.
5. Physical Access Considerations – If the Cloud Service Provider (CSP) is operated within an Infrastructure as a Service (IaaS) that is FedRAMP authorized (e.g., AWS); physical access to the physical datacenter environment will be governed by the terms of access allowed by the underlying infrastructure provider as defined in the FedRAMP A&A authorization package.
6. Identified gaps between required FedRAMP Security Control Baselines and Continuous Monitoring controls and the contractor's implementation as documented in the Security Assessment Report shall be tracked by the contractor for mitigation in a Plan of Action and Milestones (POA&M) document. Depending on the severity of the gaps, the Government may require them to be remediated before a GSA authorization is issued.
7. The contractor is responsible for mitigating all security risks found during A&A and continuous monitoring activities. All high-risk vulnerabilities must be mitigated within 30 days and all moderate risk vulnerabilities must be mitigated within 90 days from the date vulnerabilities are formally identified. The Government will determine the risk rating of vulnerabilities.

5.3 Authorization of the System

1. If the CSP Software as a Service (SaaS) or Platform as a Service (PaaS) is FedRAMP authorized (i.e., listed as FedRAMP authorized on the FedRAMP website:

   https://marketplace.fedramp.gov/index.html#/products?sort=productName&status=Compliant

   GSA will leverage the CSP's FedRAMP Assessment and Authorization package to document and assess the customer controls for which GSA has responsibility and issue a GSA ATO for the agency's instance of the CSP's SaaS or PaaS offering. The CSP shall work with the GSA to facilitate documentation and assessment of required customer controls, as necessary.

2. If the CSP SaaS or PaaS offering is NOT already FedRAMP authorized, it shall:

   a. Operate on an CSP IaaS environment that is FedRAMP authorized; AND

   b. Be listed as FedRAMP In Process on the FedRAMP Website - https://marketplace.fedramp.gov/index.html#/products?sort=productName&status=In%20Process

      OR be listed as FedRAMP Ready on the FedRAMP website - https://marketplace.fedramp.gov/index.html#/products?sort=productName&status=FedRAMP%20Ready

   c. Shall deliver within 90 days of contract award a FedRAMP Readiness Assessment Review completed by a FedRAMP 3PAO following the FedRAMP Readiness Assessment Guidelines. The FedRAMP Readiness Assessment Review demonstrates the CSPs overall readiness for FedRAMP authorization and whether it has a viable path to achieve a FedRAMP authorization within one (1) year of the contract award. If the CSP does not provide a FedRAMP Readiness Assessment as prescribed or the assessment demonstrates a significant gap in capabilities that will preclude achievement of a FedRAMP authorization within 1 year of the contract award, then, GSA will terminate the contract.

   If requirements a-c, as defined above, are met the CSP will have one (1) year from the date of contract award to achieve FedRAMP authorization. During this transitional period, GSA may issue an agency specific authorization (i.e., not FedRAMP) not to exceed one (1) year (to allow the CSP to achieve FedRAMP compliance) leveraging an existing ATO with another Federal Department/Agency (D/A) (with supporting A&A Package). The CSP may have a non-FedRAMP ATO with another D/A or be based on the GSA Moderate Impact SaaS Solutions process as described in GSA IT Security Procedural Guide 06-30, "*Managing Enterprise Risk.*" The CSP shall make available any existing assessment and authorization package for GSA review and provide necessary documentation and access to facilitate the GSA Moderate Impact SaaS A&A process. Without a FedRAMP authorization within 1 year of contract award; GSA will not be able to use the product for the option years and shall terminate the contract.

3. CSP shall ensure these essential security controls are implemented. CSP shall implement FedRAMP control parameters and implementation guidance, as applicable. Further, the CSP shall make the proposed system and security architecture of the information system available to the Security Engineering Division, in the Office of the Chief Information Security Officer for review and approval before commencement of system build (architecture, infrastructure, and code (as applicable)) and/or the start as A&A activities.

Control ID	Control Title	FedRAMP Baseline
AC-2	Account Management	L, M, H
AU-2	Audit Events	L, M, H
CM-6	Configuration Settings	L, M, H
CP-7	Alternative Processing Site	M, H
CP-8	Telecom Services	M, H
IA-2 (1)	Identification and Authentication (Organizational Users) | Network Access to Privileged Accounts	L, M, H
IA-2 (2)	Identification and Authentication (Organizational Users) | Network Access to Non-Privileged Accounts	M, H
IA-2 (12)	Identification and Authentication (Organizational Users) | Acceptance of PIV Credentials	L, M, H
IA-7	Cryptographic Module Authentication	L, M, H
MP-4	Media Storage	M, H
MP-5	Media Transport	M, H
PL-8	Information Security Architecture	M, H
RA-5	Vulnerability Scanning	L, M, H
SC-8 / SC-8(1)	Transmission Confidentiality and Integrity / Transmission Confidentiality and Integrity | Cryptographic or Alternate Physical Protection	M, H
SC-13	Cryptographic Protection	L, M, H
SC-17	PKI Certificates	M, H
SC-18	Mobile Code	M, H
SC-22	Architecture and Provisioning for Name / Address Resolution Service	L, M, H

Control ID	Control Title	FedRAMP Baseline
SC-28 (1)	Protection of Information at Rest | Cryptographic Protection	M, H
SI-2	Flaw Remediation	L, M, H
SI-3	Malicious Code Protection	L, M, H
SI-4	Information System Monitoring	L, M, H
SI-10	Information Input Validation	M, H

5.4 Reporting and Continuous Monitoring

Maintenance of the FedRAMP Authorization will be through continuous monitoring and periodic audit of the operational controls within a contractor's system, environment, and processes to determine if the security controls in the information system continue to be effective over time in light of changes that occur in the system and environment. Through continuous monitoring, security controls and supporting deliverables are updated in agreement with FedRAMP guidelines and submitted to the MAX.Gov Portal or repository designated by the FedRAMP program.

The submitted deliverables (or lack thereof) provide a current understanding of the security state and risk posture of the information systems. The deliverables will allow the Federal Departments/Agencies leveraging the services providers' cloud offering to make credible risk-based decisions regarding the continued operations of the information systems and initiate appropriate responses as needed when changes occur. Contractors will be required to provide updated deliverables and automated data feeds as defined in the FedRAMP Continuous Monitoring Plan.

The contractor shall provide continuous monitoring deliverables in support of a one (1) year conditional authorization (if necessary) to achieve FedRAMP authorization. Deliverables shall include:

- Quarterly OS, web, and database vulnerability scans (deliverable shall include raw results and findings shall be included in the POA&M document);
- Quarterly Plan of Action and Milestones (POA&M);
- Annual A&A Package updates including the System Security Plan, Contingency Plan, Configuration Management Plan, Contingency Plan Test Report, and Annual FISMA Assessment.

Upon achievement of FedRAMP authorization, GSA will accept the FedRAMP A&A and continuous monitoring documentation made available on the MAX.Gov Portal or a repository designated by the FedRAMP program in agreement with FedRAMP guidelines to satisfy the continuous monitoring requirement.

5.5 Personnel Security Requirements

Contractor shall furnish documentation reflecting favorable adjudication of background investigations for all personnel (including subcontractors) supporting the system. Contractors shall comply with GSA Order CIO 2100.1, "*GSA Information Technology (IT) Security Policy,"* and GSA Order CIO P 2181.1, "*HSPD-12 Personal Identity Verification and Credentialing Handbook*." GSA separates the risk levels for personnel working on Federal computer systems into three categories: Low Risk, Moderate Risk, and High Risk.

- Those contract personnel (hereafter known as "Applicant") determined to be in a Low Risk position will require a National Agency Check with Written Inquiries (NACI) investigation.
- Those Applicants determined to be in a Moderate Risk position will require either a Limited Background Investigation (LBI) or a Minimum Background Investigation (MBI) based on the Contracting Officer's (CO) determination.
- Those Applicants determined to be in a High Risk position will require a Background Investigation (BI).

Applicants will not be reinvestigated if a prior favorable adjudication is on file with FPS or GSA, there has been less than a one year break in service, and the position is identified at the same or lower risk level.

Once a favorable FBI Criminal History Check (Fingerprint Check) has been returned, Applicants may receive a GSA identity credential (if required) and initial access to GSA information systems. The HSPD-12 Handbook contains procedures for obtaining identity credentials and access to GSA information systems as well as procedures to be followed in case of unfavorable adjudications.

GSA shall sponsor the investigation when deemed necessary. No access shall be given to government computer information systems and government sensitive information without a background investigation being verified or in process. If results of background investigation are not acceptable, then access shall be terminated.

The Contractor shall provide a report of separated staff on a monthly basis, beginning 60 days after execution of the option period.

5.6 Sensitive Information Storage

Sensitive But Unclassified (SBU) information, data, and/or equipment will only be disclosed to authorized personnel on a need-to-know basis. The contractor shall ensure that appropriate administrative, technical, and physical safeguards are established to ensure the security and confidentiality of this information, data, and/or equipment is properly protected. When no longer required, this information, data, and/or equipment will be returned to Government control, destroyed, or held until otherwise directed. Destruction of items shall be accomplished by following NIST Special Publication 800-88, *"Guidelines for Media Sanitization."* The

destruction, purging or clearing of media specific to the CSP will be recorded and supplied upon request of the Government.

5.7 Protection of Information

The contractor shall be responsible for properly protecting all information used, gathered, or developed as a result of work under this contract. The contractor shall also protect all Government data, equipment, etc. by treating the information in accordance with its FISMA system categorization.

All information about the systems gathered or created under this contract should be considered as SBU information. If contractor personnel must remove any information from the primary work area that is included in the ATO boundary, they should protect it to the same FedRAMP requirements. The use of any information that is subject to the Privacy Act will be utilized in full accordance with all rules of conduct as applicable to Privacy Act Information.

5.7.1 Unrestricted Rights to Data

The government will retain unrestricted rights to government data. The ordering activity retains ownership of any user created/loaded data and applications hosted on vendor's infrastructure, as well as maintains the right to request full copies of these at any time.

5.7.2 Personally Identifiable Information

Personally identifiable information (PII) **<SELECT: is or is not>** in the scope of acquisition and PII **<SELECT: is or is not>** expected to be stored in the vendor's cloud solution. The collection, maintenance or dissemination of any PII that is subject to the Privacy Act and/or the E-Government Act will be handled in full accordance with all GSA rules of conduct and in accordance with GSA Privacy Program requirements.

PII (should it come into scope) will require that the vendor's cloud solution be FedRAMP authorized at least at the FIPS PUB 199 Moderate level.

5.7.3 Data Availability

The data must be available to the Government upon request within one business day or within the timeframe negotiated with the Contractor, and shall not be used for any other purpose other than that specified herein. The contractor shall provide requested data at no additional cost to the government.

5.7.4 Data Release

Any information made available to the Contractor by the Government shall be used only for the purpose of carrying out the provisions of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of the contract. In performance of this contract, the Contractor assumes responsibility for protection of the confidentiality of Government records and shall ensure that all work performed by its subcontractors shall be under the supervision of the Contractor or the Contractor's

responsible employees. Each officer or employee of the Contractor or any of its subcontractors to whom any Government record may be made available or disclosed shall be notified in writing by the Contractor that information disclosed to such officer or employee can be used only for that purpose and to the extent authorized herein. Further disclosure of any such information, by any means, for a purpose or to an extent unauthorized herein, may subject the offender to criminal sanctions imposed by 18 U.S.C. §§ 1030.

Contractor will not disclose Customer Data to any government or third party or access or use Customer Data; except in each case as necessary to maintain the Cloud Services or to provide the Cloud Services to Customer in accordance with this contract, or as necessary to comply with the law or a valid and binding order of a governmental or regulatory body (such as a subpoena or court order). Unless it would be in violation of a court order or other legal requirement, Contractor will give Government reasonable notice of any such legal requirement or order, to allow Government to seek a protective order or other appropriate remedy.

5.8 Data Ownership

All Government data collected in the system is the property of the Federal Government. All data collected by the system shall be provided by the Contractor (system provider) as requested during the contract period and at the completion of the contract period.

5.9 Confidentiality and Nondisclosure

Personnel working on any of the described tasks, may at Government request, be required to sign formal non-disclosure and/or conflict of interest agreements to guarantee the protection and integrity of Government information and documents.

Additionally, any information made available to the Contractor by the Government shall be used only for the purpose of carrying out the provisions of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of the contract. In performance of this contract, the Contractor assumes responsibility for protection of the confidentiality of Government records and shall ensure that all work performed by its subcontractors shall be under the supervision of the Contractor or the Contractor's responsible employees. Each officer or employee of the Contractor or any of its subcontractors to whom any Government record may be made available or disclosed shall be notified in writing by the Contractor that information disclosed to such officer or employee can be used only for that purpose and to the extent authorized herein. Further disclosure of any such information, by any means, for a purpose or to an extent unauthorized herein, may subject the offender to criminal sanctions imposed by 18 U.S.C. §§ 1030.

5.10 GSA Non-Disclosure Agreement

Each individual contractor/subcontractor employee who performs work on this contract is required to sign an Employee Non-Disclosure Agreement. The Contractor shall submit to the

COR a completed confidentiality and non-disclosure agreement form for each individual contractor/subcontractor.

The Contractor and all contractor/subcontractor employees may have access to sensitive data, proprietary, or confidential business information of other companies or the Government in the course of performing official duties on this contract. The term "proprietary information" means any information considered so valuable by its owners that it is held in secret by them and their licensees and is not available to the public.

All information that is (1) obtained related to or derived from this contract, and (2) results from or derived from any actual tasks assigned to contractor employees while participating on this contract is considered proprietary.

The Contractor and all contractor/subcontractor employees will not use vendor proprietary information except as necessary to perform this contract, and shall agree not to disclose such information to third parties, including any employee of the contractor/subcontractor who has not executed this nondisclosure agreement, or use such information in any manner inconsistent with the purpose for which it was obtained. Anyone failing to comply with the agreement may be subject to disciplinary action or termination of employment by the contractor/subcontractor, and possible administrative, civil, or criminal penalties.

5.11 Additional Stipulations

1. Deliverables shall be labeled Sensitive But Unclassified (SBU) or contractor selected designation per document sensitivity. External transmission/dissemination of SBU to or from a Government computer must be encrypted. Certified encryption modules must be used in accordance with FIPS PUB 140-2, *"Security Requirements for Cryptographic Modules."*
2. The Contractor shall certify applications are fully functional and operate correctly as intended on systems using the United States Government Configuration Baseline (USGCB). This includes Internet Explorer configured to operate on Windows. The standard installation, operation, maintenance, update, and/or patching of software shall not alter the configuration settings from the approved USGCB configuration. The information technology should also use the Windows Installer Service for installation to the default "program files" directory and should be able to silently install and uninstall. Applications designed for normal end users shall run in the standard user context without elevated system administration privileges. The contractor shall use Security Content Automation Protocol (SCAP) validated tools with USGCB Scanner capability to certify their products operate correctly with USGCB configurations and do not alter USGCB settings.
3. The contractor shall cooperate in good faith in defining non-disclosure agreements that other third parties must sign when acting as the Federal government's agent.
4. The contractor shall comply with any additional FedRAMP privacy requirements.

5. The Government has the right to perform manual or automated audits, scans, reviews, or other inspections of the vendor's IT environment being used to provide or facilitate services for the Government. The Contractor shall be responsible for the following privacy and security safeguards:
    a. The Contractor shall not publish or disclose in any manner, without the Contracting Officer's written consent, the details of any safeguards either designed or developed by the Contractor under this contract or otherwise provided by the Government. Exception - Disclosure to a Consumer Agency for purposes of A&A verification or to the MAX.Gov portal. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours of the request. Access to support incident investigations, shall be provided as soon as possible but not longer than 72 hours after request.
    b. Physical Access Considerations – If the SaaS provider is operated within an IaaS that is FedRAMP authorized (e.g., AWS); physical access to the physical datacenter environment will be governed by the terms of access allowed by the underlying infrastructure provider as defined in the FedRAMP A&A authorization package.
    c. The program of inspection shall include, but is not limited to:
        - Authenticated and unauthenticated operating system/network vulnerability scans
        - Authenticated and unauthenticated web application vulnerability scans
        - Authenticated and unauthenticated database application vulnerability scans
        - Automated scans can be performed by Government personnel, or agents acting on behalf of the Government, using Government operated equipment, and Government specified tools. If the vendor chooses to run its own automated scans or audits, results from these scans may at the Government's discretion, be accepted in lieu of Government performed vulnerability scans. In these cases, scanning tools and their configuration shall be approved by the Government. In addition, the results of vendor-conducted scans shall be provided in full to the Government.
    d. If new or unanticipated threats or hazards are discovered by either the Government or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.
6. The Contractor shall comply with Section 1634 of Public Law 115-91 that prohibits use of any hardware, software, or services developed or provided, in whole or in part, by— (1)

Kaspersky Lab (or any successor entity); (2) any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or (3) any entity of which Kaspersky Lab has majority ownership.

5.12 References

Guide to Understanding FedRAMP

FedRAMP Cloud Computing Documents

FedRAMP Templates

6 Mobile Application - IT Security and Privacy Requirements

The contractor shall generally, substantially, and in good faith follow GSA IT Security Policy and Guidelines including GSA Order CIO 2100.1, "*GSA Information Technology (IT) Security Policy"* and GSA IT Security Procedural Guide 12-67, "*Securing Mobile Devices and Applications,*" or current versions. In situations where there are no procedural guides, the contractor shall use generally accepted industry best practices for IT security.

6.1 General Mobile Application Guidelines

1. The Mobile Application (App) shall be integrated with a Mobile Device Management (MDM) solution. GSA currently uses MAAS 360.
2. The contractor shall provide to the GSA IT Contracting Officer Representative (COR) the source code and all supporting artifacts of the app for security testing via the GSA Static and mobile Code Scanning program. In addition, the contractor shall actively participate in the program to remediate all findings according to the most recent Static Code Scanning Standard Operating Procedure (SOP) before the beta and production App is accepted by GSA. Once the contract is awarded, GSA will provide a copy of the Static Code Scanning SOP to the contractor.
3. The contractor shall provide clear and concise documentation so that future developers and programmers can understand the processes used and are able to enhance, edit or build upon the original App. All source code information prepared for this App is the property of GSA, Federal Acquisition Service, OCCM and GSA IT.
    - The contractor shall provide detailed process and code documentation.
    - The contractor shall provide App features documentation.
    - The contractor shall support development and updates of a security authorization package for the App following the process requirements documented in GSA IT Security Procedural Guide 12-67, "*Securing Mobile Devices and Applications,"* or current version.

6.2 Mobile Device Security

The contractor shall adhere to the following requirements and guidelines for developing mobile applications. All requirements and guidelines are found in the GSA IT Security Procedural Guide 12-67, "*Securing Mobile Devices and Applications,"* which will be provided upon contract award.

A mobile application, most commonly referred to as an app, is a type of application software designed to run on a mobile device, such as a smartphone or tablet computer. Mobile applications frequently serve to provide users with similar services to those accessed on PCs. Apps are generally small, individual software units with limited capabilities and isolated functionality. The simplest apps are developed to utilize the web browser of the mobile device to provide a feature set integration much like what is found on a user's PC. However, as mobile

app development has grown, a more sophisticated approach involves developing applications specifically for the mobile environment, taking advantage of both its limitations and advantages. For example, apps that use location-based features are inherently built from the ground up with an eye to mobile devices given that you do not have the same concept of location on a PC. With this new paradigm in both mobile platforms and the applications loaded on them, GSA will concentrate security focus on the following goals:

- That all apps loaded have an initial assessment by GSA for acceptability and then a security assessment & authorization, when required
- That all apps are deployed from only trusted sources, following their security/assessment process – This presently is the Apple ITunes store for iOS and the Google Play store for Android. MaaS360 may also be used, once retrieved from these sources, for enterprise deployment
- That Terms of Service (ToS) discipline is adhered to, based on acceptability of an app – either as an individual user or for GSA as an Agency
- That apps deemed to be unacceptable are blacklisted, using MaaS360
- That a mobile app inventory for all devices be maintained
- That GSA developed apps are assessed, evaluated and approved by the AO for the system they support before deployment

6.3 Application Sources

Allowing mobile apps to be loaded from an unknown source presents one of the greatest risks to GSA's environment when using mobile devices. "Side loading" of apps is a process where a user installs an application from a source other than the Apple ITunes store or Google Play store. If a user jailbreaks a device, side loading can occur as well. Jailbreaking, or rooting, is a process where an Operating System (OS) of a mobile device grants a user or application root level access to the OS. While iOS devices that are not jailbroken/rooted protect against sideloading, the Android OS allows a user to turn such protection on/off (allow unknown sources) if not managed by MDM.

As such, the following policies apply to all GSA devices (Government and Bring Your Own Device) used in the environment to protect against side loading of apps:

- Devices shall not be jailbroken/rooted by users or apps loaded by users. GSA's MDM solution shall immediately notify an administrator of all such incidents immediately for remediation.
- Unknown sources shall not be enabled by users or applications. GSA's MDM solution shall immediately notify an administrator of all such incidents for remediation.
- GSA developed apps may be sideloaded for testing purposes only on test devices, but production deployment of GSA developed apps may only be done via the policies outlined below for Apple iOS and Google Android.

The GSA MaaS store may be employed for enterprise deployments, but only after the app has undergone the review/approval processes outlined below:

- Apple App Review guidelines
- Google Play Store Developer Policy Center

6.4 Terms of Service (ToS)

Many terms found in commercial TOS or End User License Agreements (EULA) are not acceptable when the Government is the end user. Office of Chief Information Officer (OCIO) requires that software and services within the GSA Enterprise have approved ToS or EULA.

Apps deemed to be acceptable are loaded at the discretion of the user for either personal use or as a personal productivity tool to further enhance the work experience. As such, use of the App is not mandated by the agency. Therefore, acceptance of the ToS falls upon the user as an individual. This is true even if the App is loaded using a GSA.gov domain account or registered with a user's GSA.gov email address.

Apps that are approved after formal assessment: and include a formal review by GSA Counsel as part of the review/approval process, where the ToS was found to be acceptable to the government or a modified ToS was negotiated as part of the approval review, prior to final authorization. When loaded and activated, the user is accepting the ToS (often a technical function required of the user), not as an individual, but as an employee or contract employee assigned to perform work functions for GSA.

6.5 GSA Privacy Requirements

Personally identifiable information (PII) **<SELECT: is or is not>** in the scope of the acquisition and PII **<SELECT: is or is not>** expected to be stored, processed, or transmitted in the vendor's App. The collection, maintenance or dissemination of any PII that is subject to the Privacy Act and/or the E-Government Act will be handled in full accordance with all GSA rules of conduct and in accordance with GSA Privacy Program requirements.

The contractor shall prepare a Privacy Threshold Analysis (PTA) to confirm and document PII is not in scope, or to determine which categories of information will be stored, processed, or transmitted by the App. The PTA must be completed before development begins and whenever a change with privacy impact (e.g., a new category of information is collected) is made to an existing App. PTAs are required to determine whether a Privacy Impact Assessment (PIA) and/or a System of Records Notice (SORN) is required, and if any other privacy requirements apply to the App. Instructions for the PTA and PIA forms can be found at https://www.gsa.gov/reference/gsa-privacy-program/privacy-impact-assessments-pia.

PII (should it come into scope) will require the following guidelines be adhered to.

- The vendor's App must be authorized at least at the FIPS PUB 199 Moderate level.
- For any system that collects, maintains or disseminates PII, a PIA must be completed by the contractor and provided to the GSA Privacy Office for review along with the other authorization to operate (ATO) documents.

- If the system retrieves information using PII, the Privacy Act applies and it must have a system of records notice (SORN) published in the Federal Register.
- If PII is collected from individuals by the system, a Privacy Act Statement (i.e., Privacy Notice) must be provided to users prior to their use of the application on what data is being collected and why, as well as the authority for the collection and the impact of not providing some or all of it. The Privacy Act Statement must be available to the individual directly on the form used to collect the information. Providing a link back to the Statement from the form is acceptable.

Provided below is a template for an acceptable Privacy Act Statement when bracketed sections are completed. A completed example is available at https://www.gsa.gov/reference/gsa-privacy-program/privacy-act-statement-for-design-research.

Privacy Act Statement

This (insert voluntary or mandatory) collection of personal information is authorized by (insert legal authority). We collect (developer insert categories of PII collected, e.g. name, email, etc.). Your personal information is collected so we can (developer insert purpose of collection and what effect on the individual, if any, not providing any or all of the information may have). Your personal information is stored in (developer insert App name). GSA may use this information pursuant to its published Privacy Act system of records notice (insert link to applicable GSA Privacy Act SORN).

Note: Apps that access data a user creates must assume a user may include privacy data/PII in the application unless the data creation is restricted to data controlled by the App.

All contractor staff who have significant privacy information responsibilities must complete GSA's specialized Privacy 201 Training. This includes contractors who work with PII as part of their work duties (e.g.; Human Resource staff, Finance staff, and managers/supervisors).

6.6 GSA App Development, Assessment, Authorization and Deployment

GSA developed apps are designed to take advantage of the concept of Anytime, Any Where, Any Device (A3) to allow GSA users and customers to access GSA data while mobile. As such, as GSA business lines develop apps for use on the iOS and Android environment, these apps must undergo an assessment and authorization process before being deployed. With that in mind, the following guidelines are to be followed:

- A GSA developed app that supports a GSA FISMA system must be documented in the System Security Plan and authorized to operate as part of a current ATO letter from the respective AO before deployment. GSA IT Security Procedural Guide 06-30, *"Managing Enterprise Risk,"* is to be followed for this process. Any app that is not directly tied to an already existing system authorized to operate must have an assessment performed and subsequently approved for release by the Chief Information Security Officer (CISO).

- Any mobile app development shall result in a minimum of the release of both an iOS and Android version of the app. This ensures coverage to all users within GSA and the maximum coverage for apps released to the public. Any additional application versions for alternate OS mobile platforms may be developed for such apps, but iOS and Android shall remain as the core base OS' for GSA developed mobile apps for all releases.
- All GSA developed apps must follow the respective application review and publication guidelines for the OS to which they were developed as outlined in Section 8.2 of GSA IT Security Procedural Guide 12-67, "*Securing Mobile Devices and Applications"* and the release process documented in this section.
- Other than for testing purposes on non-user provisioned mobile devices, side loading of apps in the environment is not authorized.
- The GSA MaaS360 Store is authorized for enterprise deployment of apps to GSA user devices once that app has been assessed, authorized, and published according to the guidelines outlined in this section.
- Mobile code scanning throughout the development cycle is critical, but before release by the Mobile Device Team, a mobile app must be scanned by the Systems Engineering Division (ISE) Team within the OCISO. This scan is a source code scan using the CheckMarx platform. As with all applications in GSA, no High/Critical findings are allowed from these scan results. Moderate findings should be documented in the respective POA&M for the system by which the app is authorized and accepted by the AO; Low and Informational findings should be taken into consideration by the developers for their next iteration of app development. A detailed process for mobile app release is documented at the end of this section.
- All mobile application development should take into consideration the Open Web Application Security Project (OWASP) Mobile Security Project when developing mobile apps either within GSA or for use by the general public. The guidelines for developing OWASP is outlined below:
  - OWASP Mobile Security Testing Guide
  - OWASP Mobile Security Project Home Page
  - OWASP Security Testing Guidelines for Mobile Apps
- GSA developed mobile apps must undergo an assessment review and approval process before being released for use. These apps fall into two categories that shall have slightly different processes for approval, with many common steps.
- Mobile apps that are developed as part of another system with a current ATO and provide access to an application using a different form factor (smartphones/tablets), such apps must be documented in the System Security Plan for the system they support.
- Mobile apps designed for a specific purpose not part of a current ATO stand alone in their ATO. As these apps do not have a parent system they support, the below listed process is the complete assessment process required for these apps.

All apps must follow the approval processes outlined below:

1. Apps must be scanned prior to release by the GSA Office of the CISO using the Checkmarx Application scanner. No Critical/High findings may remain for approval to be received and any moderate/medium findings must be contained in a POA&M, either for the system the app is a part of, or a separate POA&M if a standalone mobile app.
2. The privacy requirements as stated above must be met.
3. A mobile application security assessment review in accordance with the GSA-IT Procedural Guide: CIO-IT Security-12-67, "*Securing Mobile Devices and Applications*" must be completed and signed by the mobile App owner, mobile App assessor, mobile App Information System Security Manager (ISSM), a representative of the Office of the CSIO, to denote a proper assessment and review was conducted of the mobile app prior to release.

6.7 Intellectual Property

This task order is funded by the United States Government. All intellectual property generated and/or delivered pursuant to this Firm-Fixed Price Statement of Work will be subject to appropriate federal acquisition regulations which entitle the Government to unlimited license rights in technical data and computer software developed exclusively with Government funds, a nonexclusive "paid-up" license to practice any patentable invention or discovery made during the performance of this task order, and a "paid-up" nonexclusive and irrevocable worldwide license to reproduce all works (including technical and scientific articles) produced during this task order.

6.8 Confidentiality and Nondisclosure

The preliminary and final deliverables and all associated working papers and other material deemed relevant by the agency that have been generated by the contractor in the performance of this contract, are the property of the U.S. Government and must be submitted to the COR at the conclusion of the contract. The U.S. Government has unlimited data rights to all deliverables and associated working papers and materials.

All documents produced for this project are the property of the U.S. Government and cannot be reproduced or retained by the contractor. All appropriate project documentation will be given to the agency during and at the end of this contract. The contractor shall not release any information without the written consent of the Contracting Officer.

Personnel working on any of the described tasks may, at Government request, be required to sign formal non-disclosure and/or conflict of interest agreements to guarantee the protection and integrity of Government information and documents.

Additionally, any information made available to the Contractor by the Government shall be used only for the purpose of carrying out the provisions of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the

performance of the contract. In performance of this contract, the Contractor assumes responsibility for protection of the confidentiality of Government records and shall ensure that all work performed by its subcontractors shall be under the supervision of the Contractor or the Contractor's responsible employees. Each officer or employee of the Contractor or any of its subcontractors to whom any Government record may be made available or disclosed shall be notified in writing by the Contractor that information disclosed to such officer or employee can be used only for that purpose and to the extent authorized herein. Further disclosure of any such information, by any means, for a purpose or to an extent unauthorized herein, may subject the offender to criminal sanctions imposed by 18 U.S.C. §§ 1030.

6.9 GSA Non-Disclosure Agreement

Each individual contractor/subcontractor employee who performs work on this contract is required to sign an Employee Non-Disclosure Agreement. The Contractor shall submit to the COR a completed confidentiality and non-disclosure agreement form for each individual contractor/subcontractor.

The Contractor and all contractor/subcontractor employees may have access to sensitive data, proprietary, or confidential business information of other companies or the Government in the course of performing official duties on this contract. The term "proprietary information" means any information considered so valuable by its owners that it is held in secret by them and their licensees and is not available to the public.

All information that is (1) obtained related to or derived from this contract, and (2) results from or derived from any actual tasks assigned to contractor employees while participating on this contract is considered proprietary.

The Contractor and all contractor/subcontractor employees will not use vendor proprietary information except as necessary to perform this contract, and shall agree not to disclose such information to third parties, including any employee of the contractor/subcontractor who has not executed this nondisclosure agreement, or use such information in any manner inconsistent with the purpose for which it was obtained. Anyone failing to comply with the agreement may be subject to disciplinary action or termination of employment by the contractor/subcontractor, and possible administrative, civil, or criminal penalties.

6.10 Personnel Security Requirements

Contractor shall furnish documentation reflecting favorable adjudication of background investigations for all personnel (including subcontractors) supporting the system. Contractors shall comply with GSA Order 2100.1 – "*GSA Information Technology (IT) Security Policy"* and GSA Order CIO P 2181.1 – "*HSPD-12 Personal Identity Verification and Credentialing Handbook*." GSA separates the risk levels for personnel working on Federal computer systems into three categories: Low Risk, Moderate Risk, and High Risk.

- Those contract personnel (hereafter known as "Applicant") determined to be in a Low Risk position will require a National Agency Check with Written Inquiries (NACI) investigation.
- Those Applicants determined to be in a Moderate Risk position will require either a Limited Background Investigation (LBI) or a Minimum Background Investigation (MBI) based on the Contracting Officer's (CO) determination.
- Those Applicants determined to be in a High Risk position will require a Background Investigation (BI).

Applicants will not be reinvestigated if a prior favorable adjudication is on file with FPS or GSA, there has been less than a one year break in service, and the position is identified at the same or lower risk level.

Once a favorable FBI Criminal History Check (Fingerprint Check) has been returned, Applicants may receive a GSA identity credential (if required) and initial access to GSA information systems. The HSPD-12 Handbook contains procedures for obtaining identity credentials and access to GSA information systems as well as procedures to be followed in case of unfavorable adjudications.

GSA shall sponsor the investigation when deemed necessary. No access shall be given to government computer information systems and government sensitive information without a background investigation being verified or in process. If results of background investigation are not acceptable, then access shall be terminated.

The Contractor shall provide a report of separated staff on a monthly basis, beginning 60 days after execution of the option period.

6.11 Additional Stipulations

1. Deliverables shall be labeled Sensitive But Unclassified (SBU) or contractor selected designation per document sensitivity. External transmission/dissemination of SBU to or from a Government computer must be encrypted. Certified encryption modules must be used in accordance with FIPS PUB 140-2, *"Security requirements for Cryptographic Modules."*
2. The Contractor shall certify applications are fully functional and operate correctly as intended on systems using the United States Government Configuration Baseline (USGCB). This includes Internet Explorer configured to operate on Windows. The standard installation, operation, maintenance, update, and/or patching of software shall not alter the configuration settings from the approved USGCB configuration. The information technology should also use the Windows Installer Service for installation to the default "program files" directory and should be able to silently install and uninstall. Applications designed for normal end users shall run in the standard user context without elevated system administration privileges. The contractor shall use Security

Content Automation Protocol (SCAP) validated tools with USGCB Scanner capability to certify their products operate correctly with USGCB configurations and do not alter USGCB settings.

3. The Contractor shall cooperate in good faith in defining non-disclosure agreements that other third parties must sign when acting as the Federal government's agent.
4. The Government has the right to perform manual or automated audits, scans, reviews, or other inspections of the vendor's IT environment being used to provide or facilitate services for the Government. The Contractor shall be responsible for the following privacy and security safeguards:
    a. The Contractor shall not publish or disclose in any manner, without the Contracting Officer's written consent, the details of any safeguards either designed or developed by the Contractor under this contract or otherwise provided by the Government. Exception - Disclosure to a Consumer Agency for purposes of A&A verification or to the MAX.Gov portal. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours of the request. Access to support incident investigations, shall be provided as soon as possible but not longer than 72 hours after request.

        The program of inspection shall include, but is not limited to:

        - Authenticated and unauthenticated operating system/network vulnerability scans
        - Authenticated and unauthenticated web application vulnerability scans
        - Authenticated and unauthenticated database application vulnerability scans
        - Automated scans can be performed by Government personnel, or agents acting on behalf of the Government, using Government operated equipment, and Government specified tools. If the vendor chooses to run its own automated scans or audits, results from these scans may at the Government's discretion, be accepted in lieu of Government performed vulnerability scans. In these cases, scanning tools and their configuration shall be approved by the Government. In addition, the results of vendor-conducted scans shall be provided in full to the Government.

    b. If new or unanticipated threats or hazards are discovered by either the Government or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.

5. The Contractor shall comply with Section 1634 of Public Law 115-91 that prohibits use of any hardware, software, or services developed or provided, in whole or in part, by— (1) Kaspersky Lab (or any successor entity); (2) any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or (3) any entity of which Kaspersky Lab has majority ownership.

Appendix A: GSA Tailoring of NIST 800-53 Controls

The GSA Control Tailoring Workbook contains GSA defined values for NIST SP 800-53 Security and Privacy Controls. The workbook is not publicly available; contact the contracting officer who will coordinate with the GSA Office of the Chief Information Security Officer to determine if it can be made available.

1.1 SAM Integration Environment SLA Measures

1.1.1 Measure #1: Help Desk Outstanding Ticket Age

Performance Requirement:	Help Desk Outstanding Ticket Age
Acceptable Quality Level (AQL):	**Less than 10% of all Tier 2 open tickets open are more than 30 days old**
Data Source:	The Help Desk Tracking Tool
How It Is Measured:	Number of tickets older than 30 days divided by the total ticket number of tickets escalated to Tier 2 in the period.
Approach for Achieving:	Tickets are reviewed daily by the Help Desk Lead. These are addressed on a first in first out basis. When it is determined that tickets open tickets are growing in age, the Help Desk lead will evaluate root causes and shift focus on the oldest tickets.
Data Accessibility:	GSA providing IBM the ability to have access to the help desk tool data for actual escalation time and date.
Restrictions:	Escalations from Tier 1 to Tier 2 must be at 10% or below. Tickets that have dependencies on Tier 3 or external agencies will not be counted. Reports containing metrics related to this metric will be provided to IBM by the third-party tool owner. System defects and enhancements that prevent closure of the ticket will not be counted since this is not a reflection of the Help Desk effectiveness.
Owner:	Help Desk Lead

Pass Example: Current open ticket count as of the end of the month is 1,000. There are 70 tickets determined to be older than 30 days. Therefore 70/1000 = 7%

1.1.2 Measure #2: Help Desk Ticket Closure Rate

Performance Requirement:	Help Desk Ticket Closure Rate
Acceptable Quality Level (AQL):	**More than 90% of the total tickets escalated to Tier 2 over the last 30 days have been closed**
Data Source:	The Help Desk Tracking Tool
How It Is Measured:	Number of tickets closed in a month divided by the number of tickets escalated to Tier 2
Approach for Achieving:	The Help Desk Lead will assign resources, so ticket closure rate stays close to the number of those escalated to Tier 2. This is to ensure that open ticket counts do not increase over time.
Data Accessibility:	GSA providing IBM the ability to have access to the help desk tool data for actual escalation time and date.

Restrictions:	Escalations from Tier 1 to Tier 2 must be at 10% or below. Reports containing metrics related to this metric will be provided to IBM by the third-party tool owner.
Owner:	Help Desk Lead

Pass Example: Throughout the course of the month, there were 3,000 help desk tickets escalated to Tier 2 help desk. Within the same period, 2,880 help desk tickets were closed. Therefore 2,880/3,000 = 96%

1.1.3 Measure #3: Help Desk Tickets Closed the Same Day

Performance Requirement:	Help Desk Tickets Closed the Same Day
Acceptable Quality Level (AQL):	**More than 30% of Tier 2 tickets closed within 72 hours**
Data Source:	The Help Desk Tracking Tool
How It Is Measured:	Number of monthly total tickets escalated to Tier 2 that are closed within 72 hours. The time starts when the ticket is placed in the Tier 2 queue and closed when set to 'Pending Customer'
Approach for Achieving:	Once a ticket is escalated and verified by the Help Desk lead as a properly escalated ticket, it is assigned to a Tier 2 agent. The agent will research the issue, provide a resolution and move the ticket to Pending Customer who has three days to respond before it is closed.
Data Accessibility:	GSA providing IBM the ability to have access to the help desk tool data for actual escalation time and date.
Restriction:	Escalations from Tier 1 to Tier 2 must be at 10% or below. Tickets that have dependencies on Tier 3 or external agencies will not be counted. Reports containing metrics related to this metric will be provided to IBM by the third-party tool owner. System defects and enhancements that prevent closure of the ticket will not be counted since this is not a reflection of the Help Desk effectiveness.
Owner:	Help Desk Lead

Pass Example: Throughout the course of the month, there were 3,000 help desk tickets escalated to Tier 2 help desk. Within the period, there were 1,200 tickets that were closed within 72 hours. Therefore 1,200/3,000 = 40%

1.1.4 Measure #4: Help Desk Average Tier 2 Technical Initial Review Time

Performance Requirement:	Help Desk Average Initial Review Time
Acceptable Quality Level (AQL):	**Less than 3 (business days)**
Data Source:	The Help Desk Tracking Tool

How It Is Measured:	Determined from the time a Tier 2 ticket is escalated to the time is initially reviewed and the user has been contacted. (Business Days). IBM receives a document every week that measures the time it takes for Tier 2 agent to respond to a user after FSD has escalated the item.
Approach for Achieving:	Once a ticket is escalated to Tier 2 Technical, a Tier 2 agent should assign the ticket to themselves and contact the user immediately.
Data Accessibility:	GSA providing IBM the ability to have access to the help desk tool data for actual escalation time and date.
Restriction:	Escalations from Tier 1 to Tier 2 must be at 10% or below. Tickets that have dependencies on Tier 3 or external agencies will not be counted. Reports containing metrics related to this metric will be provided to IBM by the third-party tool owner. System defects and enhancements that prevent closure of the ticket will not be counted since this is not a reflection of the Help Desk effectiveness.
Owner:	Help Desk Lead

1.1.5 Measure #5: Help Desk Average Tier 2 Close Time

Performance Requirement:	Help Desk Average Tier 2 Close Time
Acceptable Quality Level (AQL):	**Less than 5 (business days)**
Data Source:	The Help Desk Tracking Tool
How It Is Measured:	Determined from the time a Tier 2 ticket is escalated to the time it is closed. (Business Days)
Approach for Achieving:	Once a ticket is escalated and verified by the Help Desk lead as a properly escalated ticket, it is assigned to a Tier 2 agent. The agent will research the issue, provide a resolution and move the ticket to Pending Customer who has three days to respond before it is closed
Data Accessibility:	GSA providing IBM the ability to have access to the help desk tool data for actual escalation time and date.
Restriction:	Escalations from Tier 1 to Tier 2 must be at 10% or below. Tickets that have dependencies on Tier 3 or external agencies will not be counted. Reports containing metrics related to this metric will be provided to IBM by the third-party tool owner. System defects and enhancements that prevent closure of the ticket will not be counted since this is not a reflection of the Help Desk effectiveness.
Owner:	Help Desk Lead

1.1.6 Measure #6: Help Desk Reopened Tier 2 Technical Tickets

Performance Requirement:	Reopened Tier 2 Technical Tickets
Acceptable Quality Level (AQL):	**Less than 5% Reopened**
Data Source:	The Help Desk Tracking Tool
How It Is Measured:	Tickets that were moved to resolved but reopened by the user because issue was not resolved. Service Now has a tool that allows you to see if any tickets were reopened during a period of time selected.
Approach for Achieving:	Tier 2 Technical Agents should not close any help desk tickets until they have verified with the user that the issue is resolved.
Data Accessibility:	GSA providing IBM the ability to have access to the help desk tool data for actual escalation time and date.
Restriction:	Escalations from Tier 1 to Tier 2 must be at 10% or below. Tickets that have dependencies on Tier 3 or external agencies will not be counted. Reports containing metrics related to this metric will be provided to IBM by the third-party tool owner. System defects and enhancements that prevent closure of the ticket will not be counted since this is not a reflection of the Help Desk effectiveness.
Owner:	Help Desk Lead

1.1.7 Measure #7: Help Desk Foreign Registrant Tickets

Performance Requirement:	Help Desk Foreign Registrant Tickets
Acceptable Quality Level (AQL):	**Less than 25% of all Tier 2 Tickets are Foreign**
Data Source:	The Help Desk Tracking Tool
How It Is Measured:	Total count of Tier 2 tickets opened regarding foreign registrations
Approach for Achieving:	IBM maintains effective monitoring of the help desk queue, so issues reported by foreign registrations can be investigated immediately so other foreign entities do not experience the same issues.
Data Accessibility:	GSA providing IBM the ability to have access to the help desk tool data for actual escalation time and date.

Restriction:	Escalations from Tier 1 to Tier 2 must be at 10% or below. Tickets that have dependencies on Tier 3 or external agencies will not be counted. Reports containing metrics related to this metric will be provided to IBM by the third-party tool owner. System defects and enhancements that prevent closure of the ticket will not be counted since this is not a reflection of the Help Desk effectiveness.
Owner:	Help Desk Lead

1.1.8 Measure #8: Reputation – Number of Reputation Incidents

Performance Requirement:	Number of Reputation Incidents
Acceptable Quality Level (AQL):	**Zero**
Data Source:	Stakeholder manual identification
How It Is Measured:	A reputation incident is one in which unapproved content is displayed on a production website, generally referred to as defacement. Defacement incidents are tracked across the environment as a whole (defacement of any website or component is treated the same). This is a yes/no metric. Time to recover from defacement contributes to unavailability calculations.
Approach for Achieving:	The IBM team continually strives to support GSA and its stakeholders to be successful. Activities outlined in the QCP support the quality efforts which include process controls, auditing, testing defect identification and defect correction. The integrity of all the AOCS systems is highly visible and any disruption or negative event can result in erosion of GSA's reputation.
Data Accessibility:	Incorrect data displayed on the website as result of a system issue where approved specification (data, functional or security) is not met. This is exclusive of extracts which fall under data quality. Data displayed as user entered or interfaced from another system will not be considered.
Restriction:	Agreement to reputation events will involve concurrence from FAS, CIO, COR and the IBM team.
Owner:	All Team Members

1.1.9 Measure #9: Availability – Response Time

Performance Requirement:	Availability of www.sam.gov
Acceptable Quality Level (AQL):	**99.80%**

Data Source:	Rational Performance Test monitoring
FPDS Requirements:	Present a screen to users within 5 seconds Changes to the technical environment which may negatively impact data submission and/or reporting shall not be implemented between July and October
How It Is Measured:	Unavailable if system wide response takes longer than 5 seconds. Measured at the solution edge, net of scheduled maintenance. Calculated as the total hours of site availability per month divided by the total hours of a month. The site is considered unavailable when no external user is able to access the website.
Approach for Achieving:	The IBM team maintains the software and hardware of SAM. The hosting team continually monitors the servers and application for availability.
Data Accessibility:	Server and application monitoring tools are utilized to observe availability of the system.
Restriction:	Third party data center (hosting vendor) maintains 100% uptime.
Owner:	Hosting & Infrastructure Lead

Example: The AOCS systems were unavailable for 1 hour on 10/5/2013. Since there are 31 days in October and 24 hours in a day, the total possible available hours are 744.

743/744= 99.86% = Pass

1.1.10 Measure #11: Availability - Extracts

Performance Requirement:	Availability of Extracts
Acceptable Quality Level (AQL):	**99.80%**
Data Source:	Stakeholder manual identification
How It Is Measured:	All Extracts will be posted and accessible for the time period of the approved specification. Unavailable if active users are unable to access the posted extracts. Calculated as the total hours of available extracts per month divided by the total hours of a month.
Approach for Achieving:	The IBM team continually monitors the SAM extracts for availability. Extracts are posted daily and undergo a quality control process of review prior to posting. Posted extracts are audited periodically for availability.
Data Accessibility:	Server and application monitoring tools are utilized to observe availability of the system.
Restriction:	Third party data center (hosting vendor) maintains 100% uptime.
Owner:	Extracts & Interfaces Lead

Example: Extracts were unavailable for 1 hour on 10/5/2013. Since there are 31 days in October and 24 hours in a day, the total possible available hours are 744.

743/744= 99.86% = Pass

1.1.11 Measure #13: Availability – SAM Scheduled Maintenance

Performance Requirement:	Scheduled Maintenance
Acceptable Quality Level (AQL):	**Less than 16 Hours**
Data Source:	Hyperic Monitoring
Requirement:	System downtime (defined as the system is not accessible and operable by the user), will not exceed 8 hours per 12-month period (approximately 99.9% up time) exclusive of scheduled down time. Scheduled down time may occur not more frequently than once each month for a time period of up to 24 hours (noon Saturday to noon Sunday) with no scheduled down time during the month of September.
How It Is Measured:	Total scheduled downtime each month will not exceed 16 hours
Approach for Achieving:	IBM will request downtime at least 24 hours prior the maintenance window. Upon approval, the scheduled downtime will count towards the total available time for the month. The IBM team will work to minimize downtime by combining activities that require server reboot and therefore needing a scheduled maintenance window.
Data Accessibility:	Server and application monitoring tools are utilized to observe the activities of the system.
Restriction:	Unscheduled maintenance as a result of external agency failure in communication will not count against this metric. An example would be change in an external interface without prior notification resulting in the SAM servers requiring a reboot to resume normal operations. Exceptions must be approved by GSA.
Owner:	Hosting & Infrastructure Lead

1.1.12 Measure #14: Availability – Interface Availability

Performance Requirement:	Availability of Interfaces
Acceptable Quality Level (AQL):	**97.00%**
Data Source:	Hyperic Monitoring
How It Is Measured:	Agency critical interfaces run within an hour of specific execution time. Calculated as the total hours of Interface availability per month divided by the total hours of a month.

Approach for Achieving:	IBM maintains a Master Interface spreadsheet that lists out those interfaces. Each interface specification outlines the time in which the interface needs to run. If an interface does not run within an hour of the specified time, the monitoring team will report this as a miss and research the reason for the late delivery. The team will continue to implement process improvements to address the root causes
Data Accessibility:	Manual interface monitoring and use of Interface Tracking spreadsheet.
Restriction:	Third party data center (hosting vendor) maintains 100% uptime.
Owner:	Extracts & Interfaces Lead

There are 75 interfaces in total that SAM, maintains which are listed on the Interface Master List. If an interface is determined to not be operational, this is noted on the Interfaces Tracking Spreadsheet.

1.1.13 Measure #17: Business Process – Average Cycle Time

Performance Requirement:	A Record's Average Cycle Time
Acceptable Quality Level (AQL):	**7 Days or less**
Data Source:	Database Query
How It Is Measured:	The average time it takes a user to complete a registration and move from Draft to Active. The start time of a new or updated registration is captured by the system. The date and time in which a registration becomes active is also captured. All of the start times and activated times for a month are used calculate the average by using those records that were actually completed within the reporting period.
Approach for Achieving:	On a weekly basis, the IBM team provides a metric dashboard that contain the average cycle time. The team will continually look at ways in which reduction in cycle times can be achieved such as working with third party agencies to increase processing speed and performing maintenance on the application to expedite the user registration process.
Data Accessibility:	Database queries using PIT start and activation times.
Restriction:	IGT only registrations will be excluded as they are processed instantaneously. Pending CAGE or IRS will not exceed 7 days.
Owner:	Extracts & Interfaces Lead

1.1.14 Measure #18: Business Process – Interface Jobs - Extracts (Daily)

Performance Requirement:	Interface Job Extracts (Daily)

Acceptable Quality Level (AQL):	**Less than 8 hours**
Data Source:	Database Query
How It Is Measured:	The average time it takes to generate the daily extract file
Approach for Achieving:	Continuous 24/7 monitoring and sends out the alert emails to the concerned Interface POC's if the interface is taking longer than usual or fixing the bug before it hits the SLA
Data Accessibility:	Automated monitoring emails which sends out every day to the team about the status of the interfaces, documented in Interface monitoring document
Restriction:	Includes only entity profiles within the federal government for many functions, including, procurement, contracts, payments, size determination, and validation
Owner:	Extracts & Interfaces Lead

1.1.15 Measure #19: Business Process – Interface Jobs – Extracts (Monthly)

Performance Requirement:	Interface Job Extracts (Monthly)
Acceptable Quality Level (AQL):	**Less than 24 hours**
Data Source:	Database Query
How It Is Measured:	The average time it takes to generate the monthly extract file
Approach for Achieving:	Continuous 24/7 monitoring and sends out the alert emails to the concerned Interface POC's if the interface is taking longer than usual or fixing the bug before it hits the SLA
Data Accessibility:	Automated monitoring emails which sends out every day to the team about the status of the interfaces, documented in Interface monitoring document
Restriction:	Includes only entity profiles within the federal government for many functions, including, procurement, contracts, payments, size determination, and validation
Owner:	Extracts & Interfaces Lead

1.1.16 Measure #20: Business Process – Exclusions Created

Performance Requirement:	Exclusions Created via e-mail or upload
Acceptable Quality Level (AQL):	**Less than 24 hours**
Data Source:	Database Query
How It Is Measured:	The average time it takes to generate an exclusion.

Approach for Achieving:	Continuous 24/7 monitoring and sends out the alert emails to the concerned Interface POC's if the interface is taking longer than usual or fixing the bug before it hits the SLA
Data Accessibility:	Automated monitoring emails which sends out every day to the team about the status of the interfaces, documented in Interface monitoring document
Restriction:	Does not include exclusions entered in via the front end.
Owner:	Extracts & Interfaces Lead

1.1.17 Measure #21: Security - Outages due to security

Performance Requirement:	Outages due to security incidents (unplanned unavailability)
Acceptable Quality Level (AQL):	**No more than 1 outage per month**
Data Source:	Stakeholder manual identification
How It Is Measured:	Number of outages due to incidents (unplanned unavailability). Sam.gov is unavailable due to a security incident.
Approach for Achieving:	Continuous monitoring and improvements through vulnerability scanning and remediation, monthly patching, ongoing assessment and improvement of security controls through coordination with the ISSO and system owner
Data Accessibility:	Outages that are requested by GSA as a result of a formally defined security incident as outlined in IT Security Procedural Guide: Incident Response (IR) CIO-IT Security-01-02.
Restriction:	None
Owner:	Information Assurance Lead

1.1.18 Measure #22: Security - Security Risks and Controls

Performance Requirement:	Proportion of information security risks for which satisfactory controls have been fully implemented
Acceptable Quality Level (AQL):	**90% deployed IAW approved schedule**
Data Source:	Stakeholder manual identification
How It Is Measured:	Security Related Items Identified on the POA&M have a plan of action and are remediated in the appropriate timeframe.
Approach for Achieving:	GSA and IBM will follow the Security Plan process of process of scanning and identifying potential vulnerabilities in the.gov applications.

Data Accessibility:	Plan of Action and Milestone (POA&M) report provided by GSA. As defined in the security requirements, all High POA&Ms are to be remediated within 30 days of being identified as a POA&M.
Restriction:	GSA will provide IBM monthly updates to content within the POA&M for SLA reporting. Pending or approved AoRs may override the POA&M requirement and therefore will not be counted. POA&M items may be approved by GSA to be completed in accordance with a scheduled maintenance window or FastPath or Quarterly release that is outside of the 30-day window. These approved items will not be included in the calculation. Exceptions beyond 30 days for remediation due to planned release scheduling must be approved by GSA.
Owner:	Information Assurance Lead

Example: There were 20 POA&Ms identified in a month by GSA. 18 have been addressed within 30 days. 18/20 = 90% = Pass.

1.1.19 Measure #23: Security - Security Reporting Timeliness

Performance Requirement:	Time lag between detection, reporting and acting upon security incidents
Acceptable Quality Level (AQL):	**At least 90% of incidents addressed per response table**
Data Source:	Stakeholder manual identification
How It Is Measured:	Security incidents are responded to in the timeframes identified in current Incident Response Table
Approach for Achieving:	GSA and IBM will follow the Security Plan process of timely identification and reporting of security incidents. Weekly meetings between the GSA ISSO and IBM Information Assurance Lead will review any open security incidents.
Data Accessibility:	GSA ISSO to maintain and provide agreed upon incident response table.
Restriction:	GSA to provide IBM the Incident Response Table
Owner:	Information Assurance Lead

1.1.20 Measure #24: Data Quality - Data Stewardship Quality Index

Performance Requirement:	Data Stewardship Quality Index
Acceptable Quality Level (AQL):	**Average 99.8% across the relevant time period**
Data Source:	Stakeholder manual identification

How It Is Measured:	Quality of data as presented within extracts as indicated by the number of DUNS numbers with data defects.
Approach for Achieving:	Each month as the monthly extract files are generated, a quality check is conducted on the outputs against the criteria identified in the AOCS Data Quality plan
Data Accessibility:	Data element errors defined in the approved version of the Operational Data Quality Plan.
Restriction:	This will be measured on the monthly extract files. The daily files use the same data subsets and therefore are affected in the same manner as the monthly files.
Owner:	Extracts & Interfaces Lead

Example Pass Calculation:

Number of records in the file = 600,000

Number of DUNS with defects = 1,000

1,000/600,000 = .17 or 99.83%

Example Data Quality Report (The first row indicates a failed metric):

Date	Total Data Quality Issues	# of DUNS in File	Percent of Issues per DUNS	%
1/1/2015	1,200	500,000	0.24%	99.76%
2/1/2015	1,100	550,000	0.20%	99.80%
3/1/2015	1,000	600,000	0.17%	99.83%
4/1/2015	900	650,000	0.14%	99.86%
5/1/2015	800	700,000	0.11%	99.89%

Example of Data Quality threshold from the Operational Data Quality Plan:

#	Data Element	Validation Description	Showstopper	H/M/L	Threshold %
1	DUNS	Data Is Present - Make sure there are no blank values	Y	H	0.00%
2	DUNS	Length - Make sure all are 9 Characters	Y	H	0.00%
3	DUNS-PLUS4	Length - Make sure all are 4 Characters	Y	H	0.00%

1.1.21 Measure #25: Data Quality - Extract Provision & Reporting Timeliness

Performance Requirement:	Extract Provision Timeliness
Acceptable Quality Level (AQL):	**95% of Daily and Monthly extracts are posed on time within the month.**
Data Source:	Stakeholder manual identification
FPDS Requirements:	Provide capability to return online standard reports within 10 seconds exclusive of network transit time. For all reports, standard and ad hoc, that are less than 10,000 lines and there are no time-outs. For all reports, standard and ad hoc, over than 10,000 lines the time-out rate is not more than 5%.
How It Is Measured:	Total number of failed events across a month that extracts are late relative to the agreed calendar.
Approach for Achieving:	IBM maintains a master Interface spreadsheet that lists out those interfaces which generate extracts. Each extract interface specification outlines the time in which the file needs to be posted to SAM. If a file is not posted on time, the monitoring team will report this as a miss and research the reason for the late delivery. The team will continue to implement process improvements to address the root causes
Data Accessibility:	Agencies responsible for password access to secure folders.
Restriction:	Only Extracts listed at the time of approval of this document will be considered for this metric
Owner:	Extracts & Interfaces Lead

Example Pass Calculation: 10 files not posted on time = 396-10=386

386/396= 97%

Example Fail Calculation: 25 files not posted on time =396-25=371

371/396=94%

The list of Daily and Monthly Extracts:

#	Extract Name	Daily Tu-Sa	Monthly	Monthly First Sunday	Monthly 15th	Monthly Last Sunday	Once per FY
1	Legacy CCR FOUO 4082	X	X	X			
2	Legacy CCR FOUO 40822	X	X	X			
3	Legacy CCR MPIN	X	X	X			
4	Legacy CCR Proprietary 4082	X	X	X			
5	Legacy CCR Proprietary 40822	X	X	X			
6	Legacy CCR Sensitive 4082	X	X	X			
7	Legacy CCR Sensitive 40822	X	X	X			
8	Legacy CCR Complete 4082	X	X	X			
9	Legacy CCR Complete 40822	X	X	X			
10	Legacy CCR GSA Complete		X			X	
11	Legacy CCR FOIA		X		X		
12	Legacy FedReg Extract	X					
13	SAM Public Current! NOT bein osted due to D&B/GSA discussions	X	X	X			
14	SAM FOUO	X	X	X			
15	SAM Sensitive	X	X	X			
16	SAMS stem-On I	X	X	X			
17	SAM MPIN	X	X	X			
18	SAM FSRS	X	X	X			
19	SAM Re sand Certs osted unti I GSA testin is com lete		X	X			
20	SAM Exclusion Public Extract Fu II volume dail file	X					
		X					
22	Bio-Preferred Fiscal Year Report (Posted once per FY}						X

1.1.22 Measure #26: Data Quality - Extract Provision Consistency

Performance Requirement:	Extract Provision Consistency
Acceptable Quality Level (AQL):	**Less than 12 Extracts Missed per Year**
Data Source:	Stakeholder manual identification and interface monitoring
How It Is Measured:	Number of times on which the **monthly** extracts are not delivered timely due to technical or data quality issues. Any extract not posted within 4 hours of the specification will be considered a miss.
Approach for Achieving:	Monthly files are generated from the ETL servers and graphs are run throughout the night to produce the extract of the most current data in SAM. The interfaces that run the graphs are monitored for execution throughout the night. Any failure in the graph creation of the extract can cause a delay in posting of the extract in a timely manner. Additionally, GSA will conduct acceptance testing and provide disposition of extract posting. Any failure to post or delay in posting, the IBM team will notify a GSA POC for communication to stakeholders.
Data Accessibility:	Interface tracking spreadsheet is maintained by the IBM data and interface team. Any breach to SLAs will be reported on the monitoring spreadsheet.
Restrictions:	Monthly Extracts listed at the time of approval of this document will be considered for this metric
Owner:	Extracts & Interfaces Lead

There are 18 monthly files that are currently part of the SAM extracts:

Extract Name	Monthly	Monthly First Sunday	Monthly 15th	Monthly Last Sunday	Once per FY
Legacy CCR FOUO 4082	X	X			
Legacy CCR FOUO 40822	X	X			
Legacy CCR MPIN	X	X			
Legacy CCR Proprietary 4082	X	X			
Legacy CCR Proprietary 40822	X	X			
Legacy CCR Sensitive 4082	X	X			
Legacy CCR Sensitive 40822	X	X			
Legacy CCR Complete 4082	X	X			
Legacy CCR Complete 40822	X	X			
Legacy CCR GSA Complete	X			X	
Legacy CCR FOIA	X		X		
SAM Public (Currently NOT being posted due to D&B/GSA discussions)	X	X			
SAM FOUO	X	X			
SAM Sensitive	X	X			
SAM System-Only	X	X			
SAM MPIN	X	X			
SAM FSRS	X	X			
SAM Reps and Certs (NOT being posted until GSA testing is complete)	X	X			

1.1.23 Measure #27: Program Management - Deliverable Timeliness

Performance Requirement:	Deliverable Timeliness
Acceptable Quality Level (AQL):	**100.00%**
Data Source:	Stakeholder manual identification
How It Is Measured:	Percentage of deliverables and scheduled items available and accepted on schedule.
Approach for Achieving:	Program deliverables are listed in the deliverables tracking spreadsheet within the Connections website. The IBM team will follow the policies documented within the QCP to address the accuracy and timeliness of deliverables.
Data Accessibility:	GSA to acknowledge receipt of deliverables on the same day. Deliverables are posted on the Connections website that can be accessed by anyone with an approved account.
Restriction:	None
Owner:	PMO Lead

Any missed deliverable in a month will result in a failure of this metric.

1.1.24 Measure #28: Program Management - Risk Management

Performance Requirement:	Risk Management
Acceptable Quality Level (AQL):	**There are no unmitigated or unaccepted High-level risks to the program**
Data Source:	Stakeholder manual identification
How It Is Measured:	Risks identified in the monthly risk log delivered within the Monthly Steward Report will have a mitigation strategy for all items marked as high.
Approach for Achieving:	Items are added to the risk log as issues / risks arise. The team conducts monthly risk reviews and updates the risk log. Only current known risks that are documented for consideration of mitigation will be counted within this metric.
Data Accessibility:	GSA and IBM to meet at least quarterly to review current risk log which is also delivered in the monthly Steward Report.
Restriction:	None
Owner:	PMO Lead

1.1.25 Measure #29: Release Quality - Defects Per Release

Performance Requirement:	Defects Per Release
Acceptable Quality Level (AQL):	**Less than 5 Serious defects per 100 RTC Items**
Data Source:	Rational Team Concert
How It Is Measured:	Less than 5 Serious software defects as a result of the production deployment. (1 Serious defect for every 20 RTC delivered items)
Approach for Achieving:	Items that can be traced to a requirement such as Defect, Enhancement and O&M make up the RTC count. 5 Serious defects identified within 30 days after the release.
Data Accessibility:	All defects are maintained in the Rational Team Concert (RTC) tool. Items are marked for delivery in the due date field and may be tracked to completion. Once an item is successfully implemented in production, it is closed.
Restrictions	None
Owner:	Program Manager

Pass Example: A release contained 120 items. 5 serious defects were opened in the first 30 days after the release.

Fail Example: A release contained 120 items. 6 serious defects were opened in the first 30 days

1.1.26 Measure #30: Release Quality - Production Scope

Performance Requirement:	Production Releases contain the agreed / scheduled scope
Acceptable Quality Level (AQL):	**95% of requirements scheduled have been delivered**
Data Source:	Stakeholder manual identification
How It Is Measured:	Missed functionality as indicated by the approved requirements specifications not implemented.
Approach for Achieving:	Approved system specifications added to a release scope prior to end of requirements phase. Requirements that are agreed upon will be developed and delivered to testing for validation. Per the System Engineering plan, approved requirements are designed and developed according to specification and reviewed accordingly. System testing including GAT and UAT will validate proper and complete incorporation of the requirements.
Data Accessibility:	Requirements are maintained in the Rational Team Concert (RTC) Requirements Composer tool. These requirements are linked to individual RTC numbers. Once a requirement is approved for a release, it is tracked to completion within the RTC item.
Restriction:	This is effective for quarterly releases only.
Owner:	Program Manager

During the months when no release is added to production or no new requirements are implemented, the previous score will carry over to the current month.

1.1.27 Measure #31: Release Quality - Production Releases on Schedule

Performance Requirement:	Production Releases are delivered on schedule
Acceptable Quality Level (AQL):	**Delivered on schedule**
Data Source:	Stakeholder manual identification
How It Is Measured:	Release date is met as agreed upon by GSA and IBM.
Approach for Achieving:	GSA and IBM will work together to develop and work towards a quarterly release scope and plan. Once the release date is set and the items for delivery are agreed upon, the teams will have regularly scheduled meetings to discuss progress of the release. The teams will target to have the release date agreed upon at least 90 days prior to the release. Any change to a release date, due to a dependency on GSA, will not count against IBM as a missed schedule delivery.
Data Accessibility:	Release items are maintained in the Rational Team Concert (RTC) tool. Items are marked for delivery in the due date field and may be tracked to completion. Once an item is successfully implemented in production, it is closed.
Restriction:	This is effective for quarterly releases only. This measure will not be counted due to reasons beyond failure of a passing test disposition or incomplete delivery of agreed upon scope.
Owner:	Program Manager

During the months when no release is added to production, the previous score will carry over to the current month.

REQUEST FOR QUOTE

MULTIPLE AWARD BPA TASK ORDER
INSTRUCTIONS AND INFORMATION FOR THE OFFEROR

Issued by GSA Region 5, Federal Acquisition Service

Project Name: Operations and Maintenance of the Federal Procurement Data System (FPDS) Next Generation and System for Award Management Integration Environment

ITSS Solicitation #: ID16210006, 47QDCB21K0007

Project Number: N/A

Contract Type: Unless otherwise negotiated, this Task order is being solicited and will be awarded using the following contract type.

☐ firm fixed-priced, ☐ labor hour or T&M Task Order, ☒ Combination FFP-time and materials.
(double click box and select "not checked" or "checked")

Issuing Agency: GSA Region 5, Federal Acquisition Service

Requiring Activity: GSA Office of the Chief Information Officer (OCIO)

Contractors: Multiple

Federal Supply Schedule: Federal Supply Schedule 70, IT

Contract #: Multiple

BPA #: Multiple (based on solicitation ID16190002)

BPA Title: CIO Modernization and Enterprise Transformation (COMET)

NAICS Code: 541519 – Other Computer Related Services

Product Service Code – DB02 IT and Telecom – Compute Support Services, Non-HPC

NOTE: ONLY FIRMS WHO CURRENTLY HOLD A COMET BLANKET PURCHASE AGREEMENT WITH GSA ARE ELIGIBLE TO PARTICIPATE IN THIS PROCURREMENT ACTION.

Contents

1. Introduction 4
2. Schedule of Items and Prices 4
3. Performance Work Statement (PWS) 4
4. Delivery Requirements 4
4.1 Time of Delivery/Period of Performance 4
4.2 Place of Delivery 4
5. Quote Preparation - General Instructions 4
Cover Page 4
Ability to Perform 5
Accurate and True Statements 5
Assumptions 5
Elaborations 5
Electronic Submission 5
Extraneous Material 5
FSS Contract and COMET BPA Reference 5
Quote Clarity 5
Quote Retention 6
Restrictive Markings 6
Security Classification 6
6. Quote Contents 6
7. Quote Format and Restrictions 9
Proposal Volumes 9
Submission Format 10
Page Formatting 10
Page Limitations 10
Page Limitation Exceptions 11
8. Modifications to the Quote 11
9. Proposal / Quotation Submission 11
Quote Due Date 11
Submission Instructions 11
10. Minimum Acceptance Period 11
11. No-Quote Notification 11
12. Quote Evaluation 12
Step 1 – Evaluation of Technical Capability 12
Factor 1 - Technical Approach 12
Factor 2 – Management & Staffing Plan 13
Factor 3 – Past Performance Relevance 13
Step 2 – Price/Rate Verification and Evaluation 14
Step 3 – Best Value Determination 15
12. Post-Quote Government Requests for Clarification 15
13. Task order Award 16
Basis of Award 16
Award Format and Contents 16
Post Award Debriefing 16

14. Quality Assurance / Quality Control 16
15. Invoicing and Payment 16
16. Proposal Preparation and Pre-Award Costs 16
17. Representations and Certifications 16
18. Subcontracting Plan 16
19. Funding 17
20. Privacy 17
21. Requests for Changes, Clarifications or Additional Information 17
22. TERMS AND CONDITIONS 18
SCHEDULE CONTRACT TERMS AND CONDITIONS: 18
PROVISIONS INCORPORATED BY REFERENCE: 18
FAR 52.217-5, Evaluation of Options (Jul 1990) 18
PROVISIONS IN FULL TEXT: 18
FAR 52.252-1, Solicitation Provisions Incorporated by Reference (Feb 1998) 18
FAR 52.204-24 Representation Regarding Certain Telecommunications and Video Survelliance Services or Equipment (See Attachments) 18
FAR 52.204-26 Covered Telecommunications Equipment or Services Representation (See Attachments) 18
CLAUSES INCORPORATED BY REFERENCE: 18
FAR 52.232-18, Availability of Funds (Apr 1984) 18
FAR 52.212-4, Contract Terms and Conditions – Commercial Items, Alternate I (Jan 2017) 18
FAR 52.232-33, Payment by Electronic Funds Transfer—System for Award Management (Jul 2013) 18
GSAR 552.237-73, Restriction on Disclosure of Information (Jun 2009) 18
CLAUSES IN FULL TEXT: 19
FAR 52.217-8, Option to Extend Services (Nov 1999) 19
FAR 52.217-9, Option to Extend the Term of the Contract (Mar 2000) 19
The 19
GSAM 552.232-39 Unenforceability of Unauthorized Obligations. {FAR Deviation){July 2015) 19
FAR 52.204-25 Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment (See Attachments) 20
IT Security Provisions and Clauses as set forth in the Performance Work Statement 20
23. ATTACHMENTS 20
ATTACHMENT 1 - PWS 20
ATTACHMENT 2 - Schedule of Items and Prices 20
ATTACHMENT 3 – NDAA 889 Restriction Representations FAR 52.204-24 AND FAR 52.204-26 AND CLAUSE FAR 52.204-25 20

1. Introduction

The Federal Acquisition Service, General Services Administration, Region 5, on behalf of the GSA FAS Office of Fleet Management hereby issues a request for quote (RFQ) under the referenced BPA. Identifying information is provided on this title page of this RFQ. Quotes for this requirement are only being solicited from the firms that were awarded a BPA for CIO Modernization and Enterprise Transformation (COMET) Support Services. Other firms are not authorized to participate in this procurement.

The BPAs, upon which this requirement is based, were competitively solicited and awarded to multiple vendors. Unless otherwise stated, the terms and conditions of the referenced BPA and the FSS Schedule solicitation and contract apply to this Task order.

This Task order is for the purchase of services that fall within the scope of the BPA title and work description.

2. Schedule of Items and Prices

See paragraph 5.6, below

3. Performance Work Statement (PWS)

The offeror who is awarded this task order shall perform the specific work objectives and tasks and furnish the deliverables that are identified in the attached Performance Work Statement.

4. Delivery Requirements

4.1 Time of Delivery/Period of Performance

The period of performance for this task order shall be twelve months from the date of award, plus two (2) twelve month option periods and two (2) six month option periods.

4.2 Place of Delivery

All items shall be delivered FOB Destination to the following location.

See PWS Section 4 - Deliverables

5. Quote Preparation - General Instructions

The offeror's quote must include all information requested and must be submitted in accordance with the following instructions.

Cover Page

The cover or introductory page or pages of the quote shall contain, at a minimum –

(1) offeror's name
(2) offeror's contact information
(3) project title
(4) solicitation number
(5) date of quote

(6) date of quote expiration
(7) offeror's DUNS number, and
(8) offeror's FSS contract number.

Ability to Perform

The quote shall demonstrate the offeror's ability to perform the functions and meet the needs and stated requirements of the Government as set forth in the PWS (Performance Work Statement) and any associated, accompanying, or referenced laws, regulation, provisions or documents.

Accurate and True Statements

All information presented in the quote shall be accurate and true according to the offeror's best belief. The penalty for making false statements in quotes is prescribed in 18 U.S.C. 1001.

Assumptions

The quote shall clearly state in a separate section all or any assumptions, conditions of engagement, or exceptions to the solicitation made by the offeror. If not noted, the government will presume that there are none and that the offeror agrees with all of the terms, conditions and requirements of the solicitation. It is not the responsibility of the Government to seek out and identify assumptions, conditions, or exceptions buried within the offeror's quote.

Elaborations

Elaborate brochures, documentation, binding, detailed artwork, or other embellishments are unnecessary and not desired.

Electronic Submission

Quote shall be submitted electronically, as described in the quote submission instructions, below.

Extraneous Material

The quote shall not include, by reference, any extraneous material. The quote shall not mention or reference external material (material not included in the quote) that would not be easily understood by a general practitioner in the field of expertise related to this requirement.

FSS Contract and COMET BPA Reference

Any products, services, or labor hours offered that are not on GSA FSS contract and COMET BPA shall be identified as Other Direct Cost (ODC) items and their prices shall be documented as commercial market prices (see FSS 70 IT contract clause 52-212-4 (e) & (i)).

Quote Clarity

The quote shall be clear and concise. All claims and capabilities shall be substantiated

by references, documented experience, and/or examples. The quote should not simply re-phrase or re-state the Government's PWS and performance objectives. The quote must show how the offeror intends to meet the government's requirement.

Quote Retention

In accordance with FAR Subpart 4.8 (Government Contract Files), the Government will retain one copy of all unsuccessful Quotes.

Restrictive Markings

Offerors who include in their quotes data they do not want disclosed to the public for any purpose or used by the Government except for evaluation purposes, shall mark the title page with the following legend:

> "This quote includes data that shall not be disclosed outside the Government and shall not be duplicated, used or disclosed--in whole or in part--for any purpose other than to evaluate this proposal or quote. If, however, a TO is awarded to this offeror as a result of--or in connection with--the submission of this data, and the Government incorporates the quote as part of the award, the Government shall have the right to duplicate, use, or disclose the data. Also, this restriction does not limit the Government's right to use information contained in this data if it is obtained from another source without restriction. The data subject to the restriction is contained in sheets (insert numbers or other identification of sheets)";

and mark each sheet of data it wishes to restrict with the following legend:

> "Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this proposal or quote."

The Government assumes no liability for disclosure or use of unmarked data and may use or disclose the data for any purpose. Unless restricted, information submitted in response to this request may become subject to disclosure to the public pursuant to the provisions of the Freedom of Information Act (5 U.S.C. 551).

Security Classification

The quote shall be unclassified.

6. Quote Contents

Quotes must –

6.1. Confirm that the offeror will furnish the item(s) or services described in the attached Performance Work Statement.

6.2. **Technical and Management Approach**: Provide a quote to include an explanation of the Technical and Management Approach that is being proposed for accomplishing the work and information demonstrating the relevance of the offeror's past experience performing the type of work described in the PWS. The offeror shall identify and describe the methodology and analytical techniques to be used in fulfilling the technical requirements identified in the task order. The offeror

should tailor the technical approach to achieve the Government's requirements and objectives. The offeror's proposal shall be relevant to this task order and reflect an effective understanding of task order requirements. The Technical and Management Approach shall describe the following (see Section 2 of the Performance Work Statement for specifics):

- Meeting the objectives, conditions, and task requirements.
- Operations and Maintenance for the legacy FPDS applications hosted in AWS and all aspects of the SAM Integration Environment hosted in AWS.
- Operate and maintain the Award data to support the Reporting functionality in the modernized Beta.SAM.gov
- Help Desk Support
- Support retiring the legacy FPDS applications
- Meet all GSA and IAE security requirements
- Meet Service Level Agreement (SLA) standards/metrics
- Adhere to Section 508 Mandates for Government

6.3. **Key Personnel and Project Staffing**: The offeror shall discuss its project staffing approach, describing the project staffing strategy, rationale for the proposed labor mix, and the experience, skills, and qualifications of the proposed personnel. The offeror shall specifically address the following:

- Rationale for choosing the Key Personnel. Describe how each Key Person would be involved in each task and how their qualifications and experience uniquely qualify them for the Key Personnel positions. Include resumes, any certifications, and a letter of commitment for each Key Person.
- Rationale for projected staffing and approach to how each task is staffed including estimated hours and labor mix of the Key and non-Key Personnel, their expected work location, and functional knowledge.
- The value that the non-Key Personnel add to the project team, including their specific skills, experience, and qualifications.
- Rationale for proposed labor categories and level of effort for the task order.
- Approach to hiring, retaining, replacing, and surging personnel with appropriate skillsets throughout the life of this task order.

6.4. **Relevant Past or Present Experience**: The offeror shall elaborate on its experience on projects that are similar in size, scope, and complexity to the requirements contained in the task order. The offeror shall discuss the scope of work, applicability to the tasks outlined in the requirements, the client and project relationship to the GSA FPDS task order, the specific responsibilities of the offeror, major deliverables produced, performance measures/service levels applied, and any problems or issues that occurred and the corrective action taken.

Submit three examples of past performance of projects worked on within the past three years. Two of the three past performance examples shall show the offeror's direct experience as a prime contractor, and for at least one (1) of these two examples the offeror shall have performed a substantial portion of the work. Examples should be of similar scope and complexity to the requirements identified

in the requirements. The remaining experiences can include both the prime contractor and any subcontractors.

6.5 Pricing

- **Offered Prices** – Each offeror shall submit a price quote based on its respective BPA labor rates, which are the lower of the rates in the BPA or the rates in the contractor's current FSS contract. Use the attached Schedule of Items and Prices to submit the offered firm fixed- prices and labor hour price of the item(s) based on the BPA pricing. The price quote shall reflect the complete costs to perform the stated requirements. Offerors shall enter their proposed labor categories, labor hour, labor rates and any offered discounts on the price "buildup" tabs in the columns indicated on the attached Schedule of Items and Prices (Attachment 2). Offerors should submit fully responsive price quotes providing their most advantageous offer to the government. Prices shall include all costs to perform the work described in the PWS. Please use the tabs to fill out the pricing for the base year and option years for a total submitted price.

- **Discounts** – Offerors are encouraged to provide price discounts. Any offered discounts shall be clearly indicated. All offered discounts will be incorporated into the winning offeror's award. . (See in Step 2 – Price/Rate Verification and Evaluation, in Section 11, below)

- **FSS Contract Pricing** – For this order, all rates, prices and pricing terms will be governed and must be supported by those set forth in the applicable MAS IT contract and COMET BPA. **The quote shall reflect the total estimated ceiling price to deliver the requirements.** Quote pricing, whether labor category rates or a total solution price, shall be supported with back up information based on the offeror's MAS IT contract rates and COMET BPA rates. Quotes shall include all conditions or assumptions made by the offeror in arriving at the proposed price.

- **Types of Pricing Used in this Order** – The Government contemplates awarding one Firm Unit Priced Labor Hour task order resulting from this solicitation.

  Fixed Prices –

  - The offeror shall quote the labor mix, level of effort and labor rate of each member of the Phase In team, Program Management Team and for each FPDS Operations and Maintenance team members. The offeror shall quote for the different CLIN configurations for each year/option year etc.
  - The contractor will be paid a fixed amount for each CLIN.

  Reimbursable Prices -

  - Reimbursable Items –The government has entered estimated ceiling amounts in the Schedule of Items and Prices as place holders for the following items should they be needed. These items will be reimbursed On a Time and Material basis.
    - SAM/FPDS Software / Tools

- Other Direct Costs
- Training

➢ The offeror shall quote its offered labor rate prices on the "FPDS DevOps Labor Hour Rates" tab in the Schedule of Items and Prices. These quoted labor rates will be applied for the performance of this task BPA order.
➢ Software Tools, Other Direct Cost items, and Training may be purchased by the contractor upon pre-approval by the government, with total amounts not to exceed the ceilings in the Schedule of Items and Prices.

- **Separate Price Volume –** The Schedule of Items and Prices (Attachment 4) shall be submitted in a separate volume from the non-price portion of the quote.

6.7. Confirm that the offeror will perform work and deliver items according to the government's work statement and delivery schedule.
6.8 Verify compliance with any contract security requirements stated in the PWS Section 8.
6.9. Reference the BPA and Solicitation number provided in the title of this document.
6.10. Confirm compliance with Section 508 of the Rehabilitation Act of 1973. *[All services and/or products provided in response to this solicitation shall comply with Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d), and the Architectural and Transportation Barriers Compliance board Electronic and Information Technology (EIT) Accessibility Standards (36 CRF Part 1194).]*
6.11. Confirm SAM (System for Award Management) registration *[The Contractor must be registered in SAM to receive an award in response to this solicitation. Vendors may register at http://www.sam.gov.]*
6.12 Complete the certification found in FAR 52.204-24 Representation Regarding Certain Telecommunications and Video Survelliance Services or Equipment and FAR 52.204-26 Covered **Telecommunications Equipment or Services Representation** (**Attached**).
6.13 Confirm compliance with FAR 52.204-25 Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment (**Attached**).
6.14 Comply with other requirements in this RFQ.
6.15 Be clear, concise, and shall include sufficient detail for effective evaluation and for substantiating the validity of stated claims. The offer should not simply rephrase or restate the Government's requirements, but rather shall provide convincing rationale to address how the offeror intends to meet these requirements. Offerors shall assume that the Government has no prior knowledge of their facilities and experience, and will base its evaluation on the information presented in the offer.

7. Quote Format and Restrictions

Proposal Volumes

Quotes shall be presented in two volumes with the page limits specified below. Volume 1 shall include all pertinent information that demonstrates that offeror's ability to accomplish the performance objectives in the performance work statement and contain past performance information (Factor 1, 2 and 3, respectively and Confirmations/Verifications under Section 5 of RFQ). Volume 2 shall contact offeror's price quote.

Submission Format

(1) The quote shall be prepared and submitted in electronic format. All word processing documents/files shall be written in Microsoft Word format with all external objects embedded (not linked) OR in portable document format (.pdf). All spreadsheet documents/files shall be written in Microsoft Excel format. *[Note: This stipulation is for compatibility with government software and is not an endorsement of Adobe Systems, Inc. or Microsoft Corporation or their respective products.]*

(2) Multimedia files will not be accepted, e.g., QuickTime or Windows Media Player, RealPlayer, etc.

(3) The offeror is not required to submit hard copies of the quote or any attachments.

Page Formatting

Each page shall conform to the following:

(1) **Page Margin.** No less than ¾" on top, bottom, and sides

(2) **Font.** No smaller than 11 point Arial or 12 point Times New Roman.

(3) **Spacing.** No less than single spacing.

Page Limitations

(1) The government has limited the size of quotes to reduce burden on the evaluation team. These limitations are set forth in the Quote Page Limitations Table, below. The government reserves the right to not read or include in the evaluation any pages that exceed the limit. These limitations apply to both electronic versions and/or hard copy (if requested) of the quote.

(2) A page is defined as follows: Printing on one side of a standard letter size 8.5 x 11 inch sheet of paper or "letter size" electronic page. If text is printed on both sides of a hard copy sheet of paper it is considered to be two pages. Fold-out hard copy or "legal size" electronic sheets may be substituted for "letter size" sheets provided they are used for charts and diagrams, only.

Quote Page Limitations

Section Name	Maximum Pages
Technical – Technical Approach	35 pages total – offerors are free to determine how many pages they wish to devote to Tech Approach and to Mgt & Staffing Plan
Management & Staffing Plan	
Past Performance	Two pages per referenced project and should be no more than a total of six pages for the prime offeror and two pages for each principal subcontractor. (A principal subcontractor is defined as one who performs more than 20% of the labor dollars of the task order.)
Price Quote	No page limit

Page Limitation Exceptions

The page limitations do not include the following:

(1) Front Cover Page and Back Cover Page, provided no quote information appears other than the offeror's name and other company identifying information, offeror's contact information, project title, solicitation number, date of preparation, and company logos
(2) Section Tab/Separator Pages, provided no quote information appears on the page other than Section Name/Number
(3) Contents Outline
(4) List of Tables
(5) List of Figures
(6) Pages intentionally left blank
(7) Any required safety or security forms
(8) Individual employees' resumes or curriculums vitae (CVs)
(9) Key Personnel Letters of Intent
(10) COI Certification (if applicable) or other certifications or representations.

NOTE: The offeror is NOT required to use the maximum allowable number of pages when making their submission.

8. Modifications to the Quote

Should it be necessary to make revisions and/or updates to a quote, the electronic version shall be re-submitted in its entirety with the corrections noted. Revisions and/or updates to hard copy versions may be made by submitting, as a minimum, the full page on which the revision or correction is made.

9. Proposal / Quotation Submission

Quote Due Date

Quotes are due on or before the date and time specified in the ITSS Request for Quote.

Submission Instructions

Submit quotes electronically through the GSA Information Technology Solution Shop (ITSS) procurement portal (web.ITSS.gsa.gov) under the solicitation number noted above. If you have technical difficulties using the ITSS system please contact GSA ITSS Technical Support at web.ITSS.gsa.gov, or by calling toll free 877 / 243-2889 and follow the prompts.

10. Minimum Acceptance Period

Quotations allowing less than 120 calendar days for Government acceptance and order award may be rejected as unacceptable.

11. No-Quote Notification

This task order is being solicited under a multiple award BPA. It is the government's position to

encourage competition for each BPA task order. Therefore, if you choose not to submit a quote for this task order, please notify the contracting officer on or before the date and time that quotes are due and provide a reason for your decision. This information may assist the government to improve the competitive environment.

12. Quote Evaluation

The Government will evaluate offerors' quotes using the following three (3) step process to determine which firm will provide the best value to the government and the highest level of performance confidence. The evaluation shall cover the factors listed below. If this task order has option periods, they will be included in the quote evaluation and subsequent award decision; however, the evaluation of options shall not obligate the Government to exercise the option(s). The quote will be evaluated as a whole regardless of subcontractor involvement. An offeror will be considered to have not met a requirement of this solicitation if that requirement is not addressed in the quote. Offerors will have until the deadline stated in the section Submission of Quotes to submit their quote.

Step 1 – Evaluation of Technical Capability

In this step the government will evaluate and assign an adjectival or numerical rating to each of the non-price evaluation factors. These factors will be evaluated in descending order of importance.

- Non-Price Factor 1 - Technical Approach
- Non-Price Factor 2 – Management & Staffing Plan
- Non-Price Factor 3 - Past Performance Relevance

NOTE: If any factor is evaluated as "not confident" the quote will be eliminated from the competition and will not be eligible for award.

Factor 1 - Technical Approach

The government will evaluate the technical approach portion of the proposal to determine the degree to which the application of the offered technical approach will accomplish the goals of this requirement under PWS Section 2B "Technical Objectives" with minimum performance and cost risk to the government. Specifically, the government will evaluate ---

- The degree to which the offeror shall demonstrate a clear understanding of the project goals and end state and an explanation of how the offeror plans to meet the goals and achieve the government's desired end state.
- The degree to which the offeror demonstrates a clear understanding of the individual elements, processes, and functions that the solution must have to accomplish the project goals, including recommendations or solutions as appropriate.
- The degree to which the offeror demonstrates their capability to perform the type of functions that are required to accomplish the tasks identified in the PWS.
- The degree to which the offeror demonstrates a comprehensive understanding of the applicable laws, guidance and policies as noted in the PWS.

Factor 2 – Management & Staffing Plan

The government will evaluate the management and staffing plan to determine the degree to which the management approach and staff capabilities (as described in resumes or narratives as specifically identified below) will result in successful accomplishment of this requirement with minimum performance and cost risk to the government. Specifically the government will evaluate---

- The degree to which the staffing plan includes labor categories, a labor mix, and levels of effort (labor hours) appropriate for accomplishing this requirement.
- The degree to which the proposed personnel (including subcontractor personnel, if proposed) possess the experience, special qualifications, security clearances, certification and training necessary to successfully perform this requirement (as provided in personnel narratives). For Key Personnel, resumes must be provided for Government decision, clearly identifying the requested qualifications.
- The degree to which the draft Phase-In Plan adequately addresses the complexities of the IT program and environment discussed in the PWS, the learning strategies to be employed, and an appropriate defined risk management plan, to include identification, assessment, and mitigation strategies.

Factor 3 – Past Performance Relevance

Under this factor, the government will evaluate the degree to which the offeror's three past or current projects are similar to this requirement. The Past Performance factor will be evaluated based on an overall consideration of the elements noted below. The following elements are not sub-factors and will not be individually rated, but will be evaluated as a whole to arrive at the past performance relevance rating.

- Past performance reflects/identifies experience on projects that are similar in size, scope, and complexity to the requirements contained in the requirements.
- Past performance reflects current experience and the offeror's roles and responsibilities are similar in scope and complexity to the requirements contained in the requirements.
- Past performance reflects the offeror's approach to client support including quality assurance, risk management, and maintaining effective lines of communication.

Some portion of the three examples must have been performed within the last three years to be consider, with two of the three past performance examples showing the offeror's direct experience as a prime contractor, and for at least one (1) of these two examples the offeror shall have performed a substantial portion of the work.

Non-price factor ratings will be based on the following general criteria. If warranted, the government may also assign a plus (+) or a minus (-) designator on the Highly Confident, Confident, and Somewhat Confident ratings to more clearly delineate an offeror's capabilities. After each non-price factor is assigned a rating, an overall non-price factor rating will be assigned.

Rating	General Description
Highly Confident	The Government is very confident that the offeror has a firm understanding of the requirement, has performed several similar requirements in the past, and proposes a very sound approach. The quotation submitted provides the Government with a high degree of confidence that the offeror is capable of successful performance.
Confident	The Government is confident that the offeror has a firm understanding of the requirement, has performed similar requirements in the past, and proposes a sound approach. The quotation submitted provides the Government with confidence that the offeror is capable of successful performance.
Somewhat Confident	The Government is somewhat confident that the offeror has an understanding of the requirement, has performed somewhat similar requirements in the past, and/or proposes an acceptable approach. The quotation submitted provides the Government with a mild degree of confidence that the offeror is capable of successful performance.
Not Confident	The Government is not confident that the offeror has an understanding of the requirement, has performed somewhat similar requirements in the past, and/or proposes an acceptable approach. The quotation submitted provides the Government with no degree of confidence that the offeror is capable of successful performance.

Step 2 – Price/Rate Verification and Evaluation

In this step the government will review the offerors' rates and prices to ensure that they are fair and reasonable and are in compliance with the requirements of the BPA and the FSS contract under which they are quoted.

> ***Note: When doing its evaluation, the Government reserves the right to normalize (adjust) prices, if necessary, to ensure an equitable price comparison and competition.***

No price information shall be included within the non-price/technical volume. The pricing portion of the quotation shall be submitted using the Government-provided Schedule of Items and Prices (Attachment 2, below). If modifications are made to the Schedule of Items and Prices, they shall be clearly marked, along with an explanation of the modification.

The Government has provided pre-filled Not to Exceed (NTE) amounts in the Schedule of Items and Prices. The totals for Training, Other Direct Costs (ODCs), and Software Tools shall remain as pre-filled by the Government. Any changes to these amounts will be reverted to the original amounts prior to the price evaluation. These amounts shall be inclusive of any proposed indirect rates. Profit or fee will not be permitted on travel,

software or ODCs, but it is included in labor rates. These items will be reimbursed on a Cost Reimbursable basis.

Total Evaluated Price
The total evaluated price shall be the total amount of all line items, for all option periods, whether quoted by the offeror or amounts pre-filled by the government. The evaluation shall confirm that any discount offered on an individual labor category line item is consistently offered each time that labor category line item is quoted. Quoted rates and discounted amounts can change from year to year. If the offeror quotes different discounts for a labor category line item in different parts of the proposal during a given year, all discounts for that labor category line item will be adjusted to equal the least or smallest discount offered when calculating the total evaluated price. Should this adjustment be necessary it will be for evaluation purposes, ONLY. Any such quoted discount differences will not be adjusted when incorporating them into the winning offeror's award.

At the Government's sole discretion, it MAY perform an evaluation of the price to determine if CLIN prices offered are realistic for the work to be performed and provide reasonable and balanced pricing over the total period of performance.

Step 3 – Best Value Determination.

This procurement is being conducted in accordance with the procedures in FAR 8.405. This is not a FAR Part 15 negotiated competition; therefore, the procedures in FAR Part 15.3 (Source Selection) DO NOT apply to this solicitation. The acquisition evaluation will be conducted utilizing a best value approach, which seeks to select an offer with the best value to meet the Government's need. Best value is defined as the expected outcome of an acquisition that, in the Government's estimation, provides the greatest overall benefit in response to the requirement, in accordance with FAR 2.101

To arrive at the best value, the non-price level of confidence scores will be ranked and then each quote, along with its respective price, will be assessed against its eligible competitor. If the offeror with the lowest price does not also have the highest non-price level of confidence score, thus offering the Government the best value, the Government will use a trade-off approach based on the relative risks and benefits of the individual quotes. This trade-off approach will identify the quote offering the best value to the Government. <u>When making these comparisons, the non-price factors level of confidence will be considered more important than price</u>.

12. Post-Quote Government Requests for Clarification

The Government intends to make award based on the initial quote submissions without conducting exchanges. Therefore, each offer should contain the Offeror's best terms from a price and technical standpoint. However, the Government reserves the right to hold exchanges if, during the evaluation, it is determined to be in the best interest of the Government. Exchanges are fluid interaction(s) between the Contracting Officer (CO) and the contractors that may address any aspect of the quote and may or may not be documented in real time. Exchanges may be conducted with one, some or all offerors as the Government is not required to conduct exchanges with any or all contractors responding to this RFQ. Exchanges, if any, with the offeror who has been determined to provide the best value to the government shall not constitute a competitive

range determination and shall not entitle other offerors, if any, an opportunity to revise their quotes.

13. Task order Award

Basis of Award

The government will award a task order to that firm offering the best value to the government, price and other factors considered.

Award Format and Contents

The Task Order resulting from this solicitation will be awarded electronically on a GSA Form 300 in the GSA ITSS system. The vendor receiving the award will be notified by email through the ITSS system's automated notification function. The Task Order will contain all applicable vendor, product identification, order processing, price, and invoicing and payment information.

Post Award Debriefing

This procurement is being accomplished in accordance with FAR 8.4, which does not sanction debriefings as are required, when requested, by FAR 15.5. However, in accordance with FAR 8.405-d(2), a brief explanation of the basis for the award decision will be provided upon request by an unsuccessful offeror.

14. Quality Assurance / Quality Control

An order resulting from this solicitation will be subject to the quality assurance and quality control provisions of the BPA, including the Contractor's Quality Control Plan and the Government's Quality Assurance Surveillance Plan (QASP).

15. Invoicing and Payment

The invoice and payment instructions will be provided in the task order award document.

16. Proposal Preparation and Pre-Award Costs

This RFQ does not commit the Government to pay any quote or proposal preparation and submission or other pre-award costs.

17. Representations and Certifications

The Government shall rely on the offeror's Representations and Certifications, as submitted in response to the applicable FSS contract when making any award based on this solicitation.

18. Subcontracting Plan

If applicable, the government shall rely on the offeror's Subcontracting Plan, as submitted in response to the applicable FSS contract when making any award based on this solicitation.
Note: Subcontracting Plans are not required from small businesses.

19. Funding

The Government intends to fully fund this requirement. In the event the Government is unable to fully fund this requirement, the appropriate incremental funding provisions will be included in the award.

20. Privacy

Information received by the Government, from vendors, in response to this solicitation that is subject to the Privacy Act shall be used in complete accordance with all rules of conduct as applicable to Privacy Act Information.

21. Requests for Changes, Clarifications or Additional Information

The government Contracting Officer is the offeror's single point of contact for questions, clarifications, comments, and additional information regarding this solicitation. ADDRESS ALL QUESTIONS REGARDING THIS SOLICITATION TO THE CONTRACTING OFFICER ON OR BEFORE THE QUOTE DUE DATE SPECIFIED IN THE SOLICITATION.

Additionally, no representative of the vendor or the Government is authorized to negotiate or otherwise change the terms and conditions of this solicitation, or enter into any additional agreements regarding this solicitation without the written approval of the Contracting Officer.

Address correspondence to –

Primary
Mr. Chris Payton
Contracting Officer
U.S. General Services Administration
Federal Acquisition Service, Great Lakes Region
Contracts Division
230 S. Dearborn Street, Room 3800
Chicago, IL 60604
Phone: 312 / 353-7036
Email: chris.payton@gsa.gov

Alternate
Mr. Eben Greybourne
Supervisory Contracting Officer
U.S. General Services Administration
Federal Acquisition Service, Great Lakes Region
Contracts Division
230 S. Dearborn Street, Room 3808
Chicago, IL 60604
Office Phone: (312) 886-3811
eben.greybourne@gsa.gov

22. TERMS AND CONDITIONS

SCHEDULE CONTRACT TERMS AND CONDITIONS:

All applicable contract clauses and terms and conditions from the contractor's GSA Schedule and applicable Blanket Purchase Agreement will be incorporated under any resultant task order.

PROVISIONS INCORPORATED BY REFERENCE:

The following provisions are incorporated by reference with the same force and effect as if provided in full text:

FAR 52.217-5, Evaluation of Options (Jul 1990)

PROVISIONS IN FULL TEXT:

The following provisions are incorporated in full text:

FAR 52.252-1, Solicitation Provisions Incorporated by Reference (Feb 1998)

(Required if any provisions are incorporated by reference)

This solicitation incorporates one or more solicitation provisions by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make the full text available. The offeror is cautioned that the listed provisions may include blocks that must be completed by the offeror and submitted with its quote. In lieu of submitting the full text of those provisions, the offeror may identify the provision by paragraph identifier and provide the appropriate information with its quote.

FAR 52.204-24 Representation Regarding Certain Telecommunications and Video Survelliance Services or Equipment (See Attachments)

FAR 52.204-26 Covered Telecommunications Equipment or Services Representation (See Attachments)

CLAUSES INCORPORATED BY REFERENCE:

The following clauses are incorporated by reference with the same force and effect as if provided in full text:

FAR 52.232-18, Availability of Funds (Apr 1984)

FAR 52.212-4, Contract Terms and Conditions – Commercial Items, Alternate I (Jan 2017)

FAR 52.232-33, Payment by Electronic Funds Transfer—System for Award Management (Jul 2013)

GSAR 552.237-73, Restriction on Disclosure of Information (Jun 2009)

Upon request, the Contracting Officer will make the full text of the clauses available.

CLAUSES IN FULL TEXT:

The following clauses are incorporated in full text:

FAR 52.217-8, Option to Extend Services (Nov 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor prior to expiration of the task order. (end of clause)

FAR 52.217-9, Option to Extend the Term of the Contract (Mar 2000)

The Government may extend the term of this contract by written notice to the Contractor prior to expiration of the contract; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 30 days before the contract expires. The preliminary notice does not commit the Government to an extension. If the Government exercises this option, the extended contract shall be considered to include this option clause. The total duration of this contract, including the exercise of any options under this clause, shall not exceed 60 months. (end of clause)

(g) The contractor and subcontractors must insert the substance of this section in all subcontracts.

GSAM 552.232-39 Unenforceability of Unauthorized Obligations. {FAR Deviation){July 2015)

As directed in AL-2015-03, the following clause is inserted in lieu of FAR clause 52.232-39:]

(a) Except as stated in paragraph (b) of this clause, when any supply or service acquired under this contract is subject to any [commercial supplier agreement (as defined in 502.101)] End User License Agreement (EULA), Terms of Service (TOS), or similar legal instrument or agreement, that includes any [language, provision, or] clause requiring the Government to indemnify the Contractor or any person or entity for damages, costs, fees, or any other loss or liability that would create an Anti-Deficiency Act violation (31 U.S.C. 1341), the following shall govern:

(1) Any such [language, provision, or] clause is unenforceable against the Government.

(2) Neither the Government nor any Government authorized end user shall be deemed to have agreed to such clause by virtue of it appearing in the [commercial supplier agreement. If the commercial supplier agreement] EULA, TOS, or similar legal instrument or agreement. If the EULA, TOS, or similar legal instrument or agreement is invoked through an "I agree" click box or other comparable mechanism (e.g., "click-wrap" or "browse-wrap" agreements),

execution does not bind the Government or any Government authorized end user to such clause.

(3) Any such [language, provision, or] clause is deemed to be stricken from the [commercial supplier agreement] EULA, TOS, or similar legal instrument or agreement.

(b) Paragraph (a) of this clause does not apply to indemnification by the Government that is expressly authorized by statute and specifically authorized under applicable agency regulations and procedures.

End of Clause

FAR 52.204-25 Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment (See Attachments)

IT Security Provisions and Clauses as set forth in the Performance Work Statement

23. ATTACHMENTS

ATTACHMENT 1 - PWS

ATTACHMENT 2 - Schedule of Items and Prices

ATTACHMENT 3 – NDAA 889 Restriction Representations FAR 52.204-24 AND FAR 52.204-26 AND CLAUSE FAR 52.204-25

PERFORMANCE WORK STATEMENT

A procurement by the
U.S. General Services Administration
Region 5 Contracting Division

on behalf of

CLIENT AGENCY:

General Services Administration (GSA) GSA Office of Systems Management (QD)
Integrated Award Environment (IAE)/System for Award Management (SAM)
1800 F Street NW Washington, DC 20405.

PROJECT TITLE:

Operations and Maintenance of Federal Procurement Data System (FPDS) Next Generation (NG) - fpds.gov and System for Award Management (SAM) Integration Environment

PROJECT NUMBERS:

47QDCB21K0007 ID16210006

This requirement is being solicited as a Task Order under the COMET BPA

NAICS 541519 - Other Computer Related Services
Product Service Code DB02 IT and Telecom – Compute Support Services, Non-HP

ORIGINAL VERSION DATED

14 December 2020

Post Award Document Revision History

Revision Number	Description of Changes	Requested By	Date

Contents

Contents

1. INTRODUCTION 7
1.1 Requiring Organization Mission 7
Office of Systems Management (OSM), Integrated Award Environment (IAE) 7
Organizational Mission 7
IAE/SAM Program History 7
IAE/SAM Current Status 8
beta.SAM.gov / Modernized SAM.gov 8
1.2 Procurement Objective 8
1.3 Scope 9
1.4 Background 9
1.5 Applicable Documents, Definitions, Abbreviations & Acronyms 9
2A ADMINISTRATIVE OBJECTIVES AND REQUIREMENTS 11
2A.1 General Performance Requirements 11
2A.1.1 Resources 11
2A.1.2 General Communication 11
2A.1.3 Identification of Employee Affiliation 11
2A.1.4 Business Relations 12
2A.1.5 Contractor Response 12
2A.1.6 Professional Appearance 12
2A.1.7 Team Continuity and Employee Retention 12
2A.2 General Meeting Requirements 13
2A.2.1 Initial Business/Kick-off Meeting 13
2A.2.2 Ad hoc Technical / Work Status 13
2A.2.3 Contract Administration Meetings 13
2A.3 Program / Project Management Requirements 13
2A.3.1 General Program / Project Management Requirements 13
2A.3.2 Phase-In Support 14
2A.3.3 Phase-Out Support 14
2A.4 Subcontract Management 14
2B Business and Technical Objectives 14
2B.1 Business Objectives 14
2B.1.1 Operations and Maintenance 14

2B.1.2 Operate and maintain the Entity/Award data to support the Reporting/Search functionality in the modernized Beta.SAM.gov 16
2B.1.3 Help Desk Support 16
2B.1.4 Support retiring the legacy FPDS applications 16
2B.1.5 Maintain Integration code between Legacy SAM and Beta SAM 16
3. QUALITY 16
3.1 Contractor Quality Control Plan (QCP) 16
3.2 Performance Based Requirements - Service Level Agreement (SLA) 17
3.3 Government Quality Assurance Surveillance Plan (QASP) 17
4. DELIVERABLES 18
4.1 Contractor Submission 18
4.2 Government Review 18
4.3 Government Delays in Reviewing Deliverables or Furnishing Items 18
4.4 Deliverable Table 19
4.5 Data Requirements / Descriptions 20
4.5.1 Contractor Employee Non-Disclosure Agreement 20
4.5.2 Kick-off Meeting Minutes 20
4.5.3 Quality Control Plan 20
4.5.4 Staff Matrix 21
4.5.5 Funds and Expenditure Report 21
4.5.6 Monthly Status Report (MSR) (alternate) 21
4.5.7 Technical Reports 22
4.5.8 Trip Reports 22
4.5.9 Phase-In Plan 22
4.5.10 Phase-Out Plan 22
4.5.11 Monthly Invoice 23
4.5.12 Other Reports 24
5. PERFORMANCE PLACE, TIME, AND RESTRICTIONS 24
5.1 Period of Performance 24
5.2 Place of Performance 24
5.2.1 Performance at the Contractor's Facility 24
5.2.2 Performance at the Government's Facility 24
5.2.3 Applicability of Telework 24
5.2.4 Unplanned Government Facility Closures 25
5.3 Time of Performance - Hours of Work 26
5.3.1 Normal Hours 26
5.3.2 Holidays 26

5.3.3 Expedited Performance 26
5.4 Travel 26
5.5 Limitations on Contractor Performance 26
6. PERSONNEL 27
6.1 General Requirements 27
6.2 Specific Expertise and Experience 28
6.3 Training 28
6.3.1 Contractor Staff Training 28
6.3.2 Mandatory Government Training 28
6.4 Key Positions / Key Personnel 29
6.4.1 Definition & List of Key Personnel 29
6.4.2 Key Personnel Substitution 30
6.5 Personnel Retention and Recruitment 31
6.6 Non-Key Personnel Substitutions 31
6.7 Staff Maintenance 31
6.8 Contractor Employee Work Credentials. 31
7. GOVERNMENT FURNISHED PROPERTY/INFORMATION/ACCESS 32
7.1 General 32
7.2 Government Furnished items (Property) 32
7.2.1 Facilities 32
7.2.2 Equipment 32
7.2.3 Materials 32
7.2.4 Data 32
7.3 Use of Government Property 33
7.3.1 Soft Phones 33
7.3.2 Mobile/Wireless Telephones and Smart Devices 33
7.3.3 Electronic Mail (E-mail) 33
7.3.4 Copiers and Fax Machines 33
7.3.5 Computer and Internet 33
7.3.6 Canvassing, Soliciting, or Selling 33
7.3.7 Security Violations Using Government Equipment 33
7.4 Validation of Government Furnished Items (GFI) and Equipment Inventory 34
8. SECURITY 34
8.1 Non-Disclosure Statement. 34
8.2 Compliance with Security Requirements 35
8.2.1 Assessment and Authorization (A&A) 35

8.2.2 GSA Information Technology IT Security Requirements 36
8.2.3 Recurring Security Deliverables 36
8.2.4 Updated A&A documentation including the System Security Plan and Contingency Plan 36
8.2.5. User Certification/Authorization Review Documents 37
8.2.6 Separation of Duties Matrix 37
8.2.7 Information Security Awareness and Training Records 37
8.2.8 Annual FISMA Self-Assessment 37
8.2.9 System(s) Baseline Configuration Standard Document 37
8.2.10 System Configuration Settings Verification 37
8.2.11 Configuration Management Plan 38
8.2.12 Contingency Plan Test Report 38
8.2.13 Incident Response Test Report 38
8.2.14 Information System Interconnection Agreements 38
8.2.15 Rules of Behavior 38
8.2.16 Penetration Testing Report 38
8.2.17 Personnel Screening and Security 39
8.2.18 Policies and Procedures 39
8.3 Employee Security Requirements 40
8.3.1 New Contractor Personnel 40
8.3.2 Departing Contractor Personnel 40
8.4 Common Access Card & ID Badges 40
8.5 Facility Security Requirements 40
8.6 Personal Identity Verification 40
8.7 Additional Security Requirements 40
9. SPECIAL INSTRUCTIONS 41
9.1 Contractor Performance Assessment Reporting System (CPARS) Assessment 41
9.2 Personal Services 41
9.3 Privacy Act 42
9.4 Rehabilitation Act Compliance (Section 508) 42
9.5 Final Invoice and Release of Claims 42
9.6 Other Direct Costs (ODCs) 42
9.6.1 Cost of Software Maintenance Renewals 43
9.7 Avoidance and/or Mitigation of Actual or Potential Organizational Conflicts of Interest 43
9.8 Task Order Management 43
9.8.1 Contracting Officer's Representative (COR) 43
9.8.2 Government Technical Representative 43

9.9 Technical Direction 44
9.10 Data Ownership/Release/Availability/Rights 44
9.11 Data Rights 45
9.12 Limited Use of Data 45
9.13 Proprietary Data 46
9.14 Inspection and Acceptance 46
9.15 Contract Type 46
9.16 Ceiling Price Notification 46
9.17 Task Order Funding 46
Incremental Funding 46
9.18 Material and Material Handling Costs 47
9.19 Productive Direct Labor Hours 47
9.20 Invoicing and Payment 47
9.21 Payment for Unauthorized Work 48
10 ATTACHMENTS 48
Attachment A – Contractor Non-Disclosure Agreement 48
Attachment B – QASP (Quality Assurance Surveillance Plan) 48
Attachment C – FPDS SLA (Service Level Agreement) 48
Attachment D – FPDS FY20 Software Inventory 48
Attachment E – FPDS AWS Server List 48
Attachment F – FPDS NonProd Network Architecture 48
Attachment G – FPDS Production And Coop Network Architecture 48
Attachment H – FPDS Monthly Steward Report Metrics 48
Attachment I – SAM SLA (Service Level Agreement) 48
Attachment J – SAM Integration Software Inventory 48
Attachment K – SAM AWS Server List 48
Attachment L – SAM Integration Network Architecture 48
Attachment M – CIO 12-2018_ IT Policy Requirements Guide 48
Attachment N – IT Security Procedural Guide 48

1. INTRODUCTION

1.1 Requiring Organization Mission

Office of Systems Management (OSM), Integrated Award Environment (IAE)

Organizational Mission

The Integrated Award Environment (IAE) mission is to support a common, secure business environment that facilitates and supports cost-effective acquisition of, and payment for, goods and services; effective management of federal acquisition and assistance awards; and consistent transparency into federal acquisition and assistance awards.
The IAE vision is to continue to evolve and integrate the existing shared portfolio of seven (7) electronic systems used for awarding and administering federal financial assistance (i.e., grants, loans) and contracts through Scaled Agile Framework (SAFe) development processes on the FAS Cloud Services (FCS) platform, or other common platform as specified by the government in writing.
The largest and most complex of the e-Government initiatives, the IAE works on behalf of the acquisition and financial assistance communities to save money, be more efficient, reduce burdens on the communities we serve, and improve federal award management.

Any existing legacy systems shall be operated as normal before they are migrated into the modernized new system. The Contractors are expected to provide the Operations & Maintenance (O&M) support and meet the Service Level Agreement (SLA). The vendor shall also provide transition support to the modernization teams as it relates to FPDS.

IAE/SAM Program History

In 2002, the Integrated Acquisition Environment was created as an e-Government (e-Gov) initiative under the President's Management Agenda. As part of the e-Gov initiative, the Office of Management and Budget (OMB) designated GSA as the executive agent of the Integrated Acquisition Environment. In 2013, the Integrated Acquisition Environment was renamed the Integrated Award Environment (IAE) by its governance to reflect its management of procurement, grants, and federal assistance data. In 2017, the organization was renamed as The Office of Systems Management (QD), Integrated Award Environment (IAE).

The concept behind the IAE is to provide federal agencies and contractors with a shared IT system to manage the acquisition and grants-making process from solicitation through closeout. The goals of the IAE program are to (1) create a simpler, common, integrated Information Technology (IT) service that promotes competition, transparency, and integrity; (2) increase data sharing across the Government and with the public to enable better decisions in procurement, logistics, payment, and performance assessment; and (3) take a unified approach to obtaining modern tools to leverage investment costs across the federal government for award-related IT services.

The IAE enables all phases of the federal awards management lifecycle, manages the common source of entity information for acquisition and financial assistance

(grants and loans) communities, provides a market research source for contract administration to the federal acquisition community as well as private and commercial firms that are interested in doing business with the government, and stores information that the public in general seeks on how tax dollars are being spent. IAE provides subcontract reporting opportunities for agency and contractor communities. IAE provides data for government and non-government stakeholders including the general public.

IAE is governed by the Award Committee for eGov (ACE) structure which includes the Procurement Committee for eGov (PCE) and the Financial Assistance Committee for eGov (FACE). Additionally, all IAE operations are coordinated and prioritized through a Change Control Board (CCB) that consists of voting representatives from each of the 24 Chief Financial Officer (CFO) Act agencies. These same agencies contribute funding for the IAE operations.

IAE/SAM Current Status

IAE currently sees more than one trillion dollars and 3.3 million transactions in federal assistance and procurement awards across all the IAE systems. With growing numbers, IAE currently has more than 3.4 million registered users and more than 500 million hits or page views per month.

The current IAE systems were developed over several years as free-standing, web-based systems to fulfill different roles throughout the acquisition and grants-making process. Many are operated and maintained by independent contractors. Shared functional components of the application stack for these systems are limited to co-location services that cover some systems and a consolidated end-user help desk that supports a different subset of the systems.

Current IAE systems consist of the following:

1. System for Award Management (SAM)
2. Federal Procurement Data System (FPDS)
3. Electronic Subcontracting Reporting System (eSRS)
4. Federal Funding Accountability and Transparency Act (FFATA) Subaward Reporting System (FSRS)
5. Contractor Performance Assessment Reporting System (CPARS)
6. Federal Awardee Performance and Integrity Information System (FAPIIS)
7. beta.SAM.gov

beta.SAM.gov / Modernized SAM.gov

IAE is in the process of merging all seven (7) of our current operational systems into a single website known as SAM.gov (currently being built as beta.SAM.gov) with the goal of streamlining the process for our users who make, receive, and manage federal awards.

1.2 Procurement Objective

The Government's procurement object is to award a task order under ID15210002 to a highly capable company who will provide the Operations & Maintenance (O&M) support and meet the Service Level Agreements (SLA) for the FPDS system and the SAM Integration environment. The FPDS system will be supported until it is migrated into the

modernized IAE beta.SAM.gov/SAM.gov environment. SAM Integration environment support will be ongoing.

This procurement process must be completed and awarded before 2/14/2021 to reduce the risk of not having system continuity due to the existing contract reaching its end. For the SAM Integration environment, work should not start until after the April 2021 SAM cutover to beta.SAM.

1.3 Scope

The scope of this effort encompasses the following work and initiatives.

a. **Operations and Maintenance**
    1. **Operate and maintain the legacy FPDS applications hosted in AWS**
    2. **Operate and maintain all aspects of the SAM Integration Environment hosted in AWS.**
b. **Operate and maintain the Award data to support the Reporting functionality in the modernized Beta.SAM.gov**
c. **Help Desk Support**
d. **Support retiring the legacy FPDS applications**
e. **Meet all GSA and IAE security requirements**
f. **Meet Service Level Agreement (SLA) standards/metrics**
g. **Adhere to Section 508 Mandates for Government**

The details are stated in Section 2B.

This task order will be placed under the Mission Oriented Business Integrated Services (MOBIS) Federal Supply Schedule, Solicitation No.: TFTP-MC-000874-B (Refresh 16) Special Item Number (SIN) 874-1 Consulting Services or the Consolidated Federal Supply Schedule (00CORP), Special Item Number (SIN) C874-1 Consulting Services. It is anticipated that work will be performed using a Labor Hour or Time and Material type order.

Work will be performed over the period of approximately three years, with an anticipated Base Period of 12 months and four Option Periods of 12 months each.

1.4 Background

This procurement was initiated in 2020 when the FPDS system modernization was delayed and the current contract cannot continue O&M services after it expires. The SAM Integration work was added to this procurement as well to support this environment after the cutover to beta.SAM in April 2021.

A highly capable vendor shall be awarded to take over the required O&M and defined tasks in order to have a seamless transition of migrating the FPDS system into the IAE modernization system as well as to support the SAM integration Environment which will be the backend for beta.SAM where cutover is set for April 2021 (see attached network architecture diagrams).

1.5 Applicable Documents, Definitions, Abbreviations & Acronyms

The documents, if required, (i.e., certifications, specifications, standards, policies, and

procedures), current at time of contract/order award, identified in the list below, are incorporated with the same force and effect as if provided in full text. Succeeding revisions may be substituted or incorporated as required with full notice and disclosure to the contractor. The Government will provide access to available documents and technical information as required and upon contractor request, if not available via a hyperlink within this PWS.

1. Applicable Document
   a. **FPDS SLA (Service Level Agreement)**
   b. **FPDS FY20 Software Inventory**
   c. **FPDS FY20 AWS Server List**
   d. **FPDS NonProd Network Architecture**
   e. **FPDS Production And Coop Network Architecture**
   f. **FPDS Monthly Steward Report Metrics**
   g. **SAM SLA (Service Level Agreement)**
   h. **SAM Integration Environment Software Inventory**
   i. **SAM Integration Environment AWS Server List**
   j. **SAM integration Network Architecture**

2. Definitions, Abbreviations & Acronyms

CO – Government Contracting Officer

COR – Contracting Officer's Representative

FCS – FAS Cloud Services, the platform supporting the application for beta.sam.gov / Modernized SAM

FTE – Full Time Equivalent, the number of labor hours equal to those that would be worked by one employee in a year. For this procurement action 1960 hours is considered an FTE.

CPARS – Contractor Performance Assessment Reporting System – This is a system that generates reports that are created by the government evaluators to document contractor performance.

IAE – Integrated Award Environment

Normal Workweek - A work week is 40 hours

Overtime - Time worked by a contractor's employee in excess of the employee's normal workweek. (Note: Premium pay is not authorized under this contract for overtime work.)

OSM – GSA Office of Systems Management

Quality Assurance - A planned and systematic pattern of all actions necessary to provide confidence to the government that adequate technical requirements are established; products and services conform to established technical requirements; and satisfactory performance is achieved. For the purpose of this document, Quality Assurance refers to actions by the government.

Quality Assurance Personnel (QAP) - A functionally qualified government person(s) responsible for surveillance of contractor performance and providing communications to the contractor(s) and PCO.

Quality Assurance Surveillance Plan (QASP) - A plan detailing the contract surveillance procedures and containing the **Objectives, Measures and Expectations** that will be used to evaluate contractor performance of the PWS objectives.

Quality Control - Those actions taken by a contractor to control the production of outputs to ensure that they conform to the contract requirements.

2A ADMINISTRATIVE OBJECTIVES AND REQUIREMENTS

2A.1 General Performance Requirements

2A.1.1 Resources

It is the Government's objective to rely upon Contractor resources to perform this requirement. To meet this object, the Contractor shall furnish or provide all personnel, personnel management and supervision, all related internal supporting business functions (including background and "overhead" personnel), materials, supplies, equipment, and facilities to perform the full range of services required by this PWS. The team cross-training shall be managed by the Contractor to ensure the coverage of the resource changes or absence. Exceptions shall include government furnished items or data if so stipulated in Section 7, below.

2A.1.2 General Communication

It is the Government's objective that the Contractor maintain regular and direct interface with the Contracting Officer (CO); the Contracting Officer's Representative (COR), and other identified Government representatives. The contractor shall not contact nor take direction from unauthorized Government representatives, under any circumstances.

2A.1.3 Identification of Employee Affiliation

In compliance with FAR 37.144(c), contractor employees shall avoid creating an impression in the minds of members of the public or Congress that they are Government officials by taking the following measures.

- All contractor personnel shall be required to wear Government-approved or provided picture identification badges so as to distinguish themselves from Government employees when working at the Government site.
- Additionally, the contractor shall comply with all visitor identification requirements when visiting the Government site.
- When conversing with Government personnel during business meetings, over the telephone or via electronic mail, contractor personnel shall identify themselves as such to avoid situations arising where sensitive topics might be better discussed solely between Government employees.
- Contractors shall identify themselves on any attendance sheet or any coordination documents they may review.
- Electronic mail signature blocks shall identify their company affiliation.

- Where practicable, contractors occupying co-located space with the Government should identify their work space area with their name and company affiliation.

2A.1.4 Business Relations

A primary element of project success is the business relationship between the contractor and Government representatives. It is the Government's objective that a successful business relationship be maintained. The Contractor shall contribute to meeting this objective by making every effort to establish and maintain clear and constant communication channels with the Government authorized representatives for the purpose of:

- Promptly identifying PWS and/or business relationship issues of controversy and the bilateral development and implementation of corrective action plans.
- Ensuring the professional and ethical behavior of contractor personnel.
- Maintaining effective and responsive subcontractor management (if applicable).
- Ensuring the contractor support team is fully aware and engaged in strengthening the interdependency that exists between the contractors and their Government counterparts.
- Facilitating contractor–Government collaboration for continuous improvement in performing PWS tasks, reducing risks and costs, and meeting the mission needs.
- Providing meaningful feedback during discussions about project execution, when required.
-

2A.1.5 Contractor Response

The contractor shall ensure prompt response to Government inquiries, requests for information or requests for contractual actions.

2A.1.6 Professional Appearance

It is the Government's objective that all personnel involved with this project present a professional appearance. To meet this object the Contractor personnel shall present a neat and professional appearance appropriate to the work being performed at all times when interacting with Government representatives, working in Government facilities, or representing the Government at meetings or before third parties.

2A.1.7 Team Continuity and Employee Retention

The Government recognizes the benefits in maintaining the continuity of contractor team members. These benefits include but are not limited to retention of corporate knowledge, minimizing contractor familiarization, maintaining/increasing performance levels, schedule adherence and preserving organizational interfaces developed over time. These benefits also accrue to the Contractor. Within the context of effective and efficient personnel management, the Contractor shall take reasonable and appropriate steps to retain the qualified employees staffed against this contract to maintain continuity and performance while effectively reducing costs borne by the Government.

2A.2 General Meeting Requirements

The contractor shall participate in the following meetings. Nothing discussed in any meetings or discussions between the Government and the contractor shall be construed as adding, deleting, or modifying the contractual agreement without written authorization from the Contracting Officer.

2A.2.1 Initial Business/Kick-off Meeting

Within 5 business days following the contract/order award (or other time mutually agreed between the parties), the contractor and its key personnel shall meet with the GSA CO, GSA COR, and other identified Government representatives to ensure a common understanding of the requirements, goals, expectations, end products, and objectives of the contract/order. The contractor shall discuss the overall understanding of the project and review the background information and materials provided by the Government. Discussions will also include the scope of work, deliverables to be produced, how the efforts will be organized and project conducted; assumptions made/expected end results. A concerted effort shall be made to gain a thorough understanding of the Government expectations. However, nothing discussed in this or in any subsequent meetings or discussions between the Government and the contractor shall be construed as adding, deleting, or modifying any contract/order requirements, including deliverable specifications and due dates. The contractor shall also address the status of any issues that will affect contractor start-up/ramp-up toward achieving full service/support capability. The contractor will be responsible for taking minutes of this meeting. This meeting can be held at either the Contractor's or Government's location, as appropriate.

2A.2.2 Ad hoc Technical / Work Status

The contractor shall, if requested by the Government, participate in monthly status meetings or ad hoc technical meetings at a mutually agreeable time and place to discuss tasking, work progress, technical problems, performance issues, or other technical matters. During these meetings the contractor shall at least provide accomplishments, problems and issues, and planned actions. The contractor shall take minutes of these meetings and include them in the Monthly Status Report. These meetings will occur at a time and place mutually agreed upon by the parties.

2A.2.3 Contract Administration Meetings

The CO may require the authorized contractor representative to meet or participate in a teleconference with authorized Government personnel as often as deemed necessary to discuss performance or administrative issues. The contractor may also request a meeting with the CO when deemed necessary. The content of meetings shall be documented in writing, as agreed between the parties. Minutes shall be approved by both parties and shall be included in the Government contract file.

2A.3 Program / Project Management Requirements

2A.3.1 General Program / Project Management Requirements

The contractor shall be solely responsible for managing the work performed in the execution of the contract/order. This includes the responsibility to:

- Assign appropriate resources to each task.
- Maintain clear organizational lines of authority.
- Use SAFe Agile methodologies (Refer to https://www.scaledagileframework.com/) and IAE Jira and Confluence to ensure effective task management and administration, following the requirements set forth in the PWS.
- Maintain the personnel, organization, and administrative control necessary to ensure that the work delivered meets the specification requirements.
- Establish and use proven policies, processes, analyses, and best practices.
- The contractor shall be fully responsible for management, control, and performance of any subcontractor used in support of the contract/order. Use of a subcontractor on the contractor's team shall not relieve the prime contractor of responsibility nor accountability in the execution of the contract/order

Additionally, the contractor shall:

- Bring problems or potential problems affecting performance to the attention of the CO as soon as possible.
- Notify the COR, CO, and other identified Government representatives immediately of any projected, anticipated, or known delays that may impede contactor performance.
- When requested, deliver written reports to the CO to memorialize all verbal reports.
- Provide, in writing, the results of all meetings in which proposals are put forth that have the potential for affecting and/or changing contract agreements, requirements or conditions, and these shall be brought to the attention of the CO.

2A.3.2 Phase-In Support

The contractor shall provide phase-in support in accordance with the phase-in plan as required per PWS paragraph 4.5.9

2A.3.3 Phase-Out Support

The contractor shall provide phase-out support in accordance with the phase-out plan as required per PWS paragraph 4.5.10

2A.4 Subcontract Management

The Contractor shall be fully responsible for management, control, and performance of any Subcontractor used on this contract. If a Subcontractor is being used, the Prime Contractor must inform the Government. Use of a Subcontractor on the Contractor's team shall not relieve the Prime Contractor of responsibility nor accountability in the execution of this contract/order.

2B Business and Technical Objectives

2B.1 Business Objectives

2B.1.1 Operations and Maintenance

2B.1.1.1 Operate and maintain the legacy FPDS applications independent of where the application is hosted in AWS cloud

Contractor shall provide Agile project management support for FPDS. Contractor shall coordinate directly with GSA's IAE Program Manager and Program Management Office (IAE PMO) to report status, issues, and the resolution of issues on a weekly basis. As needed, Contractor shall provide input to the IAE PMO to support responses to inquiries from leadership and oversight agencies, including the Acquisition Committee for E-Government (ACE), Office of Management and Budget (OMB), Congress, and the Government Accountability Office (GAO).

During O&M, the contractor is required to provide the system update (service packs) to align the system with the procurement policy changes and minor system enhancements; apply the data management as needed. The service pack is usually once every quarter, 4 times a fiscal year.

For tasks that involve other contractors, Contractor shall establish the requirements or quality standards necessary, shall oversee the schedule of deliverables, assist with functional support as needed, and verify that deliverables meet requirements and quality standards. Contractor is responsible to support all current up and downstream interfaces. Contractor shall closely monitor the cloud infrastructure costs and implement remediation to keep costs under control. Contractor shall report to the IAE PMO, indicating any areas of concern in the weekly report, and integrate the information into the overall end-to-end performance status.

2B.1.1.2 Operate and maintain all aspects of the SAM Integration Environment hosted in the AWS cloud

Contractor shall provide Agile project management support for the SAM Integration Environment. Contractor shall coordinate directly with GSA's IAE Program Manager and Program Management Office (IAE PMO) to report status, issues, and the resolution of issues on a weekly basis. As needed, Contractor shall provide input to the IAE PMO to support responses to inquiries from leadership and oversight agencies, including the Acquisition Committee for E-Government (ACE), Office of Management and Budget (OMB), Congress, and the Government Accountability Office (GAO). All releases need to be lined up with beta.sam.gov releases once integrated.

For tasks that involve other contractors, Contractor shall establish the requirements or quality standards necessary, shall oversee the schedule of deliverables, assist with functional support as needed, and verify that deliverables meet requirements and quality standards. Contractor is responsible to support all current up and downstream interfaces. Contractor shall closely monitor the cloud infrastructure costs and implement remediation to keep costs under control. Contractor shall report to the IAE PMO, indicating any areas of concern in the weekly report, and integrate the information into the overall end-to-end performance status. The support needed for troubleshooting any functional/technical/performance related issues need to collaborate with beta.sam.gov teams.

2B.1.2 Operate and maintain the Entity/Award data to support the Reporting/Search functionality in the modernized Beta.SAM.gov

Contractor shall operate and maintain the Entity/Award data and provide the Entity/Award data as applicable to IAE modernized system for the data desimission through Contract Data reports, Search, APIs, Data Extracts, etc. Contractor shall coordinate with the IAE modernization teams and platform team (FCS) for any delay of data synchronization. When the above said has an issue, Contractor shall provide the support on the analysis or troubleshooting. Contractor shall take proper actions, such as Data Management, to correct the Award data issues.

2B.1.3 Help Desk Support

The Contractor is responsible for the escalated Tier 2 issues received from the Federal Service Desk (FSD), also referred to as the 'Help Desk'. The desired outcome is for users to have prompt access to qualified, knowledgeable IT Help Desk support during business hours (8am-6pm) and to use the Help Desk to resolve all technical and functional questions and problems.

For policy related questions, or for issues that require Government intervention (such as the deletion of Government-owned reports), the Contractor shall escalate them to the appropriate Tier 3 IAE Government Representative. The Tier 2 help desk provider is required to accept and respond to help desk issues/requests that could not be resolved by the FSD.

2B.1.4 Support retiring the legacy FPDS applications

When IAE is working on retiring the legacy FPDS applications, Contractor shall provide the adequate support when required by the Authorized Government representatives. Coordination and collaboration are critical during the process of retiring the FPDS system. Contract shall plan the work with Jira, share the schedule with IAE modernization team for a smooth FPDS decommission.

2B.1.5 Maintain Integration code between Legacy SAM and Beta SAM

The contractor will maintain the integration code between Legacy SAM and Beta SAM for SAM and FPDS.

3. QUALITY

Both the Contractor and the Government have responsibilities for providing and ensuring quality services, respectively.

3.1 Contractor Quality Control Plan (QCP)

The Contractor shall be responsible for quality assurance and quality control of all services performed and all items delivered under this contract/order.

The Contractor shall prepare and maintain a Quality Control Plan (QCP) as a guide for implementing quality assurance and quality control procedures. The Contractor shall submit the QCP to the Government for information and acceptance. The Government has the right to require revision of the Contractor's QCP should its implementation fail to control the quality of items and/or services delivered under this contract/order.

The QCP shall include an explanation of the processes and procedures for ensuring satisfactory performance and delivery of quality items and/or services. Additionally, as a minimum, the QCP shall include the following items.

- A description of the inspection system to cover all major services and deliverables. The description shall include specifics as to the areas to be inspected on both a scheduled and unscheduled basis, frequency of inspections, and the title of inspectors.
- A description of the methods to be used for identifying and preventing defects and deficiencies in the quality of service performed.
- A description of the records to be kept to document inspections and corrective or preventive actions taken.

All records of inspections performed shall be retained and made available to the Government upon request throughout the task order performance period, and for the period after task order completion, until final settlement of any claims under this task order.

The Contractor shall implement a quality program based on its QCP. In compliance with the QCP, the Contractor shall manage, surveil, assess, improve and/or correct contract performance to ensure the quality of the services and deliverable products, as a minimum, meet the level of quality required by the Government Functional Managers or Technical Representatives.

In the event of quality concerns, identified by the Government, the Contractor shall immediately take corrective action in response to Government required changes to the QCP.

The QCP shall be delivered to the Government as stipulated in the Delivery Schedule, see Paragraph 4.5.2 of this PWS, below.

3.2 Performance Based Requirements - Service Level Agreement (SLA)

This contract / order includes a Service Level Agreement (SLA)(PWS Attachment C). The SLA augments the QASP (Quality Assurance Surveillance Plan) by providing performance targets and acceptable levels of product or service quality for specific deliverables that are more detailed than the performance expectations described in the QASP. In addition to defining Acceptable Quality Levels (AQLs), the elements of the SLA provide the basis for determining Incentives and Disincentives in conjunctions with the evaluation of contractor performance.

3.3 Government Quality Assurance Surveillance Plan (QASP)

The Government will periodically evaluate Contractor performance under this contract / order in accordance with the attached Quality Assurance Surveillance Plan (QASP). The purpose of this evaluation is to ensure that Contractor performance meets Government requirements. The Government reserves the unilateral right to change the QASP at any time during contract performance provided the changes are communicated to the Contractor by the effective date of the change. The QASP along with the included “Surveillance Objectives, Measures, and Expectations” describes the evaluation procedures, PWS items to be evaluated, and the measures against which performance will be evaluated. The Government reserves the right to review services to be provided, including those developed or performed at the contractor's facilities, to determine

conformity with performance and technical requirements as prescribed in the applicable inspection clause (see Paragraph 9.14, below). The evaluation results will be documented in the Contractor's CPARS (Contractor Performance Assessment Reporting System) report. The QASP is provided as an attachment to this PWS.

4. DELIVERABLES

4.1 Contractor Submission

Deliverables are to be transmitted with a cover letter on the prime contractor's letterhead. Each deliverable shall include an introductory summary describing the contents. Deliverables shall be provided electronically through GSA's web-based procurement system, as required, and to any other destination(s) as required per the Government's request. The contractor shall provide hard copy deliverables as required per the Government's request. All deliverables shall be produced using software tools/versions as approved by the Government.

This project will be accomplished using Agile methodologies, and as such, specific deliverables, not identified here, will be identified in each sprint. Written deliverables must be concise and clearly written, using plain language guidelines. The Contractor must ensure the accuracy, functionality, completeness, professional quality, and overall compliance with Government guidelines and requirements of all deliverables.

All deliverables developed are the property of the Government and must not be used by the Contractor for any other purpose. All project-related information or documentation, with no exceptions, must be treated as confidential and proprietary during and after the completion of this effort and submitted to the project lead. Additional supplemental restrictions or qualifications or acceptance criteria may be provided at each sprint.

4.2 Government Review

Government personnel will have 10 business days to review deliverables (to include resubmissions) and provide written acceptance/rejection. Authorized Government representatives will notify the contractor of deliverable acceptance or provide comments in writing. The contractor shall incorporate Government comments, or provide rationale for not doing so within 5 business days of receipt of comments. Government acceptance of the final deliverable will be based on resolution of Government comments or acceptance of rationale for non-inclusion. Additional changes volunteered by the contractor will be considered a resubmission of the deliverable.

4.3 Government Delays in Reviewing Deliverables or Furnishing Items

If contractor performance or submission of deliverables is contingent upon receipt of Government furnished items (data, equipment, materials, facilities, and support) or input, or upon Government review and approval of interim items or draft documents (collectively referred to as Government Performance), the Government shall specify, if not already specified within this PWS, when it will provide such items or input, or the time it will need to perform reviews or give approvals. If the Government fails to meet item, input, review, or approval deadlines, contractor performance or submission of deliverables shall automatically be extended one business day for each day of government delay. The contractor shall promptly advise the Contracting Officer of any delays in receipt of Government furnished items, input, reviews, or approvals.

4.4 Deliverable Table

The contractor shall perform or deliver the items listed in the following table on the dates and to the locations specified.

PWS Ref.	Event or Item Title	Delivery Time	Delivery Place
	Project Start	Date of Award	
Sec 4, 8, 10	Contractor Employee Non-disclosure Agreement (one for each employee assigned to work on this order	After award but prior to commencement of performance by each Contractor or Subcontractor employee	Electronically to the GSA ITSS System & email to the IAE COR
Sec 2A.2	Kick-off Meeting	within 5 business days after award or as agreed by the parties	
Sec 2A.2	Kick-off Meeting Minutes	within 5 business days after the kick-off meeting	Electronically to the GSA ITSS System & email to the COR
Section 3	Quality Control Plan-Draft	10 Business Days after award.	Electronically to the GSA ITSS System & email to the COR
Section 3	Quality Control Plan-Final	30 Business Days after Government review. (The Government shall review and provide comments within 7 business days after receipt of the draft QCP.)	Electronically to the GSA ITSS System & email to the COR
Section 4, Section 2B	Deliverables on each Agile sprint	The last day of the Agile Sprint for the committed deliverables	GSA's web-based procurement system
Section 4	Staff Matrix A complete and current list of Contractor employees and the task/office/function they are supporting	Furnished at the kick-off meeting with an update furnished on or before the date of any personnel change.	Electronically to the GSA ITSS System & email to the COR
Section 4	Funds and Man-Hour Expenditure Report	NLT 10 business days after the end of the reporting period.	Electronically to the GSA ITSS System & email to the COR
Section 4	Monthly Status Report – Final	NLT 10 business days after the end of the reporting period.	Electronically to the GSA ITSS System & email to the COR

Section 4	Technical Reports / Studies - Draft	As required by Technical Directive.	Electronically to the GSA ITSS System & email to the COR
Section 4	Technical Reports / Studies - Final	10 Business Days after Government review. (The Government shall review and provide comments within 7 business days after receipt of the draft report/study.)	Electronically to the GSA ITSS System & email to the COR
Section 8	Vulnerability Scanning	NLT 10th day of each quarter	Electronically to the GSA ITSS System & email to the COR
Section 8	Plan of Action & Milestones Update	NLT 10th day of each quarter	Electronically to the GSA ITSS System & email to the COR
Section 8	System Security Plan	NLT 10 business days after the new option year starts	Electronically to the GSA ITSS System & email to the COR
Section 8	Incident report	NLT 3 business days after the incident happens	Electronically to the GSA ITSS System & email to the COR
Section 8	Contingency Plan	NLT 10 business days after the new option year starts	Electronically to the GSA ITSS System & email to the COR
Section 8	System(s) Baseline Configuration Standard Document	90 Business Days after award	Electronically to the GSA ITSS System & email to the COR
Section 8	System Configuration Settings Compliance scan report	NLT 10th day of each quarter	Electronically to the GSA ITSS System & email to the COR

4.5 Data Requirements / Descriptions

Documentation provided in response to the objectives will be in the Government's template format. If no format is prescribed, documents may be in the Contractor's preferred format using standard Microsoft Office products.

The content of all data items, if not self-explanatory from the template format, shall be agreed upon between the parties.

4.5.1 Contractor Employee Non-Disclosure Agreement

The Contractor shall furnish a signed "Contractor Employee Non-Disclosure Agreement" for each Contractor and Subcontractor employee assigned to work under this contract / order, prior to their starting work.

4.5.2 Kick-off Meeting Minutes

The Contractor shall take minutes of the kick-off meeting which shall capture the names of the attendees, the key points of the discussion, questions raised and answered, and action items.

4.5.3 Quality Control Plan

The Contractor shall deliver a QCP as defined in Paragraph 3.1, above.

4.5.4 Staff Matrix

The Contractor shall furnish a complete and current list of Contractor and Subcontractor employees who are assigned to work under this contract / order. The matrix shall include the staffing chart showing the name of each employee, his or her position in the staffing plan, job title, and the Government's task/office/function they are supporting. The lines of authority and responsibility of each staff member shall also be made clear to the Government. The matrix shall be updated with each change in personnel, job title, position in the staffing plan, or assignment of area of responsibility.

4.5.5 Funds and Expenditure Report

The contractor shall provide a Funds and Expenditure Report that provides the current task order accounting information indicated below in support of the monthly invoice. The Contractor can determine the format of the report provided it includes, at a minimum, the following information:

- Expenditures for labor, material, travel, and any other charges.
- Matrix of Actual hours expended vs. planned and/or funded hours, and an explanation of significant variances between planned and expended hours. The report shall include amounts for the current monthly reporting period and the cumulative actual vs. planned hours and amounts for the entire contract/order up to the report date.
- Burn rates for the current period and the cumulative amount for the entire contract/order up to the report date. The information shall be presented in numerical and chart format for each CLIN
- Crosswalk of costs incurred for work performed to amounts billed.
- Current and cumulative task funding status (direct labor, travel, and other direct cost funding status to be reported separately, if required).

Charges shall not exceed the authorized cost limits established for labor and support Items. The government will not pay any unauthorized charges. Original or copies of receipts, travel vouchers, etc. shall be maintained by the contractor to support charges other than labor hours and made available to government auditors upon request. Travel documents shall be furnished in accordance with government Travel Regulations

4.5.6 Monthly Status Report (MSR) (alternate)

The contractor shall provide a MSR that briefly summarizes, by task, the management and technical work conducted during the month. The contractor shall provide the following information, plus any other information that the contractor determines to be germane to the tasks.

- Status of tasks, schedules, deliverables. Status of tasks shall include a summary description and updated milestone schedule noting changes, issues and/or variances, concerning --
  - all tasks completed and deliverables made during the reporting period,
  - all tasks currently on-going during the reporting period, and

  - all known tasks assigned for future reporting periods.
- Staffing (if a separate staffing matrix is not a required deliverable)
- Status of funding and expenditures (if a separate Funds and Expenditure Report is not a required deliverable)
- Problems or issues and proposed resolutions
- Government action requested or required

4.5.7 Technical Reports

Content and format of technical reports shall be agreed upon between the parties.

4.5.8 Trip Reports

Not applicable

4.5.9 Phase-In Plan

The contractor may or may not propose a transition period, for a duration to be determined and proposed by the contractor, but shall not exceed a period of 30 calendar days. The transition period is defined as the period of time (during the phase-in) when the new contractor and the incumbent contractor will both be providing support to the client as required to support the transition to the newly awarded contract/order. If the contractor chooses to propose a transition period, such period shall be included and addressed within the below identified phase-in plan.

The contractor shall develop a phase-in plan. Such phase-in plan shall present a clear understanding of the phase-in tasks required, the issues likely to result from non-incumbent contractor performance, and the contractor's proposal to resolve such issues. The phase-in plan shall include a clear and feasible strategy for delivering services required within the periods specified by the plan and shall include a detailed plan-of-action and milestones to transition the functions identified in this PWS in a well-planned, orderly, and efficient manner. The phase-in plan shall include, at a minimum:

- Staffing plan.
- Development and submission of required deliverables.
- Interface with the Government and incumbent contractor (if applicable) during phase-in, to include meetings or status reports, as required.
- Approach to maintaining quality and minimizing disruption during phase-in.
- Development and dissemination of operating instructions, procedures, and control directives.

4.5.10 Phase-Out Plan

The FPDS system is going to be decommissioned and replaced by the modernized functionalities from the IAE's new Sam.gov system. During phase-out of the contract/order, which is determined to be a period of 30 calendar days prior to the lifecycle end date of the contract/order, a smooth and orderly close-out is necessary to ensure a minimum disruption to vital Government business. The contractor shall cooperate to the extent required to permit an orderly changeover

to the successor contractor from IAE modernization system team(s). The phase-out will be deemed completed by the COR and/or other identified Government representatives when it is determined by the Government that the transition of property, data, and information developed as a part of the contract/order have been successfully changed over from the outgoing contractor to the Government and the successor contractor as required.

For SAM Integration Environment O&M support, when Phase-Out period arrives,the contractor will abide by the phase-out activities listed below.

Phase-out activities include, but are not limited to, the tasks below.

- Submission of official comprehensive phase-out plan.
- Daily communication of staffing status (i.e. projection of when incumbent contractor employees will off-board from the incumbent contract/order and identification of additional incumbent resources, such as a transition team, that may be needed to support the transition efforts) and overall phase out status, in accordance with the accepted phase-out plan.
- Maintain the phase out schedule included within the phase-out plan.
- Transition of property.
- Transition of supporting documentation.
- Transition of accounts (e.g. user accounts and user access).
- Knowledge transfer on the stored system code, or established installation, operation, and maintenance procedures of the technologies supported. The phase out plan shall clearly describe the proposed methodologies to be utilized for such transfer (e.g., written documentation, manuals, formal classroom type training, one-on-one training sessions, etc.).
- Transition of any license keys, numbers or documentation of maintenance agreements for all software utilized for the operations of this system.
- Execution and submission of phase out checklist, to include Government acceptance.

4.5.11 Monthly Invoice

The contractor shall provide a monthly invoice, no later than the 10th calendar day of the month following the monthly reporting period, to be submitted simultaneously with the MSR. As applicable, the invoice shall include but is not limited to:

- Clear identification of all costs.
- Labor hours expended (for labor hours tasks). The labor hours expenditure information shall include the identification of the employee name, labor category, hourly labor rate, and total number of labor hours expended.
- Timecards. As required, the contractor shall provide a copy of each employee's timecard/sheet. The timesheet shall identify the contractor employee name and number of hours claimed per day.
- Travel costs.
- Supporting documentation for travel costs. Refer to PWS 5.3 for specific requirements.
- Other Direct Costs.
- Supporting documentation for other direct costs. Refer to PWS 9.6 for specific requirements.

As required, the contractor shall comply with line item (i.e., per individual positions, different programs, program areas, etc.) invoicing requests

4.5.12 Other Reports

Content of other reports is self-explanatory or should be agreed upon between the parties.

5. PERFORMANCE PLACE, TIME, AND RESTRICTIONS

5.1 Period of Performance

The anticipated period of performance(s) is/are identified below.

- Base Period: Initial 12 months from date of award
- Option Period 1: 12 months following the Base Period
- Option Period 2: 12 months following Option Period 1
- Option Period 3: 6 months following Option Period 2
- Option Period 4: 6 months following Option Period 3

5.2 Place of Performance

5.2.1 Performance at the Contractor's Facility

Work is expected to be performed primarily at the contractor's facilities. Work performed at contractor facilities shall be performed according to the contractor's standard commercial practice; however, the contractor representatives at these facilities must be available for interaction with Government employees during the core hours identified in the paragraph entitled "Time of Performance - Normal Hours", below, with the exception of Government designated holidays or facility closures.

5.2.2 Performance at the Government's Facility

The Contractor may be required to perform work at both central and regional GSA offices to attend meetings, enable the Contractor to work with GSA to understand the business needs in order to effectively use Agile principles in the continuous delivery of functionality, conduct training sessions, troubleshoot, etc. If travel is required, it will be reimbursed subject to the terms and conditions of the underlying BPA/GSA Schedule contract.

5.2.3 Applicability of Telework

All work performed at locations other than those identified as Government and/or contractor facilities shall be approved prior to performing the work. Federal contractors are not governed by Office of Personnel Management (OPM), GSA, or the individual agency policies; however, this does not prohibit contractor personnel from actually working at an alternate site, when/as appropriate and specifically authorized by the Government. The contractor shall develop telework policies to comply with the following requirements and address such requirements at a generic level within their QMP. Alternate work arrangements for contractors shall be negotiated with the contractor's own employer and the appropriate agency official, to ensure policies and procedures are in close alignment and there is a clear and concise arrangement documenting the agreement. It remains the

contractor's responsibility to ensure the services are performed in accordance with the terms and conditions of the contract/order.

The contractor shall address the pertinent facts impacting performance and ensure all affected contractor resumes and other related documentation reflects the applicable work site. The contractor shall provide justification to the Government when identifying and submitting an individual as a telecommuter and address implementation processes and procedures within the QMP. The contractor shall be responsible for ensuring the Government has the required access/details necessary for the Government to perform quality assurance responsibilities.

The contractor shall comply with all agency security telework policies. The contractor shall ensure all services provided from an alternate site comply with the Federal Information Security Management Act of 2002 (FISMA) and address the following, as a minimum:

- Controlling access to agency information and information systems;
- Protecting agency information (including personally identifiable information) and information systems;
- Limiting the introduction of vulnerabilities;
- Protecting information systems not under the control of the agency that are used for teleworking;
- Safeguarding wireless and other telecommunications capabilities that are used for teleworking; and
- Preventing inappropriate use of official time or resources that violates subpart G of the Standards of Ethical Conduct for Employees of the Executive Branch by viewing, downloading, or exchanging pornography, including child pornography.

5.2.4 Unplanned Government Facility Closures

In the event of unplanned closure of the Government facility for any reason (e.g. natural disasters, Government shut-down, or severe weather) the Contractor shall make its best effort to mitigate loss of work time. If Contractor employees are working on the Government facility, this may be done by moving employees to an off-site location. If performance under this contract/order is not possible, the Contractor shall take steps to assign employees to other projects on a temporary basis or place them in leave status to minimize non-productive costs to the Government under this contract/order. Additional instructions may be provided by the Contracting Officer on a case-by-case basis. Disagreements between the parties resulting from closures shall be settled through negotiations to the maximum extent possible or shall otherwise be settled pursuant to the provisions of the Disputes provisions of this contract/order.

All services to be performed under this contract/order have been determined to be non-essential for performance during a closure. Should the Government facility be closed, the Contractor shall be notified by either the Contracting Officer, COR, or a local television or radio station. The Contractor is responsible for notifying its employees about Government closures. Contractor employees are not to report to the Government facility if it is closed and will adhere to delays, unless otherwise specifically instructed otherwise by the CO or COR.

5.3 Time of Performance - Hours of Work

5.3.1 Normal Hours

For any Contractor employees working on Government facilities, their normal business day must include core duty hours between 9 AM through 3 PM local time, Monday through Friday, excluding holidays, to coordinate with Government operations. Actual start and end times shall be at the contractor's discretion. The Contactor shall be responsible for managing the work hours of its employees who work at Contractor facilities, provided that those employees are available when necessary to interact with Government employees.

Any Contractor employee working at Government facilities shall observe federal holidays and government closures on the same dates and during the same times as the Government personnel, since Contractor employees shall not have access to the Government facilities during these days and/or times. These holidays are as follows.

5.3.2 Holidays

The Government shall observe the following holidays.

New Year's Day	Labor Day
Martin Luther King Jr., Day	Columbus Day
Presidents' Day	Veteran's Day
Memorial Day	Thanksgiving Day
Independence Day	Christmas Day

5.3.3 Expedited Performance

In the event that individual tasks or subtasks require expedited performance or extended workdays to meet schedule constraints or work volume, the Government shall communicate that need to the Contractor's Project Manager or Team Lead who, in turn, is responsible for managing the Contractor's labor resources to meet the schedule constraints. Communications regarding expedited performance shall be documented in writing, by email or otherwise, and included in the contract administration file. If Contractor employees are working at Government facilities and task completion deadlines require extended hours, the Government will provide authorization to occupy and use Government facilities beyond normal duty hours.

5.4 Travel

Not applicable.

5.5 Limitations on Contractor Performance

In compliance with FAR 37.102(c), this task order does not require the contractor to perform any inherently governmental functions. Accordingly, the contractor shall NOT perform any of the inherently governmental functions listed in FAR 7.503. Those inherently governmental functions most applicable to this procurement action are as follows:

- Determine Government policy. [7.503(c)(5)]
- Determine Federal program priorities. [7.503(c)(6)]

- Direct or control Federal employees; [7.503(c)(7)]
- Determine acquisition, disposition, or disposal of Government property; [7.503(c)(11)]
- Determining what supplies or services are to be acquired by the Government [7.503(c)(12)(i)]
- Vote on a source selection board; [7.503(c)(12)(ii)]
- Approve any contractual document on behalf of the Government; [7.503(c)(12)(iii)]
- Award Government contracts; [7.503(c)(12)(iv)]
- Administer Government contracts; [7.503(c)(12)(v)]
- Accept or reject supplies or services; [7.503(c)(12)(v)]
- Terminate Government contracts; [7.503(c)(12)(vi)]
- Determine cost reasonableness, allowability, or allocability; [7.503(c)(12)(vii)]
- Participating as a voting member on performance evaluation boards; [7.503(c)(12)(viii)]
- Determine budget policy, guidance, and strategy [7.503(c)(16)]

6. PERSONNEL

6.1 General Requirements

%%%

NOTE: The Government, at its sole discretion, may consider substitutions and/or requests for deviation from any of the following personnel qualifications (e.g., experience in lieu of education), if to do so would be in the best interest of the Government.

%%%

All contractor personnel shall meet the minimum general requirements listed below.

- All personnel shall be capable of working independently.
- All personnel shall have training and experience that is appropriate for the tasks to which they will be assigned.
- The contractor shall provide personnel that are capable of conducting themselves in a professional manner and have proper telephone and e-mail etiquette, customer service techniques, and organizational skills.
- Contractor personnel performing in a leadership capacity shall be capable of directing contractor personnel and interfacing with the Government and customers.
- Ability to communicate applicable technical subject matter expertise to management and others.
- Strong written and oral communication skills in the English language. All contractor personnel must be able to read, write, speak and understand English.
- Exceptional customer service skills.
- Strong time-management and prioritization skills.
- If applicable, all personnel shall meet the minimum requirements set for in the Federal Supply Schedule (FSS) contract or Government-wide Acquisition Contract (GWAC) upon which this task order is based.

The Contractor shall furnish adequate documentation to substantiate compliance with this

requirement for each assigned staff member. The Contractor shall certify as to the accuracy and completeness of the supporting documentation.

6.2 Specific Expertise and Experience

The contractor shall provide personnel with the appropriate skill levels. While each individual contractor employee may not possess expertise and experience in each area of performance, the Government requires that the overall contractor staff possess the aggregate skills, expertise, and experience to successfully complete all requirements.

6.3 Training

6.3.1 Contractor Staff Training

The contractor shall provide fully trained and experienced staff. Contractor personnel are required to possess the skills necessary to support the minimum requirements of the labor category under which they are performing. Training of contractor personnel shall be performed at the contractor's expense, except when the Government changes the requirements during performance of an on-going task and it is determined to be in the best interest of the Government. This will be negotiated on a case-by-case basis. Training at Government expense will not be authorized for replacement personnel or for the purpose of keeping contractor personnel abreast of advances in the state-of-the-art, or for training contractor personnel on equipment, computer languages, and computer operating systems that are available in the commercial market.

NOTE: Unless Contractor employee training is specifically identified and authorized by the Government, in writing, the Contractor shall not bill the Government for employee time spent in training or for any costs related to or associated with Contractor employee acquired training. This applies to training of any type or for any purpose, including training that is either necessary for job or employment eligibility or a prerequisite to performance of work under this contract/order, whether general in nature or specialized and unique to this requirement.

6.3.2 Mandatory Government Training

During the course of this contract / order the Government may require Contractor employees to receive specialized training in areas necessary to allow the Contractor to fulfill the requirements of this contract / order (e.g., LAN Information Assurance Training, Government unique software or software tools, Security Training). In such cases Government mandated training shall be considered part of this contract and charged against the task(s) to which the individual Contractor employee is assigned.

Mandatory Government training shall be tracked and monitored by the contractor. All required courses must be completed by the required dates by all contractor personnel. Mandatory Government training classes may be completed during work hours. It is the intent of the Government to provide 30 calendar days written notice of annual training requirements to the designated contractor representative. The designated contractor representative will be responsible for notifying subordinate contractor personnel. Failure of Contractor employees to take mandatory Government training may impair the Contractor’s ability to perform but

will not excuse the Contractor from performing.

6.4 Key Positions / Key Personnel

6.4.1 Definition & List of Key Personnel

Key Personnel are defined as those individuals who are so essential to the work being performed that the contractor shall not divert them to other projects or replace them without receiving prior approval from the Contracting Officer. This includes substitution of those originally proposed at the time of contract/task order award*. Substituted personnel must have equal or better qualifications than the person they replace, subject to the Government's discretion.

The following Contractor personnel have been initially identified by the Government as "Key Personnel" under this contract / order.**

Project Manager

- An active PMI Project Management Professional (PMP®), PMI Program Management Professional (PgMP®) Certification, or a Bachelor, or Master degree from an accredited institution in Project Management, at the time of proposal submission
- Formal training or certification in Agile software development methods
- Demonstrated experience in the management, design, implementation, and maintenance of Services similar to the requirements of the PWS
- Demonstrated experience in managing in a continuous integration and DevOps environment.
- Demonstrated experience with the management, manpower utilization, and supervision of employees (including subcontractors) of various labor categories and skills in projects similar to the requirements of the PWS. Specifically, managing teams that will coordinate with the Government and work with other contractors to support an Agile environment with a small team of developers; managing O&M of operational systems with more than a quarter million users with one million visitors per month; managing the O&M efficiency, data quality, , service delivery and the technical support (Tier 2) to the Help Desk.
- Demonstrated ability to orchestrate the management of technology scope and risks.
- Demonstrated written and verbal communication skills, including experience in presenting material to senior Government officials.

Scrum Master

- Formal training or certification in Agile software development methods at the time of proposal submission.
- Demonstrated experience working with Agile, and/or Continuous Delivery approaches and best practices, especially those that support scaling Agile to an enterprise such as the Scaled Agile Framework (SAFe)
- Demonstrated experience in using an Agile development framework including task estimation, test automation, deployment automation and Continuous Integration to improve overall Agile activity execution and product quality.
- Demonstrated experience ensuring that the technical expectations of deliverables are met through Agile processes; additionally, support the

continuous improvement of those processes
- Demonstrated experience delivering agile software solutions using best practices such as Test-Driven Development (TDD) or Adaptable Software Design.

Technical Lead

- Minimum of 5 years experience in agile software development to include Microservices architecture using open source Java technology.
- Minimum of 3 years experience with designing and developing complex software systems on a virtualized cloud environment such as Amazon AWS.
- Formal training such as a Bachelor of Science degree in Computer Science preferred
- Minimum of 2 years experience developing and deploying microservices in a cloud environment preferred.
- Minimum of 3 years experience in DevOps and CI/CD concept using tools such as Jenkins, GitHub, Docker/Kubernetes, and testing tools such SonarQube, JMeter.
- Demonstrated experience delivering Agile software solutions using best practices such as Test-Driven Development (TDD) or Adaptable Software Design
- AWS Certified Solutions Architect

**Note: Failure of the Contractor to furnish proposed key personnel shall be viewed as a breach of contract and may be grounds for a default determination by the Government.*

***Note: Should the Contractor propose additional key personnel this provision will be modified to include those additional personnel.*

6.4.2 Key Personnel Substitution

The Contractor shall not remove or replace any personnel designated as key personnel without making a written request to and receiving written concurrence from the Contracting Officer. The Contractor's request for a change to key personnel shall be made no later than ten (10) calendar days in advance of any proposed substitution and shall include a justification for the change. The request shall (1) indicate the labor category or labor categories affected by the proposed change, (2) include resume(s) of the proposed substitute in sufficient detail to allow the Government to assess their qualifications and experience, and (3) include a statement addressing the impact of the change on the Contractor performance. Requests for substitution will not be unreasonably withheld by the Government. The Government will approve initial contactor key personnel at time of award. Replacement key personnel will be approved via modification to the contract/task order. If the Government CO and the COR determine that the proposed substitution, or non-employee initiated removal of personnel without substitution or replacement, is unacceptable or would impair the successful performance of the work, the Contracting Officer will request corrective action. Should the Contractor fail to take necessary and timely corrective action, the Government may exercise its rights under the Disputes provisions of this contract or take other action as authorized under the provisions of this task order, the Prime contract upon which this order is based, or pursue other legal remedies allowable by law.

6.5 Personnel Retention and Recruitment

The contractor shall make every effort to retain personnel in order to ensure continuity until contract/order completion. If it should become necessary to substitute or replace personnel, the contractor shall immediately notify the COR and/or other identified Government representatives in writing of any potential vacancies and shall submit the resume(s) of replacement personnel within 5 calendar days of the notification. Additionally, for all new positions identified by the Government, the contractor shall submit the resume(s) of proposed personnel within 5 business days of the Government's initial request. The contractor shall submit the resume(s) of all potential personnel selected to perform under the contract/order to the COR and/or other identified Government representatives through GSA's web-based procurement system, or any other process means identified/required, for Government review and acceptance/rejection. Upon Government acceptance of a personnel resume(s), the candidate shall be available to begin performance within 14 business days. The contractor shall ensure continuity of operations during periods of personnel turnover and long-term absences. Long-term absences are considered those longer than one week in duration.

6.6 Non-Key Personnel Substitutions

Although Government approval is not required prior to replacing any of its non-key personnel staff, the Contractor shall provide resumes or other adequate documentation to verify to the Government that all proposed replacements (temporary or permanent) meet the security and minimum educational and experience requirements of this contract/order. Additionally, the Government requests the courtesy of being immediately informed of any potential vacancy or prior to any staff member being removed, rotated, re-assigned, diverted or replaced.

6.7 Staff Maintenance

The contractor shall make every effort to retain personnel in order to ensure work continuity until contract/order completion. During any periods of turnover or temporary absence of personnel, the Contractor shall ensure continuity of operations and make every effort to maintain manning without loss of service days to the Government. This may necessitate the use of temporarily assigned employees to fill short term gaps between permanently assigned employees or prolonged (more than one week) absences of current employees.

The Contractor is required to use and/or replace all personnel with those who meet the minimum qualifications as stipulated above, in this section of the PWS and should strive to replace departing personnel with those having appropriate and/or equal qualifications. Failure on the part of the Contractor to employ an adequate number of qualified personnel to perform this work will not excuse the Contractor from failure to perform required tasks within the cost, performance, and delivery parameters of this contract / order.

6.8 Contractor Employee Work Credentials.

Contractors shall ensure their employees and those of their Subcontractors have the proper credentials allowing them to work in the United States. Persons later found to be undocumented or illegal aliens will be remanded to the proper authorities.

7. GOVERNMENT FURNISHED PROPERTY/INFORMATION/ACCESS

7.1 General

The Government shall provide, without cost to the Contractor, the data, facilities, equipment, materials and services listed below. The Government furnished property and services provided as part of the contract/order shall be used only by the contractor and only to perform under this contract/order. No expectation of personal privacy or ownership using any Government electronic information or communication equipment shall be expected. All property at Government work sites, except for contractor personal items, will be assumed to be Government property unless an inventory of contractor property is submitted and approved by the CO/COR. Contractor personal items do not include government owned computers, external drives, software, printers, and/or other office equipment (e.g., chairs, desks, file cabinets). The contractor shall maintain an accurate inventory of Government furnished property.

7.2 Government Furnished items (Property)

7.2.1 Facilities

The Government will provide facilities at the authorized primary work locations as specified in PWS paragraph 5.2. Use of the facilities by contractor personnel will include all utilities, telephone, janitorial services and furniture for contractor personnel performing tasks. The Government will provide the contractor access to buildings as required, subject to the contractor personnel obtaining the required clearances and approvals.

7.2.2 Equipment

The Government will provide the following at authorized on-site Government work locations:

- A suitable work environment (i.e., telephone, office space and furniture). Office space may include a private or shared cubicle, hoteling space (space reserved for temporary use), or other such space suitable for the work required.
- A personal desktop computer or laptop and auxiliary hardware and software required in the performance of the contract/order.
- Network connectivity required to perform work assignments. Network and computer access rights commensurate with work assignments.
- The Government will replace items that are determined to be beyond economical repair by the COR and/or other identified Government representatives unless damage or loss is determined to be due to contractor negligence.

7.2.3 Materials

Not applicable

7.2.4 Data

The Government will provide access to available documents and technical information, as required and upon contractor request, if not available via a hyperlink within this PWS.

The Government will provide documents, reports, database access, data, and other information as available and as required to facilitate accomplishment of work, as stated within this PWS.

The contractor is responsible for obtaining data necessary to perform each task if that data is in the public domain and is not otherwise furnished by the government.

7.3 Use of Government Property

7.3.1 Soft Phones

Government soft phones may be provided as an application on Government provided computers. These are provided for use in conducting official business. Contractor personnel are permitted to make calls that are considered necessary and in the interest of the Government. The contractor shall follow the same policies as Government personnel for telephone usage.

7.3.2 Mobile/Wireless Telephones and Smart Devices

Government issued mobile/wireless telephone and smart devices may be assigned to contractor personnel when the Government determines it is in the Government's best interest. Contractor personnel are prohibited from using any Government issued device for personal use.

7.3.3 Electronic Mail (E-mail)

All Government e-mail access and use by contractor personnel shall be in support of the individual's official duties and contract/order responsibilities. All information that is created, transmitted, received, obtained, or accessed in any way or captured electronically using Government e-mail systems is the property of the Government. Contractor personnel are prohibited from forwarding e-mail generated from a Government provided e-mail account to personal devices.

7.3.4 Copiers and Fax Machines

Copiers are to be used to copy material for official Government business only in the performance of the contract/order. Contractor personnel shall not use fax machines for other than official Government business in the performance of the tasks in the contract/order.

7.3.5 Computer and Internet

All Internet and electronic media access accomplished by contractor personnel (utilizing Government furnished equipment) shall be for official Government business in the performance of the tasks in the contract/order.

7.3.6 Canvassing, Soliciting, or Selling

Contractor personnel shall not engage in private activities for personal gain or any other unauthorized purpose while on Government-owned or leased property, nor may Government time or equipment be utilized for these purposes.

7.3.7 Security Violations Using Government Equipment

Any contractor violating Government security policies, guidelines, procedures, or

requirements while using Government equipment or while accessing the Government network may, without notice, have their computer and network access terminated, be escorted from their work location, and have their physical access to their work location removed at the discretion of the CO/COR. The CO/COR will notify the contractor of the security violation and request immediate removal of the contractor employee.

NOTE: All Government-provided items remain the property of the Government and shall be returned upon completion of the support services. Contractor personnel supporting this requirement shall return all items issued to them when their performance on this contract/task order is ended.

7.4 Validation of Government Furnished Items (GFI) and Equipment Inventory

The Contractor shall develop and maintain a complete GFI inventory that shall be made available to the Government upon request. Within three (3) business days of receipt of any GFI, the contractor shall validate the accuracy of the materials and notify the COR and/or other identified Government representatives, in writing, of any discrepancies, and update the GFI inventory list.

NOTE: Validation shall consist of the contractor checking for physical and logical completeness and accuracy. Physical completeness and accuracy shall be determined when all materials defined as Government furnished are provided. Logical completeness and accuracy shall be determined when all materials defined and associated with a program, system, or work package are provided.

8. SECURITY

8.1 Non-Disclosure Statement.

Due to the potentially sensitive nature of the data and information associated with this requirement, each Contractor employee (including temporary employees) assigned to work under this contract / order shall complete the attached “Contractor Employee Non-Disclosure Agreement”. (PWS Attachment A) A copy of each signed and witnessed Non-Disclosure agreement shall be submitted to the COR prior to performing any work under this contract.

The Contractor shall not release, publish, or disclose sensitive information to unauthorized personnel, and shall protect such information in accordance with provisions of the following laws and any other pertinent laws and regulations governing the confidentiality of sensitive information:

- 18 U.S.C. 641 (Criminal Code: Public Money, Property or Records)
- 18 U.S.C. 1905 (Criminal Code: Disclosure of Confidential Information)
- Public Law 96-511 (Paperwork Reduction Act)

All information that is (1) obtained related to or derived from this contract, and (2) results from or derived from any actual tasks assigned to Contractor employees while participating on this contract is considered proprietary.

8.2 Compliance with Security Requirements

The contractor is required to comply with all security regulations and directives as identified herein and other security requirements as are shown elsewhere in this contract. Please refer to the below referenced Security policy documents.

GSA Information Technology (IT) Security Requirements are included in the below Security Policy Documents

- CIO 09-48, IT Security Procedural Guide: Security and Privacy IT Acquisition Requirements
- CIO 12-2018, IT Policy Requirements Guide
- CIO IT Security 06-30, Managing Enterprise Risk
- DevSecOps OCISO Program [CIO-IT_Security_19-102] [PDF - 806 KB] - 09/13/2019

All data should be encrypted in transmission and at rest.

The Contractor shall be responsible for ensuring all employees supporting this contract comply with all security requirements imposed by the Government Security Officer at all times while in Government facilities and shall follow the instructions of the local organization pertaining to security.

The Federal Information Security Modernization Act (FISMA) of 2014 provides a comprehensive framework for ensuring the effectiveness of information security controls across Federal agencies. FISMA focuses on the program management, implementation, and evaluation aspects of the security of federal information systems. It codifies existing security policies, including Office of Management and Budget (OMB) Circular A-130, Revised, and reiterates security responsibilities provided for in the Computer Security Act of 1987, the Paperwork Reduction Act (PRA) of 1995, and the Clinger-Cohen Act (CCA) of 1996.

In order to protect against cybersecurity threats and manage GSA information systems, the Vendor shall ensure that the contract is compliant with Federal security standards and GSA requirements. The Vendor must provide security and protection for information systems that support the operations and assets of the agency, including the support activities provided or managed by a contractor. Relevant areas that GSA's policies address include:

- Security Requirements
- Cloud information system
- Mobile application
- Privacy Protection
- Controlled Unclassified Information
- Incident Reporting Requirements
- Software License Management
- Telecommunications Policy
- Social Media Policy .

8.2.1 Assessment and Authorization (A&A)

Federal agencies are required by FISMA Law to undergo a security assessment to demonstrate compliance with security requirements. Assessment and

Authorizations (A&A) are required for all new systems. The result of a successful A&A is an Authority to Operate (ATO) Memo. The ATO is required before going into operation and processing the GSA information system. The failure to obtain/maintain the ATO will result in non-compliance and possible shutdown of the system .

8.2.2 GSA Information Technology IT Security Requirements

The contractor shall deliver an IT Security Plan, as required under CIO 09-48, IT Security Procedural Guide within 30 calendar days of award that describes the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this order. The IT Security Plan shall comply with applicable Federal laws including, but not limited to, 40 U.S.C. 11331, the Federal Information Security Management Act (FISMA) of 2002, and the E-Government Act of 2002. The IT Security Plan shall meet IT security requirements in accordance with Federal and GSA policies and procedures, including General Services Administration Acquisition Regulation (GSAR) clause 552.239-71. The contractor shall submit written proof of IT security authorization six months after award, and verify that the IT Security Plan remains valid annually.

8.2.3 Recurring Security Deliverables

Deliverables to be provided to the GSA COR/ISSO/ISSM Quarterly

8.2.3.1. Vulnerability Scanning

Reference: NIST 800-53 control RA-5
Provide the most recent Web Application and Operating System vulnerability scan reports.

8.2.3.2. Plan of Action & Milestones (POA&M) Update

Reference: NIST 800-53 control CA-5
Provide POA&M updates in accordance with requirements and the schedule set forth in GSA CIO IT Security Procedural Guide 09-44, "*Plan of Action and Milestones (POA&M).*"

Deliverables to be provided to the GSA COR/ISSO/ISSM Annually

8.2.4 Updated A&A documentation including the System Security Plan and Contingency Plan

8.2.4.1 System Security Plan

Reference: NIST 800-53 control PL-2
Review and update the System Security Plan annually to ensure the plan is current and accurately describes implemented system controls and reflects changes to the contractor system and its environment of operation. The System Security Plan must be in accordance with NIST 800-18, Revision 1, *"Guide for Developing Security Plans."*

8.2.4.2 Contingency Plan

Reference: NIST 800-53 control CP-2
Provide an annual update to the contingency plan completed in accordance with NIST 800-34, *"Contingency Planning Guide."*

8.2.5. User Certification/Authorization Review Documents

Reference: NIST 800-53 control AC-2
Provide the results of the annual review and validation of system users' accounts to ensure the continued need for system access. The user certification and authorization documents will illustrate the organization establishes, activates, modifies, reviews, disables, and removes information system accounts in accordance with documented account management procedures.

8.2.6 Separation of Duties Matrix

Reference: NIST 800-53 control AC-5
Develop and furnish a separation of duties matrix reflecting proper segregation of duties for IT system maintenance, management, and development processes. The separation of duties matrix will be updated or reviewed on an annual basis.

8.2.7 Information Security Awareness and Training Records

Reference: NIST 800-53 control AT-4
Provide the results of security awareness (AT-2) and role-based information security technical training (AT-3). AT-2 requires basic security awareness training for employees and contractors that support the operation of the contractor system. AT-3 requires information security technical training to information system security roles. Training shall be consistent with the requirements contained in C.F.R. Part 5 Subpart C (5 C.F.R 930.301) and conducted at least annually.

8.2.8 Annual FISMA Self-Assessment

Reference: NIST 800-53 control CA-2
Deliver the results of the annual FISMA self-assessment conducted per GSA IT Security Procedural Guide 04-26, "*Federal Information Security Modernization Act (FISMA) Implementation."* Based on the controls selected for self-assessment, the GSA OCISO will provide the appropriate test cases for completion.

8.2.9 System(s) Baseline Configuration Standard Document

Reference: NIST 800-53 control CM-2/CM-2(1)
Provide a well-defined, documented, and up-to-date specification to which the information system is built.

8.2.10 System Configuration Settings Verification

Reference: NIST 800-53 control CM-6/CM-6(1)
Establish and document mandatory configuration settings for information technology products employed within the information system that reflect the most restrictive mode consistent with operational requirements. Configuration settings are the configurable security-related parameters of information technology products that compose the information system. Systems should be configured in agreement with GSA technical guidelines, NIST guidelines, Center for Internet Security guidelines (Level 1), or industry best practice guidelines in hardening their systems, as deemed appropriate by the Authorizing Official.
Provide the most recent operating system Configuration Settings Compliance scan report.

8.2.11 Configuration Management Plan

Reference: NIST 800-53 control CM-9
Provide an annual update to the Configuration Management Plan for the information system.

8.2.12 Contingency Plan Test Report

Reference: NIST 800-53 control CP-4
Provide a contingency plan test report completed in accordance with GSA IT Security Procedural Guide 06-29, *"Contingency Planning."* A continuity test shall be conducted annually prior to mid-July of each year. The continuity test can be a table top test while the system is at the FIPS PUB 199 Low Impact level. The table top test must include Federal and hosting Contractor representatives. Functional exercises must be completed once every three years for FIPS PUB 199 Moderate impact systems and annually for FIPS PUB 199 High impact systems.

8.2.13 Incident Response Test Report

Reference: NIST 800-53 control IR-3
Provide an incident response plan test report documenting results of incident reporting process per GSA IT Security Procedural Guide 01-02, *"Incident Response."*

8.2.14 Information System Interconnection Agreements

Reference: NIST 800-53 control CA-3
Provide Interconnection Security Agreements (ISA) and supporting Memorandum of Agreement/Understanding (MOA/U), completed in accordance with NIST 800-47, *"Security Guide for Connecting Information Technology Systems,"* for existing and new interconnections. Per NIST 800-47, an interconnection is the direct connection of two or more IT systems for the purpose of sharing data and other information resources through a pipe, such as ISDN, T1, T3, DS3, VPN, etc. ISAs shall be submitted as appendices as part of the annual System Security Plan submission. ISAs shall include, if applicable, any changes since the last submission; updated ISAs are required at least every three years.

8.2.15 Rules of Behavior

Reference: NIST 800-53 control PL-4
Define and establish Rules of Behavior for information system users. Rules of Behavior shall be submitted as an appendix to the System Security Plan.

8.2.16 Penetration Testing Report

Reference: NIST 800-53 control CA-8
All Internet accessible systems, and all FIPS PUB 199 High impact systems are required to complete an independent penetration test and provide a Penetration Test Report documenting the results of the exercise as part of their A&A package. Annual penetration tests are required for these same systems in accordance with GSA Order CIO 2100.1 and CIO-IT Security-11-51, "*Conducting Penetration Test Exercises.*"

8.2.17 Personnel Screening and Security

Reference: NIST 800-53 control PS-3, NIST 800-53 control PS-7
Furnish documentation reflecting favorable adjudication of background investigations for all personnel (including subcontractors) supporting the system. Contractors shall comply with GSA Order CIO 2100.1, *"GSA Information Technology (IT) Security Policy"* and GSA Order, CIO P 2181.1, "*Homeland Security Presidential Directive-12 (HSPD-12) Personal Identity Verification and Credentialing Handbook*." GSA separates the risk levels for personnel working on Federal computer systems into three categories: Low Risk, Moderate Risk, and High Risk.

- Those contract personnel (hereafter known as "Applicant") determined to be in a Low Risk position will require a National Agency Check with Written Inquiries (NACI) investigation.
- Those Applicants determined to be in a Moderate Risk position will require either a Limited Background Investigation (LBI) or a Minimum Background Investigation (MBI) based on the Contracting Officer's (CO) determination.
- Those Applicants determined to be in a High Risk position will require a Background Investigation (BI).

Applicants will not be reinvestigated if a prior favorable adjudication is on file with FPS or GSA, there has been less than a one year break in service, and the position is identified at the same or lower risk level.

Once a favorable FBI Criminal History Check (Fingerprint Check) has been returned, Applicants may receive a GSA identity credential (if required) and initial access to GSA information systems. The HSPD-12 Handbook contains procedures for obtaining identity credentials and access to GSA information systems as well as procedures to be followed in case of unfavorable adjudications.

Deliverables to be provided to the GSA COR/ISSO/ISSM Biennially

8.2.18 Policies and Procedures

Develop and maintain current the following policies and procedures:

a. Access Control Policy and Procedures (NIST 800-53 AC-1)
b. Security Awareness and Training Policy and Procedures (NIST 800-53 AT-1)
c. Audit and Accountability Policy and Procedures (NIST 800-53 AU-1)
d. Identification and Authentication Policy and Procedures (NIST 800-53 IA-1)
e. Incident Response Policy and Procedures (NIST 800-53 IR-1, reporting timeframes are documented in GSA IT Security Procedural Guide 01-02, "Incident Response"
f. System Maintenance Policy and Procedures (NIST 800-53 MA-1)
g. Media Protection Policy and Procedures (NIST 800-53 MP-1)
h. Physical and Environmental Policy and Procedures (NIST 800-53 PE-1)
i. Personnel Security Policy and Procedures (NIST 800-53 PS-1)
j. System and Information Integrity Policy and Procedures (NIST 800-53 SI-1)
k. System and Communication Protection Policy and Procedures (NIST 800-53 SC-1)
l. Key Management Policy (NIST 800-53 SC-12)

8.3 Employee Security Requirements

The contractor shall provide personnel who already have or are capable of attaining and maintaining a Tier 2S security fitness determination. No access will be given to the Government computer information systems and Government sensitive information before the background investigation is completed.

8.3.1 New Contractor Personnel

The full names of all contractor personnel proposed to work under this contract must be submitted to the COR and GSA Security for initiation and/or verification of an individual's security clearance investigation status. No work shall commence under the contract until GSA has received either an initial Enter on Duty Date (EoDD) or a final favorable adjudication and have been approved to work on the contract.

8.3.2 Departing Contractor Personnel

The Contractor shall notify the COR, Contracting Officer and the GSA Personnel Security Officer when Contractor personnel will no longer be working on the contract. The Contractor must then turn in all badges; Government furnished equipment, and deliverables and provide an updated listing of GFE.

8.4 Common Access Card & ID Badges

When Government facilities are utilized in performance of this contract, the Government will provide photo identification, such as Common Access Card (CAC) and Restricted Area Badge (as required). The Contractor shall comply with all requirements necessary to obtain a CAC and Restricted Area Badge. Once issued, these credentials will allow Contractor employees unescorted entry into Government facilities.

8.5 Facility Security Requirements

The contractor needs to apply for the GSA access card (PIV) so its personnels can come to government facilities for meetings or in-person activities. See section 8.4 for ID Badges.

8.6 Personal Identity Verification

The Contractor shall comply with the following Personal Identity Verification clause.

52.204-9, Personal Identity Verification of Contractor Personnel. (Jan 2006)
(a) The Contractor shall comply with agency personal identity verification procedures identified in the contract that implement Homeland Security Presidential Directive-12 (HSPD-12), Office of Management and Budget (OMB) guidance M-05-24, and Federal Information Processing Standards Publication (FIPS PUB) Number 201.
(b) The Contractor shall insert this clause in all subcontracts when the subcontractor is required to have physical access to a federally-controlled facility or access to a Federal information system.

8.7 Additional Security Requirements

"Contracts involving GSA information systems must incorporate the CIO 09-48 IT Security Procedural Guide: Security and Privacy IT Acquisition Requirements and

CIO 12-2018 IT Policy Requirements Guide. Incorporating applicable requirements from these guides will ensure GSA information systems are secure and compliant with relevant laws.

- ***GSA Information Systems: Ensure contractor implements the requirements identified in MV-19-04 [PDF - 263 KB] --***
  - ***CIO 09-48, IT Security Procedural Guide: Security and Privacy IT Acquisition Requirements [DOCX - 277 KB]***
  - ***CIO 12-2018, IT Policy Requirements Guide [PDF - 277 KB]***

End of Clause

9. SPECIAL INSTRUCTIONS

9.1 Contractor Performance Assessment Reporting System (CPARS) Assessment

Upon request by the Government, the contractor shall submit a self-evaluation of their performance at least annually utilizing a Government provided template. From time of Government request, the contractor shall have 7 business days to provide input to the GSA COR. The contractor self-assessment will then be submitted to the Government client where they will utilize this information to formulate an independent performance evaluation that will be processed through the Contractor Performance Assessment Reporting System. The requirements of the FAR and its supplements as it pertains to CPARS reporting shall be adhered to.

9.2 Personal Services

This is not a “Personal Services” contract as defined by FAR 37.104. The government has taken the following steps and precautions to ensure that “Personal Services” employer-employee relationships are not created between government and contractor employees during performance of this task order. Although Contractor employees who furnish services under this contract are subject to Government technical oversight, neither the Government nor a Government authorized third party contractor or representative shall oversee Contractor employees but shall provide all direction through the Contractor’s designated representative(s) who is/are solely responsible for supervising and managing Contractor employees. In further compliance with this regulation:

- All tasks will be initiated using approved Task Directive Forms, email, Agile tools (such as Jira) or other approved form of documentation.
- All government direction or approval of contractor initiated suggestions shall be documented using approved Task Directive Forms or other approved form, email, Agile tools of documentation
- All government contract monitors shall communicate with the contractor through the approved contractor management representative.
- All government representatives responsible for managing this task order shall be briefed on the avoidance of personal services and those actions that represent personal services, prior to assuming their contract responsibilities.

9.3 Privacy Act

Work on this project may require that contractor personnel have access to information which is subject to the Privacy Act of 1974. Personnel shall adhere to the Privacy act, Title 5 of the U.S. Code, Section 552a and applicable agency rules and regulations when handling this information. Privacy Act information is considered sensitive and appropriate safeguards shall be implemented by the contractor. The contractor is responsible for ensuring all contractor personnel are briefed on privacy Act requirements.

9.4 Rehabilitation Act Compliance (Section 508)

Unless otherwise exempt, all services and/or products provided in response to this requirement shall comply with Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d), and the Architectural and Transportation Barriers Compliance Board Electronic and Information Technology (EIT) Accessibility Standards (36 CFR part 1194).

The Contractor shall support the Government in its compliance with Section 508 throughout the development and implementation of the work to be performed. Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d) requires that when Federal agencies develop, procure, maintain, or use electronic information technology, Federal employees with disabilities have access to and use of information and data that is comparable to the access and use by Federal employees who do not have disabilities, unless an undue burden would be imposed on the agency. Section 508 also requires that individuals with disabilities, who are members of the public seeking information or services from a Federal agency, have access to and use of information and data that is comparable to that provided to the public who are not individuals with disabilities, unless an undue burden would be imposed on the agency.

Additional information regarding Section 508 can be obtained from the following web sites:

http://www.section508.gov/index.cfm?FuseAction=Content&ID=12
http://www.access-board.gov/508.htm
http://www.w3.org/WAI/Resources

9.5 Final Invoice and Release of Claims

The contractor is required as a deliverable of the contract/order to provide a final invoice no later than 30 calendar days after the end of the period of performance. Additionally, the contractor shall provide a Release of Claims no later than 90 calendar days after the end of the period of performance. The contract/order will be modified for closeout.

9.6 Other Direct Costs (ODCs)

The Government may require the contractor to purchase materials and equipment and ODCs, to include hardware, software, and related supplies critical and related to the services being acquired under the contract/order. Such requirements will be identified at the time the contract/order is issued or may be identified during the course of a contract/order by the Government or the contractor. If the contractor initiates a purchase within the scope of the contract/order and the prime contractor has an approved purchasing system, the contractor shall submit to the GSA COR a Request to Initiate Purchase (RIP) (PWS Attachment E). If the prime contractor is to lose or does not have an approved purchasing system, the contractor shall submit to the CO a Consent to Purchase (CTP) (PWS Attachment F). The RIP and CTP shall include the purpose, specific items, estimated cost, cost comparison, and rationale. The contractor shall not

make any purchases without an approved RIP from the GSA COR or an approved CTP from the CO.

9.6.1 Cost of Software Maintenance Renewals

The government shall require the contractor to purchase and maintain records and licenses of all Software Maintenance Renewals listed in the FPDS and SAM FY Inventory prior to their renewal dates. This must still follow all rules and regulations set in place above.

9.7 Avoidance and/or Mitigation of Actual or Potential Organizational Conflicts of Interest

Contractor employees may have access to sensitive government information while performing this work, may be involved in reviewing and assessing the work of other contractors, and may be involved in developing specifications and work statements for subsequent or complementary work. There is a potential for organizational conflicts of interest if the Contractor has ties with firms whose work it will review or if the Contractor is subsequently awarded a contract that uses a specification or work statement that it prepared. To avoid actual or potential organizational conflicts of interest the Contractor, in conjunction with Government scheduling and oversight controls, must be able to mitigate its relationship with a firm whose work it might review during performance of this Task Order. No specific firm is currently identified but firm may be identified during the course of contract/task order performance. Additionally, the Contractor shall refrain from seeking contracts that incorporate Contractor generated specifications or work statements until it first demonstrates, to the satisfaction of the Contracting Officer, that obtaining such other contracts will not create an actual or potential organizational conflict of interest with work performed on this task order. The Contractor shall comply with the provisions of the task order clauses entitled “Organizational Conflicts of Interest,” “Notification of Conflicts of Interest Regarding Personnel,” “Limitation of Future Contracting,” and “Annual Conflict of Interest Certification” to meet this requirement, which shall be incorporated into the Task Order.

9.8 Task Order Management

9.8.1 Contracting Officer’s Representative (COR)

The Government Contracting Officer is primarily responsible for managing this contract / order. Additionally, the work to be performed under this contract / order is subject to monitoring by an assigned Contracting Officer’s Representative (COR). The COR appointment letter, outlining the COR responsibilities under this contract/order, will be provided to the contractor under separate cover upon request. Questions concerning COR appointments should be addressed to the Contracting Officer.

9.8.2 Government Technical Representative

In addition to the COR, the Government may assign one or more Technical Representatives to monitor the technical aspects of this contract / order. The Government Technical Representative will participate in project meetings and review task order deliverables and will provide technical assistance and clarification required for contract / order performance. Refer to the attached QASP for specific information on project monitoring.

9.9 Technical Direction

All work shall be performed within the scope of this PWS and the Government will not ask or require the Contractor to perform work that is outside of the scope of this Contract/Task Order. Clarification to the work may be provided to the Contractor in writing by the Contracting Officer's Representative (COR) using a Technical Directive form or other agreed upon written documentation. The Contractor's representative shall acknowledge receipt of such technical direction in writing. If specific tasks that fall within the scope of the performance objectives of this PWS are requested, amplified, or clarified by written technical direction, the Contractor shall comply with that direction, which shall become a part of this task order. Technical direction shall be provided at the management level and Contractor employees shall perform work as specified in this Contract/Task Order as directed by the Contractor's designated project manager, who shall have full responsibility for the assignment and monitoring of Contractor employee activities.

Task directives may include deliverables that are not initially identified in this task order. If so, task directives shall include specific delivery dates and places for reports and studies or a specific completion date for support services. As an alternative, the task directives may require the Contractor to establish timelines and milestones for completion of tasks. Government specified delivery or completion dates and Government approval of Contractor proposed timelines or milestones shall be binding on the Contractor.

Technical direction does not change the total dollar value of the contract or order; however, the dollar value of specific work identified in the technical directive may be obtained from the contractor for administrative purposes (e.g. proper allocation of funds, payment of invoices).

If the Contractor believes that any technical direction requires performance of work that is outside the scope of this contract / order, the Contractor shall immediately contact the Contracting Officer.

9.10 Data Ownership/Release/Availability/Rights

All Government data collected in the system is the property of the Federal Government. All data collected by the system shall be provided by the Contractor (system provider) as requested during the contract period and at the completion of the contract period in an electronic open standard data format that is easily reusable. The data shall be provided to the Government at no additional cost. The Government shall be afforded 14 calendar days to verify and validate the data and the Contractor shall be required to correct performance if errors or omissions are found.

Any information made available to the Contractor by the Government shall be used only for the purpose of carrying out the provisions of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of the contract. In performance of this contract, the Contractor assumes responsibility for the protection of the confidentiality of Government records and shall ensure that all work performed by its subcontractors shall be under the supervision of the Contractor or the Contractor's responsible employees. Each officer or employee of the Contractor or any of its subcontractors to whom any Government record may be made available or disclosed shall be notified in writing by the Contractor that information disclosed to such officer or employee can be used only for that purpose and to the extent

authorized herein. Further disclosure of any such information, by any means, for a purpose or to an extent unauthorized herein, may subject the offender to criminal sanctions imposed by 18 U.S.C. §§ 1030.

The Contractor will not disclose Customer Data to any government or third party or access or use Customer Data; except in each case as necessary to maintain the Cloud Services or to provide the Cloud Services to Customer in accordance with this contract, or as necessary to comply with the law or a valid and binding order of a governmental or regulatory body (such as a subpoena or court order). Unless it would be in violation of a court order or other legal requirement, the Contractor will give the Government reasonable notice of any such legal requirement or order, to allow the Government to seek a protective order or other appropriate remedy.

The data must be available to the Government upon request within one business day or within the timeframe negotiated with the Contractor, and shall not be used for any other purpose other than that specified herein. The Contractor shall provide requested data at no additional cost to the government.

The Government will retain unrestricted rights to government data. GSA must own and control its data, interfaces, processes, business rules and information with the ability to export easily and readily to other applications/systems/ Contractors in readable, usable formats, without added investments as the need arises. GSA retains ownership of any user created/loaded data and applications hosted on vendor's infrastructure, as well as maintains the right to request copies of these at any time.

9.11 Data Rights

The Government shall have unlimited royalty free rights to all data originally developed, generated and delivered under this contract or order as prescribed by the clause entitled **Rights in Data—General** (FAR 52.227-14 **)** which is incorporated into this task order or into the indefinite quantity contract upon which this order is based. The Contractor shall retain all rights to data used to meet the requirements of this task order if developed solely at the Contractor's expense for their commercial applications and sales.

The Government shall have the right to use all commercially developed and privately funded data delivered under this contract or order in accordance with, and subject to, the published agreements and restrictions that accompany that data.

9.12 Limited Use of Data

All data delivered or made available to the Contractor as Government Furnished Data shall remain the property of the Government and shall only be used by the Contractor in the performance of this contract or order. The Government retains all rights to Government Furnished Data.

At the conclusion of this contract/order all Government Furnished Data shall be dealt with according to the disposition instruction provided by the Contracting Office. If the Contracting Officer fails to provide disposition instruction for Government Furnished Data within thirty days of contract/task order end, the Contractor shall return all hard copy data and delete or otherwise destroy all electronic data.

9.13 Proprietary Data

The Contractor shall not employ the use of any proprietary data or software in the performance of this contract without the advanced written consent of the Contracting Officer.

9.14 Inspection and Acceptance

Inspection and acceptance will occur in accordance with the clause entitled Inspection of Services – Time and Material and Labor Hour (FAR 52.246-6) or Inspection of Services – Fixed Price (FAR 52.246-4), or) Inspection-Supplies - Fixed Price FAR 52-246-2(I), as applicable.

Payment for the correction of defective or deficient work will be handled as follow:

The Contractor will not be paid for re-performance of defective or deficient fixed priced services per the clause FAR 52-246-4(e) Inspection of Services-FP].

The Contractor will not be paid profit associated with re-performance of any defective or deficient time and material or labor hour work per the clause FAR 52-246-6 (f) Inspectioin-T&M.

In the absence of other agreements negotiated with respect to time provided for government review or specifically stated in other parts of this PWS, deliverables will be inspected and the contractor notified of the Government's Technical Representative's findings within five (5) work days of normally scheduled review. Unacceptable or unsatisfactory work will be handled as outlined in the QASP. Acceptance of invoices shall constitute acceptance of performance.

Inspection and acceptance shall be at destination.

9.15 Contract Type

This contract / order will be awarded using a combination fixed price and labor hour contract type.

9.16 Ceiling Price Notification

Per clause 52.323-7, Payments under Time-and-Materials and Labor-Hour Contracts, the contractor is reminded – "If at any time the Contractor has reason to believe that the hourly rate payments and travel costs that will accrue in performing this contract in the next succeeding 30 days, if added to all other payments and costs previously accrued, will exceed 85 percent of the ceiling price in the Schedule, the Contractor shall notify the Contracting Officer giving a revised estimate of the total price to the Government for performing this contract with supporting reasons and documentation."

9.17 Task Order Funding

It is anticipated that the task order will be fully funded. However, if incrementally funded, the following provision applies.

Incremental Funding

(GSA 5QZA AOD Memo, Subject: Incremental Funding-3 2009 01 (revised 07-23-09)

This project may be incrementally funded. If incrementally funded, funds will be added to this task via a unilateral modification as they become available. Contractor shall not perform work resulting in charges to the government that exceed obligated funds.

The Contractor shall notify the Contracting Officer in writing, whenever it has reason to believe that in the next 60 days, when added to all costs previously incurred, will exceed 75% of the total amount so far allotted to the contract/order by the Government. The notice shall state the estimated amount of additional funds required to complete performance of the contract/order for the specified period of performance or completion of that task.

Sixty days before the end of the period specified in the Schedule, the Contractor shall notify the Contracting Officer in writing of the estimated amount of additional funds, if any, required to continue timely performance under the contract/order or for any further period specified in the Schedule or otherwise agreed upon, and when the funds will be required.

The government is not obligated to reimburse the Contractor for charges in excess of the obligated funds and the Contractor is not obligated to continue performance or otherwise incur costs that would result in charges to the government in excess of the amount obligated under this order.

End of clause

9.18 Material and Material Handling Costs

Material and material handling costs will be paid as provided in FAR 52.232-7(b) “Payments under Time-and-Materials and Labor-Hour Contracts”. Material overhead will not be authorized if the costs normally included in that overhead (purchasing staff or other material handling costs) are being directly charged to this contract/task order.

9.19 Productive Direct Labor Hours

The Contractor shall only charge for labor hours when work is actually being performed in connection with this Task Order and not for employees in a “ready” status only. For this task order 1 FTE (full time equivalent) = 1920 labor hours.

9.20 Invoicing and Payment

Payments will be made in accordance with the clause entitled Payments (FAR 52.232-1) or Payments under Time-and-Materials and Labor-Hour Contracts (FAR 52.232-7), as applicable to each task order.

The Contractor may invoice for items upon their delivery or services when rendered. Billing and payment shall be accomplished in accordance with contract terms and GSA payment procedures. Invoice submission instructions shall be provided at the time of award.

9.21 Payment for Unauthorized Work

The Contractor will not be paid for the performance of work that is not authorized under this Task Order. No payments will be made for any unauthorized supplies and/or services or for any unauthorized changes to the work specified herein. This includes any services performed by the Contractor on their own volition or at the request of an individual other than a duly appointed CO, COTR, or Government Technical Representative. Only a duly appointed CO is authorized to change the specifications, terms, or conditions under this effort.

10 ATTACHMENTS

Attachment A – Contractor Non-Disclosure Agreement

Attachment B – QASP (Quality Assurance Surveillance Plan)

Attachment C – FPDS SLA (Service Level Agreement)

Attachment D – FPDS FY20 Software Inventory

Attachment E – FPDS AWS Server List

Attachment F – FPDS NonProd Network Architecture

Attachment G – FPDS Production and Coop Network Architecture

Attachment H – FPDS Monthly Steward Report Metrics

Attachment I – SAM.gov SLA (Service Level Agreement)

Attachment J – SAM Integration Software List

Attachment K – SAM Integration Environment Prod & Non-Prod Server

Attachment L – SAM iProd VPC Environment

Attachment M – CIO 12-2018_ IT Policy Requirements Guide

Attachment N – IT Security Procedural Guide

CONTRACTOR EMPLOYEE NON-DISCLOSURE AGREEMENT

I understand that in the performance of my official duties under contract number TBD (Solicitation No. ID16210006), task/delivery order number ID05180034 between the U.S. General Services Administration and my employer, XYZ, Corp., I may have access to sensitive government or third party contractor information or proprietary business information. I, as a Government contractor, certify that I will not disclose, publish, divulge, release, or make known, in any manner or to any extent, to any individual other than an appropriate or authorized Government employee, with a specific need to know, the content of any sensitive information to which I have access or which is presented to me by the Contracting Officer or other Government Official during the course of my employment, or any time thereafter.

I understand that for the purpose of this agreement, procurement sensitive information and proprietary business information include procurement data, contract information, plans, strategies, trade secrets, financial and cost and price data, technical proposals and any other information that the government or a third party contractor may deem sensitive.

I agree that the described information is "inside information" and shall not be used for private gain by myself or another person, particularly one with whom I have family, business, or financial ties. For the purposes of this agreement, "inside information" means information obtained under Government authority which has not become part of the body of public information. I specifically will not disclose any such information to employees of my company or any other contractor employees who have not signed this agreement. I will take all reasonable precautions to prevent the unauthorized disclosure and use of such information. I agree that I shall not release, publish, or disclose such information to unauthorized personnel, and I shall protect such information in accordance with relevant laws and regulations available for research and review at any Law Library. Among these laws may be various provisions of:

a) 18 U.S.C. 641 (Criminal Code: Public Money, Property or Records; 2 pgs. long)
b) 18 U.S.C. 1905 (Criminal Code: Disclosure of Confidential Information; 2 pgs. long)
c) Public Law 96-511 (Paperwork Reduction Act; Encyclopedic in length)

I hereby certify that I have read the non-disclosure agreement described above and I am familiar with the directives and policies governing the disclosure of procurement sensitive information. I will fully and completely observe these directives and will not disclose such information to any unauthorized person during or after performance of my duties under the contract and task/delivery order referenced above. I affirm that I have received a written and/or verbal briefing by my company concerning my responsibilities under this agreement. I understand that violation of this agreement may subject me to criminal and civil penalties.

_____
Employee Signature Date

_____
Employee's typed/printed name

_____
Witness Signature Date

_____
Witness's typed/printed name

QUALITY ASSURANCE SURVEILLANCE PLAN (QASP)

FOR

Task Order ITSS Solicitation # ID16210006
FPDS & SAM Integration Environment O&M

A procurement by the
U.S. General Services Administration
Region 5 Federal Acquisition Service, Acquisition Operations Division
on behalf of
National Marketing and Communications Division (NMCD)
Chicago, Illinois

NAICS 541519 – Other Computer Related Services
DB02 IT and Telecom – Compute Support Services, Non-HP

Introduction

This QASP (Quality Assurance Surveillance Plan) has been developed in accordance with FAR 46.4.

This QASP has been developed to provide an effective and systematic method for monitoring, evaluating, and documenting contractor performance of the requirements in the PWS (Performance Work Statement), SOW (Statement of Work), or SOO (Statement of Objectives) of this task order. The government will monitor contractor performance to assess the acceptability of the services provided or items delivered and not the details of how the contractor accomplishes the work.

The Government retains the right to inspect all services and supplies furnished under this contract / order in accordance with the provisions of the contract regardless of their specific inclusion in this QASP.

Contractor Responsibility

The contractor, and not the government, is responsible for managing work, ensuring that performance is satisfactory and compliant with contract provisions, and performing quality control and quality assurance functions to ensure that products and/or services meet contract requirements. Additionally, the contractor is responsible for taking all actions necessary to correct unsatisfactory, deficient, or non-compliant work.

Surveillance Monitoring

Contractor performance under this task order will be monitored by the GSA Contracting Officer's Representative (COR).

Surveillance methods will include review and analysis of services and end items, monitoring timeliness of deliveries, and observance of management practices and professionalism exhibited by contractor employees. The specific performance objectives are listed and described in the PWS/SOW/SOO or in the following Surveillance Objectives, Measures, and Expectations (if applicable).

Responsibilities of the Contract Monitors

A. The Contracting Officer's Representative (COR), with assistance from subject matter experts (SMEs) if required, is responsible for monitoring, evaluating, and documenting contractor performance. The COR shall perform the following functions.

   1. Discuss performance requirements with the contractor during the pre-performance conference.

   2. Establish a schedule for routine monitoring events, if applicable.

   3. Review, monitor, and evaluate all items (services performed, work products, and/or delivered items) as listed in the PWS/SOW/SOO in accordance with the stated performance measures. Verification of the level of performance compliance shall be performed by analysis, demonstration, inspection, or test. The evaluator shall determine the degree to which contractor performance meets the established performance standards.

4. Verify timeliness of deliveries and performance.

5. Hold performance assessment meetings with the government SMEs and management, if required.

6. Complete and/or compile performance documents for each evaluation period. These documents include—
   a. The Contractor's Monthly Project Status Reports, if applicable.
   b. The Contractor's Monthly Labor Hour and Expenditure Report, if applicable.
   c. The Contractor Performance Report (using the CPARS (Contractor Performance Assessment Reporting System) Standard Contractor Performance Report, or other approved reporting document) - The Contractor Performance Report should be completed by the COR within two weeks after the end of each evaluation period. The Contractor Performance Report is to include the following information.
      (1) Contract or Order number
      (2) Dates of the evaluation period.
      (3) The standards and measures used to make performance evaluations.
      (4) Input from the contract monitors, COR and any assisting SMEs, including--
         (a) Observations of performance (positive, acceptable, negative, unacceptable, including both successful achievements and deficiencies) in each of the areas listed on the Performance Evaluation Report. This can include observations and input from stakeholders and those reliant upon or recipients of the contractor's performance.
         (b) Notation of deficiencies or non-compliance with contract or delivery order provisions, statement of work requirements, or task directives. These notations will include a narrative describing the deficiencies or non-compliance, a reference to the contractual provisions or requirement related to the deficient or non-compliant performance, and date the deficiency or non-compliance was discovered or became known.
      (5) The date and signature of the COTR, CR and/or ACR on each entry.
   d. Documentation of the date and time the contractor is notified of any deficiency. This documentation shall include a copy of the written deficiency notification sent to and acknowledged by the contractor.
   e. Documentation of the date and time the contracting officer is notified of any contractor deficiency.
   f. Documentation of the action(s) or inaction(s) taken by the contractor to correct any deficiency.
   g. Documentation shall be made on the Performance Evaluation Report (or AF Form 372, if applicable).

7. Ensure that the narrative of all observations is accurate and factual in every respect. The narrative shall be legible and provide the evaluator's observations, evaluation, and conclusions in precise descriptive language. Generalities, personal opinions and vague or ambiguous statements are not acceptable.

8. Provide an updated copy of the Contractor Performance Report to the requiring agency's program manager and to the contracting officer upon completion of the evaluation.

9. Meet with the contracting officer to—
   a. Report the results of contractor surveillance.

b. Report the requesting agency's acceptance of services.
c. Determine the government's plan of action in the event of unacceptable, unsatisfactory, deficient, or non-compliant contractor performance.

10. Recommend needed changes to the QASP to the Contracting Officer.

B. Any assigned technical monitors shall promptly notify the GSA COR should any significant contractor performance problem arise or become known between scheduled evaluation events.

C. The contract monitors are to be objective, fair, and consistent in evaluating contractor performance.

D. Upon completion of the contract or task order, all surveillance documentation shall be included in the contract file along with all other contract documents, i.e., Statement of Work and addenda, contract/task order and all modifications, meeting reports and minutes, correspondence pertaining to this contract or order, etc.

E. Contractor performance and surveillance documentation can be used to complete Contractor performance evaluations that are submitted to the past performance data base.

Taking Corrective Actions.

The government will promptly notify the contractor of any unsatisfactory, unacceptable, deficient, non-conforming, or non-compliant performance or deliverables. The contractor shall have the opportunity to review the government's determination and provide comments.

Any contractor performance problems that result from the failure of the government to fulfill any of its obligations under the contract or order, upon which contractor performance is dependent, will not be assessed and documented as contractor deficiencies or non-compliance, to the extent of Government liability.

The contractor shall be responsible for correcting all unsatisfactory, unacceptable, deficient, or non-compliant performance. For firm fixed-price contracts, the cost of re-performing unsatisfactory, unacceptable, deficient, or non-compliant work will be the sole responsibility of the Contractor, as prescribed by paragraph (e) of the clause entitle Inspection of Services — Fixed Price (Aug 1996)(FAR 52.246-4). For Labor-Hour contracts, the cost of re-performing unsatisfactory, unacceptable, deficient, or non-compliant work will be reimbursed at the approved labor hour rate less an amount for profit, as prescribed by paragraph (f) of the clause entitle Inspection—Time-and-Material and Labor-Hour (May 2001)(FAR 52.246-6).

Disputes between the Contractor and the COR / Agency Representative regarding surveillance results should be referred to the Contracting Officer.

Failure of the contractor to take appropriate and timely corrective action will result in the government's issuance of cure or show-cause notices or pursue other remedies set forth in the provisions of the contract or as provided by law.

When unsatisfactory work is not corrected or unacceptable work is not re-performed to the Government's satisfaction, in addition to other available remedies, the Government may negotiate a reduction in the contract or task order price to reflect the reduced value received.

Additionally, the government reserves the right to include any incidents of unsatisfactory, unacceptable, deficient, or non-compliant performance, especially if uncorrected, in the contractor's past performance record.

Revisions to this QASP

This QASP and its accompanying Surveillance Objectives, Measures, and Expectations, and Contractor Performance Report format shall remain unchanged during the life of this contract or order unless modified to provide clarification or to reflect changes in the PWS/SOW/SOO or other contractual provisions. All modification will be implemented by a contract or order modification signed by the Contracting Officer and the Contractor. Revisions to this QASP are the joint responsibility of the Contracting Officer, COR, and requiring agency representative.

SURVEILLANCE OBJECTIVES, MEASURES, AND EXPECTATIONS

- SERVICES -

PERFORMANCE OBJECTIVE

The Contractor shall perform the services necessary to perform the work set forth in the PWS/SOW/TAG.

PERFORMANCE MEASURES

Contractor performance will be evaluated using the following measures, consistent with CPARS (Contractor Performance Assessment Reporting System) Standard Contractor Performance Report requirements.

1. Quality:
(This is a multi-faceted performance measure that includes work excellence, completeness, effectiveness and document format and clarity)

(Excellence) Using this measure, the Government will assess the degree to which the work performed and items or documents delivered achieve a standard of excellence or adhere to rules established by a recognized authority as a standard of performance. For example, documents will be assessed to determine the degree to which they are technically sound and free of typographical, grammatical, mathematical, and conceptual errors. Using this measure, the Government will also evaluate the degree to which the required document(s) is suitable for assessing the impacts of all reasonable alternatives and how well the recommendations will meet the intended purpose(s).

(Completeness) Using this measure, the Government will assess the degree to which the Contractor identifies, includes, addresses and/or performs all pertinent aspects of the work or all pertinent elements of delivered items, data, or services. Using this measure, the Government will also assess the degree to which the Contractor performs all stipulated or planned activities and captures the results of those activities in the various documents that are to be delivered.

(Effectiveness) Using this measure, the Government will evaluate the degree to which the Contractor's performance (work, products, and data submissions) meets all goals and objectives established in both the PWS (Performance Work Statement), Government Task Directives, and in any required Contractor's project planning documents (e.g., assessments, analysis, project plan, WBS, or execution recommendations).

(Format & Clarity) Using this measure, the Government will assess the design, flow, matrix, and/or layout used by the Contractor to present data (whether presented physically, orally, or electronically). This assessment will focus on the degree of clarity and logical organization with which the data is presented and whether or not the format facilitates easy review and use of the material. Using this measure, the Government will assess the degree to which material presented in documents (narrative, tables, diagrams, footnotes, photographs, etc.) are easy to understand by the intended audience.

2. Schedule/Timeliness:
Using this measure, the Government will assess the degree to which the Contractor meets or exceeds the delivery schedule.

3. Cost Control:
Using this measure, GSA will assess the degree to which the Contractor is able to control costs and accomplish the work at a lower cost than estimated and established in the task order budget without compromising other aspects of performance, e.g., while maintaining quality and timeliness.
[Note: This measure allows for a flexible assessment of costs.]
[Note: This factor will not be evaluated if all work is performed on a fixed price basis.]

4. Business Relationship:
Using this measure, the Government will assess the level of professionalism exhibited by the Contractor staff in interactions with Government and other personnel in connection with work being performed under this or contract.

5. Management:
Using this measure, the Government will assess the degree to which the Contractor's management is able to competently direct the work, resolve problems, interface with government program managers and technical experts, and balance the resource triangle of quality, schedule, and cost.

5. Utilization of Small Business:
Using this measure, the Government will assess the degree to which the uses small businesses to perform the work in comparison to proposed small business use.
[Note: This factor will not be evaluated if all work is performed by the prime contractor.]

5. Security:
Using this measure, the Government will assess the degree to which the Contractor complies with all required security measures and specifications. Using this measure the government will also assess security incidents and violations and subsequent corrective actions taken by the contractor.

PERFORMANCE EXPECTATIONS

Performance will be evaluated against a Performance Criteria Matrix (if provided in the PWS/SOW/SOO or as a separate document) and/or the following Satisfactory Performance Expectations.

Satisfactory Performance Expectations:
The Government will rate the contractor's performance by comparing it against the following expectations for satisfactory performance. Performance ratings will be based on the degree to which the contractor fails to meet, meets, or exceeds these satisfactory performance expectations.

Quality:
The work described and the deliverables listed in the PWS (Performance Work Statement), SOW (Statement of Work), or SOO (Statement of Objectives) shall be performed per applicable regulations, industry standards, and contract/task order requirements.

The content of data deliverables shall address all of the areas and topics prescribed by the PWS/SOW/SOO. The information in the document(s) shall focus on the solution to the Government's need. Material in the documents should be appropriate and pertinent for the scope of the subject being addressed. Documents shall be submitted in the format described in the PWS/SOW/SOO.

If required by the PWS/SOW/SOO, planning documents shall reflect an adequate understanding of the subject matter and of planned and potential activities for this project. Planning documents shall address alternatives and present sound and workable conceptual and technical conclusions and recommendations that are supported by the data acquired during the investigation portion of this project.

Reports shall capture and clearly convey the information they are intended to address per the requirements of the PWS, e.g., project status and milestone updates, problems and solutions, financial and travel information, etc.

The document format should be well organized and clear, making the information easy to find and use. However, draft formats may need minor revision and some information may not be immediately identifiable. These problems should only require minimal effort to correct prior to final submission. Ideas will be logically presented. Documents should contain few, if any, technical errors or inconsistencies between the information presented and that contained in the source documents or raw data. Document(s) will be grammatically and mathematically correct, although drafts may contain errors that require minor editing changes or corrections prior to final submission. Document content shall be consistent with common practice and industry or other established standards or protocols.

Schedule/Timeliness:
The Contractor shall perform work and submit the required documents by the time stated in the delivery schedule of the task order.

Cost:
Final costs of performance shall be within the agreed upon and approved budget.

Professionalism:
All interactions between Contractor personnel and Government personnel shall be professional and appropriate.

Management:
Management will be responsible, responsive, and pro-active in directing the work, resolving problems, interfacing with government program managers and technical experts, and balancing the resource.

Small Business Utilization:
The Contractor shall use small business to the degree originally proposed.

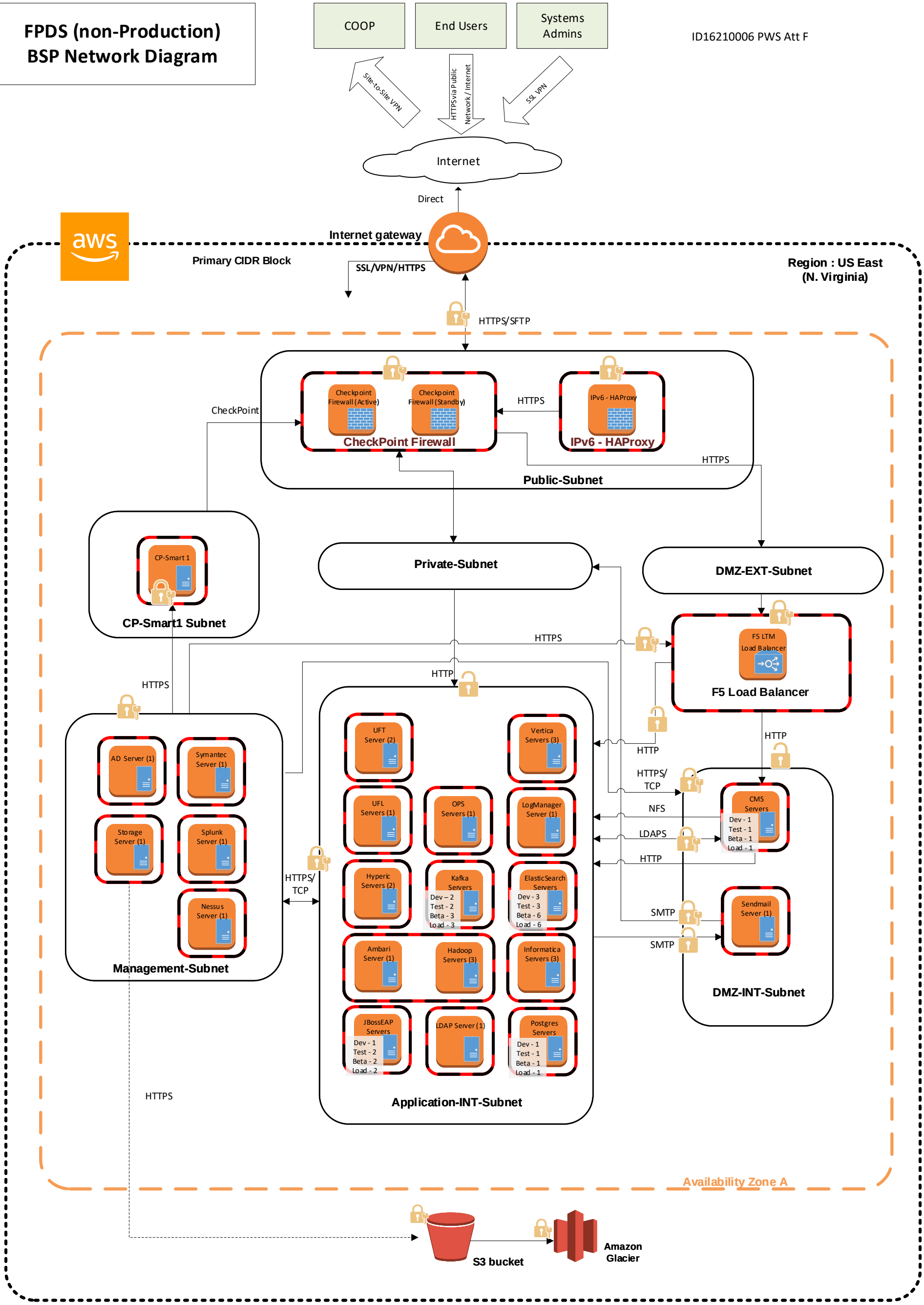
Security:
The Contractor shall comply with all required security measures and specifications and there shall be no security incidents and violations.

PERFORMANCE EVALUATION

The COR, or other Government representative responsible for evaluating Contractor performance, shall complete a contractor performance evaluation at least on an annual basis using the CPARS (Contractor Performance Assessment Reporting System) evaluation form. The report shall address each of the applicable performance measures as they specifically apply to the work described and deliverables furnished in conjunction with this contract/task order. Performance ratings will be based on the degree to which the contractor fails to meet, meets, or exceeds the above stated satisfactory performance expectations. Evaluation results will be provided to the contractor in their annual CPARS evaluation.

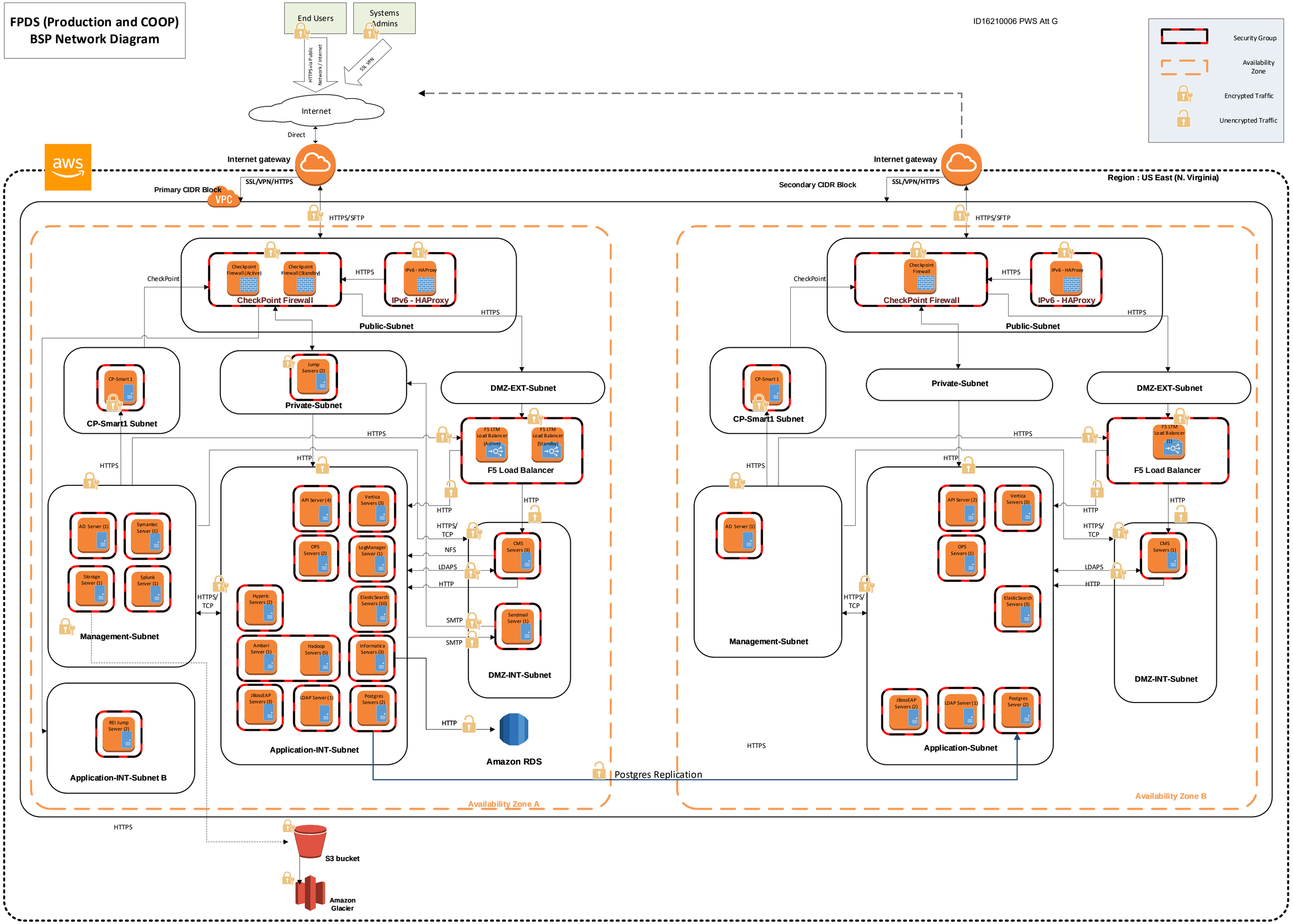
FPDS (non-Production) BSP Network Diagram

ID16210006 PWS Att F



FPDS (Production and COOP) BSP Network Diagram

ID16210006 PWS Att G



1.1 SAM Integration Environment SLA Measures

1.1.1 Measure #1: Help Desk Outstanding Ticket Age

Performance Requirement:	Help Desk Outstanding Ticket Age
Acceptable Quality Level (AQL):	**Less than 10% of all Tier 2 open tickets open are more than 30 days old**
Data Source:	The Help Desk Tracking Tool
How It Is Measured:	Number of tickets older than 30 days divided by the total ticket number of tickets escalated to Tier 2 in the period.
IBM's Approach for Achieving:	Tickets are reviewed daily by the Help Desk Lead. These are addressed on a first in first out basis. When it is determined that tickets open tickets are growing in age, the Help Desk lead will evaluate root causes and shift focus on the oldest tickets.
Data Accessibility:	GSA providing IBM the ability to have access to the help desk tool data for actual escalation time and date.
Restrictions:	Escalations from Tier 1 to Tier 2 must be at 10% or below. Tickets that have dependencies on Tier 3 or external agencies will not be counted. Reports containing metrics related to this metric will be provided to IBM by the third-party tool owner. System defects and enhancements that prevent closure of the ticket will not be counted since this is not a reflection of the Help Desk effectiveness.
IBM Owner:	Help Desk Lead

Pass Example: Current open ticket count as of the end of the month is 1,000. There are 70 tickets determined to be older than 30 days. Therefore 70/1000 = 7%

1.1.2 Measure #2: Help Desk Ticket Closure Rate

Performance Requirement:	Help Desk Ticket Closure Rate
Acceptable Quality Level (AQL):	**More than 90% of the total tickets escalated to Tier 2 over the last 30 days have been closed**
Data Source:	The Help Desk Tracking Tool
How It Is Measured:	Number of tickets closed in a month divided by the number of tickets escalated to Tier 2
IBM's Approach for Achieving:	The Help Desk Lead will assign resources, so ticket closure rate stays close to the number of those escalated to Tier 2. This is to ensure that open ticket counts do not increase over time.
Data Accessibility:	GSA providing IBM the ability to have access to the help desk tool data for actual escalation time and date.

Restrictions:	Escalations from Tier 1 to Tier 2 must be at 10% or below. Reports containing metrics related to this metric will be provided to IBM by the third-party tool owner.
IBM Owner:	Help Desk Lead

Pass Example: Throughout the course of the month, there were 3,000 help desk tickets escalated to Tier 2 help desk. Within the same period, 2,880 help desk tickets were closed. Therefore 2,880/3,000 = 96%

1.1.3 Measure #3: Help Desk Tickets Closed the Same Day

Performance Requirement:	Help Desk Tickets Closed the Same Day
Acceptable Quality Level (AQL):	**More than 30% of Tier 2 tickets closed within 72 hours**
Data Source:	The Help Desk Tracking Tool
How It Is Measured:	Number of monthly total tickets escalated to Tier 2 that are closed within 72 hours. The time starts when the ticket is placed in the Tier 2 queue and closed when set to 'Pending Customer'
IBM's Approach for Achieving:	Once a ticket is escalated and verified by the Help Desk lead as a properly escalated ticket, it is assigned to a Tier 2 agent. The agent will research the issue, provide a resolution and move the ticket to Pending Customer who has three days to respond before it is closed.
Data Accessibility:	GSA providing IBM the ability to have access to the help desk tool data for actual escalation time and date.
Restriction:	Escalations from Tier 1 to Tier 2 must be at 10% or below. Tickets that have dependencies on Tier 3 or external agencies will not be counted. Reports containing metrics related to this metric will be provided to IBM by the third-party tool owner. System defects and enhancements that prevent closure of the ticket will not be counted since this is not a reflection of the Help Desk effectiveness.
IBM Owner:	Help Desk Lead

Pass Example: Throughout the course of the month, there were 3,000 help desk tickets escalated to Tier 2 help desk. Within the period, there were 1,200 tickets that were closed within 72 hours. Therefore 1,200/3,000 = 40%

1.1.4 Measure #4: Help Desk Average Tier 2 Technical Initial Review Time

Performance Requirement:	Help Desk Average Initial Review Time
Acceptable Quality Level (AQL):	**Less than 3 (business days)**
Data Source:	The Help Desk Tracking Tool

How It Is Measured:	Determined from the time a Tier 2 ticket is escalated to the time is initially reviewed and the user has been contacted. (Business Days). IBM receives a document every week that measures the time it takes for Tier 2 agent to respond to a user after FSD has escalated the item.
IBM's Approach for Achieving:	Once a ticket is escalated to Tier 2 Technical, a Tier 2 agent should assign the ticket to themselves and contact the user immediately.
Data Accessibility:	GSA providing IBM the ability to have access to the help desk tool data for actual escalation time and date.
Restriction:	Escalations from Tier 1 to Tier 2 must be at 10% or below. Tickets that have dependencies on Tier 3 or external agencies will not be counted. Reports containing metrics related to this metric will be provided to IBM by the third-party tool owner. System defects and enhancements that prevent closure of the ticket will not be counted since this is not a reflection of the Help Desk effectiveness.
IBM Owner:	Help Desk Lead

1.1.5 Measure #5: Help Desk Average Tier 2 Close Time

Performance Requirement:	Help Desk Average Tier 2 Close Time
Acceptable Quality Level (AQL):	**Less than 5 (business days)**
Data Source:	The Help Desk Tracking Tool
How It Is Measured:	Determined from the time a Tier 2 ticket is escalated to the time it is closed. (Business Days)
IBM's Approach for Achieving:	Once a ticket is escalated and verified by the Help Desk lead as a properly escalated ticket, it is assigned to a Tier 2 agent. The agent will research the issue, provide a resolution and move the ticket to Pending Customer who has three days to respond before it is closed
Data Accessibility:	GSA providing IBM the ability to have access to the help desk tool data for actual escalation time and date.
Restriction:	Escalations from Tier 1 to Tier 2 must be at 10% or below. Tickets that have dependencies on Tier 3 or external agencies will not be counted. Reports containing metrics related to this metric will be provided to IBM by the third-party tool owner. System defects and enhancements that prevent closure of the ticket will not be counted since this is not a reflection of the Help Desk effectiveness.
IBM Owner:	Help Desk Lead

1.1.6 Measure #6: Help Desk Reopened Tier 2 Technical Tickets

Performance Requirement:	Reopened Tier 2 Technical Tickets
Acceptable Quality Level (AQL):	**Less than 5% Reopened**
Data Source:	The Help Desk Tracking Tool
How It Is Measured:	Tickets that were moved to resolved but reopened by the user because issue was not resolved. Service Now has a tool that allows you to see if any tickets were reopened during a period of time selected.
IBM's Approach for Achieving:	Tier 2 Technical Agents should not close any help desk tickets until they have verified with the user that the issue is resolved.
Data Accessibility:	GSA providing IBM the ability to have access to the help desk tool data for actual escalation time and date.
Restriction:	Escalations from Tier 1 to Tier 2 must be at 10% or below. Tickets that have dependencies on Tier 3 or external agencies will not be counted. Reports containing metrics related to this metric will be provided to IBM by the third-party tool owner. System defects and enhancements that prevent closure of the ticket will not be counted since this is not a reflection of the Help Desk effectiveness.
IBM Owner:	Help Desk Lead

1.1.7 Measure #7: Help Desk Foreign Registrant Tickets

Performance Requirement:	Help Desk Foreign Registrant Tickets
Acceptable Quality Level (AQL):	**Less than 25% of all Tier 2 Tickets are Foreign**
Data Source:	The Help Desk Tracking Tool
How It Is Measured:	Total count of Tier 2 tickets opened regarding foreign registrations
IBM's Approach for Achieving:	IBM maintains effective monitoring of the help desk queue, so issues reported by foreign registrations can be investigated immediately so other foreign entities do not experience the same issues.
Data Accessibility:	GSA providing IBM the ability to have access to the help desk tool data for actual escalation time and date.

Restriction:	Escalations from Tier 1 to Tier 2 must be at 10% or below. Tickets that have dependencies on Tier 3 or external agencies will not be counted. Reports containing metrics related to this metric will be provided to IBM by the third-party tool owner. System defects and enhancements that prevent closure of the ticket will not be counted since this is not a reflection of the Help Desk effectiveness.
IBM Owner:	Help Desk Lead

1.1.8 Measure #8: Reputation – Number of Reputation Incidents

Performance Requirement:	Number of Reputation Incidents
Acceptable Quality Level (AQL):	**Zero**
Data Source:	Stakeholder manual identification
How It Is Measured:	A reputation incident is one in which unapproved content is displayed on a production website, generally referred to as defacement. Defacement incidents are tracked across the environment as a whole (defacement of any website or component is treated the same). This is a yes/no metric. Time to recover from defacement contributes to unavailability calculations.
IBM's Approach for Achieving:	The IBM team continually strives to support GSA and its stakeholders to be successful. Activities outlined in the QCP support the quality efforts which include process controls, auditing, testing defect identification and defect correction. The integrity of all the AOCS systems is highly visible and any disruption or negative event can result in erosion of GSA's reputation.
Data Accessibility:	Incorrect data displayed on the website as result of a system issue where approved specification (data, functional or security) is not met. This is exclusive of extracts which fall under data quality. Data displayed as user entered or interfaced from another system will not be considered.
Restriction:	Agreement to reputation events will involve concurrence from FAS, CIO, COR and the IBM team.
IBM Owner:	All Team Members

1.1.9 Measure #9: Availability – Response Time

Performance Requirement:	Availability of www.sam.gov
Acceptable Quality Level (AQL):	**99.80%**

Data Source:	Rational Performance Test monitoring
FPDS Requirements:	Present a screen to users within 5 seconds Changes to the technical environment which may negatively impact data submission and/or reporting shall not be implemented between July and October
How It Is Measured:	Unavailable if system wide response takes longer than 5 seconds. Measured at the solution edge, net of scheduled maintenance. Calculated as the total hours of site availability per month divided by the total hours of a month. The site is considered unavailable when no external user is able to access the website.
IBM's Approach for Achieving:	The IBM team maintains the software and hardware of SAM. The hosting team continually monitors the servers and application for availability.
Data Accessibility:	Server and application monitoring tools are utilized to observe availability of the system.
Restriction:	Third party data center (hosting vendor) maintains 100% uptime.
IBM Owner:	Hosting & Infrastructure Lead

Example: The AOCS systems were unavailable for 1 hour on 10/5/2013. Since there are 31 days in October and 24 hours in a day, the total possible available hours are 744.

743/744= 99.86% = Pass

1.1.10 Measure #11: Availability - Extracts

Performance Requirement:	Availability of Extracts
Acceptable Quality Level (AQL):	**99.80%**
Data Source:	Stakeholder manual identification
How It Is Measured:	All Extracts will be posted and accessible for the time period of the approved specification. Unavailable if active users are unable to access the posted extracts. Calculated as the total hours of available extracts per month divided by the total hours of a month.
IBM's Approach for Achieving:	The IBM team continually monitors the SAM extracts for availability. Extracts are posted daily and undergo a quality control process of review prior to posting. Posted extracts are audited periodically for availability.
Data Accessibility:	Server and application monitoring tools are utilized to observe availability of the system.
Restriction:	Third party data center (hosting vendor) maintains 100% uptime.
IBM Owner:	Extracts & Interfaces Lead

Example: Extracts were unavailable for 1 hour on 10/5/2013. Since there are 31 days in October and 24 hours in a day, the total possible available hours are 744.

743/744= 99.86% = Pass

1.1.11 Measure #13: Availability – SAM Scheduled Maintenance

Performance Requirement:	Scheduled Maintenance
Acceptable Quality Level (AQL):	**Less than 16 Hours**
Data Source:	Hyperic Monitoring
Requirement:	System downtime (defined as the system is not accessible and operable by the user), will not exceed 8 hours per 12-month period (approximately 99.9% up time) exclusive of scheduled down time. Scheduled down time may occur not more frequently than once each month for a time period of up to 24 hours (noon Saturday to noon Sunday) with no scheduled down time during the month of September.
How It Is Measured:	Total scheduled downtime each month will not exceed 16 hours
IBM's Approach for Achieving:	IBM will request downtime at least 24 hours prior the maintenance window. Upon approval, the scheduled downtime will count towards the total available time for the month. The IBM team will work to minimize downtime by combining activities that require server reboot and therefore needing a scheduled maintenance window.
Data Accessibility:	Server and application monitoring tools are utilized to observe the activities of the system.
Restriction:	Unscheduled maintenance as a result of external agency failure in communication will not count against this metric. An example would be change in an external interface without prior notification resulting in the SAM servers requiring a reboot to resume normal operations. Exceptions must be approved by GSA.
IBM Owner:	Hosting & Infrastructure Lead

1.1.12 Measure #14: Availability – Interface Availability

Performance Requirement:	Availability of Interfaces
Acceptable Quality Level (AQL):	**97.00%**
Data Source:	Hyperic Monitoring
How It Is Measured:	Agency critical interfaces run within an hour of specific execution time. Calculated as the total hours of Interface availability per month divided by the total hours of a month.

IBM's Approach for Achieving:	IBM maintains a Master Interface spreadsheet that lists out those interfaces. Each interface specification outlines the time in which the interface needs to run. If an interface does not run within an hour of the specified time, the monitoring team will report this as a miss and research the reason for the late delivery. The team will continue to implement process improvements to address the root causes
Data Accessibility:	Manual interface monitoring and use of Interface Tracking spreadsheet.
Restriction:	Third party data center (hosting vendor) maintains 100% uptime.
IBM Owner:	Extracts & Interfaces Lead

There are 75 interfaces in total that SAM, maintains which are listed on the Interface Master List. If an interface is determined to not be operational, this is noted on the Interfaces Tracking Spreadsheet.

1.1.13 Measure #17: Business Process – Average Cycle Time

Performance Requirement:	A Record's Average Cycle Time
Acceptable Quality Level (AQL):	**7 Days or less**
Data Source:	Database Query
How It Is Measured:	The average time it takes a user to complete a registration and move from Draft to Active. The start time of a new or updated registration is captured by the system. The date and time in which a registration becomes active is also captured. All of the start times and activated times for a month are used calculate the average by using those records that were actually completed within the reporting period.
IBM's Approach for Achieving:	On a weekly basis, the IBM team provides a metric dashboard that contain the average cycle time. The team will continually look at ways in which reduction in cycle times can be achieved such as working with third party agencies to increase processing speed and performing maintenance on the application to expedite the user registration process.
Data Accessibility:	Database queries using PIT start and activation times.
Restriction:	IGT only registrations will be excluded as they are processed instantaneously. Pending CAGE or IRS will not exceed 7 days.
IBM Owner:	Extracts & Interfaces Lead

1.1.14 Measure #18: Business Process – Interface Jobs - Extracts (Daily)

Performance Requirement:	Interface Job Extracts (Daily)

Acceptable Quality Level (AQL):	**Less than 8 hours**
Data Source:	Database Query
How It Is Measured:	The average time it takes to generate the daily extract file
IBM's Approach for Achieving:	Continuous 24/7 monitoring and sends out the alert emails to the concerned Interface POC's if the interface is taking longer than usual or fixing the bug before it hits the SLA
Data Accessibility:	Automated monitoring emails which sends out every day to the team about the status of the interfaces, documented in Interface monitoring document
Restriction:	Includes only entity profiles within the federal government for many functions, including, procurement, contracts, payments, size determination, and validation
IBM Owner:	Extracts & Interfaces Lead

1.1.15 Measure #19: Business Process – Interface Jobs – Extracts (Monthly)

Performance Requirement:	Interface Job Extracts (Monthly)
Acceptable Quality Level (AQL):	**Less than 24 hours**
Data Source:	Database Query
How It Is Measured:	The average time it takes to generate the monthly extract file
IBM's Approach for Achieving:	Continuous 24/7 monitoring and sends out the alert emails to the concerned Interface POC's if the interface is taking longer than usual or fixing the bug before it hits the SLA
Data Accessibility:	Automated monitoring emails which sends out every day to the team about the status of the interfaces, documented in Interface monitoring document
Restriction:	Includes only entity profiles within the federal government for many functions, including, procurement, contracts, payments, size determination, and validation
IBM Owner:	Extracts & Interfaces Lead

1.1.16 Measure #20: Business Process – Exclusions Created

Performance Requirement:	Exclusions Created via e-mail or upload
Acceptable Quality Level (AQL):	**Less than 24 hours**
Data Source:	Database Query
How It Is Measured:	The average time it takes to generate an exclusion.

IBM's Approach for Achieving:	Continuous 24/7 monitoring and sends out the alert emails to the concerned Interface POC's if the interface is taking longer than usual or fixing the bug before it hits the SLA
Data Accessibility:	Automated monitoring emails which sends out every day to the team about the status of the interfaces, documented in Interface monitoring document
Restriction:	Does not include exclusions entered in via the front end.
IBM Owner:	Extracts & Interfaces Lead

1.1.17 Measure #21: Security - Outages due to security

Performance Requirement:	Outages due to security incidents (unplanned unavailability)
Acceptable Quality Level (AQL):	**No more than 1 outage per month**
Data Source:	Stakeholder manual identification
How It Is Measured:	Number of outages due to incidents (unplanned unavailability). Sam.gov is unavailable due to a security incident.
IBM's Approach for Achieving:	Continuous monitoring and improvements through vulnerability scanning and remediation, monthly patching, ongoing assessment and improvement of security controls through coordination with the ISSO and system owner
Data Accessibility:	Outages that are requested by GSA as a result of a formally defined security incident as outlined in IT Security Procedural Guide: Incident Response (IR) CIO-IT Security-01-02.
Restriction:	None
IBM Owner:	Information Assurance Lead

1.1.18 Measure #22: Security - Security Risks and Controls

Performance Requirement:	Proportion of information security risks for which satisfactory controls have been fully implemented
Acceptable Quality Level (AQL):	**90% deployed IAW approved schedule**
Data Source:	Stakeholder manual identification
How It Is Measured:	Security Related Items Identified on the POA&M have a plan of action and are remediated in the appropriate timeframe.
IBM's Approach for Achieving:	GSA and IBM will follow the Security Plan process of process of scanning and identifying potential vulnerabilities in the.gov applications.

Data Accessibility:	Plan of Action and Milestone (POA&M) report provided by GSA. As defined in the security requirements, all High POA&Ms are to be remediated within 30 days of being identified as a POA&M.
Restriction:	GSA will provide IBM monthly updates to content within the POA&M for SLA reporting. Pending or approved AoRs may override the POA&M requirement and therefore will not be counted. POA&M items may be approved by GSA to be completed in accordance with a scheduled maintenance window or FastPath or Quarterly release that is outside of the 30-day window. These approved items will not be included in the calculation. Exceptions beyond 30 days for remediation due to planned release scheduling must be approved by GSA.
IBM Owner:	Information Assurance Lead

Example: There were 20 POA&Ms identified in a month by GSA. 18 have been addressed within 30 days. 18/20 = 90% = Pass.

1.1.19 Measure #23: Security - Security Reporting Timeliness

Performance Requirement:	Time lag between detection, reporting and acting upon security incidents
Acceptable Quality Level (AQL):	**At least 90% of incidents addressed per response table**
Data Source:	Stakeholder manual identification
How It Is Measured:	Security incidents are responded to in the timeframes identified in current Incident Response Table
IBM's Approach for Achieving:	GSA and IBM will follow the Security Plan process of timely identification and reporting of security incidents. Weekly meetings between the GSA ISSO and IBM Information Assurance Lead will review any open security incidents.
Data Accessibility:	GSA ISSO to maintain and provide agreed upon incident response table.
Restriction:	GSA to provide IBM the Incident Response Table
IBM Owner:	Information Assurance Lead

1.1.20 Measure #24: Data Quality - Data Stewardship Quality Index

Performance Requirement:	Data Stewardship Quality Index
Acceptable Quality Level (AQL):	**Average 99.8% across the relevant time period**
Data Source:	Stakeholder manual identification

How It Is Measured:	Quality of data as presented within extracts as indicated by the number of DUNS numbers with data defects.
IBM's Approach for Achieving:	Each month as the monthly extract files are generated, a quality check is conducted on the outputs against the criteria identified in the AOCS Data Quality plan
Data Accessibility:	Data element errors defined in the approved version of the Operational Data Quality Plan.
Restriction:	This will be measured on the monthly extract files. The daily files use the same data subsets and therefore are affected in the same manner as the monthly files.
IBM Owner:	Extracts & Interfaces Lead

Example Pass Calculation:

Number of records in the file = 600,000

Number of DUNS with defects = 1,000

1,000/600,000 = .17 or 99.83%

Example Data Quality Report (The first row indicates a failed metric):

Date	Total Data Quality Issues	# of DUNS in File	Percent of Issues per DUNS	%
1/1/2015	1,200	500,000	0.24%	99.76%
2/1/2015	1,100	550,000	0.20%	99.80%
3/1/2015	1,000	600,000	0.17%	99.83%
4/1/2015	900	650,000	0.14%	99.86%
5/1/2015	800	700,000	0.11%	99.89%

Example of Data Quality threshold from the Operational Data Quality Plan:

#	Data Element	Validation Description	Showstopper	H/M/L	Threshold %
1	DUNS	Data Is Present - Make sure there are no blank values	Y	H	0.00%
2	DUNS	Length - Make sure all are 9 Characters	Y	H	0.00%
3	DUNS-PLUS4	Length - Make sure all are 4 Characters	Y	H	0.00%

1.1.21 Measure #25: Data Quality - Extract Provision & Reporting Timeliness

Performance Requirement:	Extract Provision Timeliness
Acceptable Quality Level (AQL):	**95% of Daily and Monthly extracts are posed on time within the month.**
Data Source:	Stakeholder manual identification
FPDS Requirements:	Provide capability to return online standard reports within 10 seconds exclusive of network transit time. For all reports, standard and ad hoc, that are less than 10,000 lines and there are no time-outs. For all reports, standard and ad hoc, over than 10,000 lines the time-out rate is not more than 5%.
How It Is Measured:	Total number of failed events across a month that extracts are late relative to the agreed calendar.
IBM's Approach for Achieving:	IBM maintains a master Interface spreadsheet that lists out those interfaces which generate extracts. Each extract interface specification outlines the time in which the file needs to be posted to SAM. If a file is not posted on time, the monitoring team will report this as a miss and research the reason for the late delivery. The team will continue to implement process improvements to address the root causes
Data Accessibility:	Agencies responsible for password access to secure folders.
Restriction:	Only Extracts listed at the time of approval of this document will be considered for this metric
IBM Owner:	Extracts & Interfaces Lead

Example Pass Calculation: 10 files not posted on time = 396-10=386

386/396= 97%

Example Fail Calculation: 25 files not posted on time =396-25=371

371/396=94%

The list of Daily and Monthly Extracts:

#	Extract Name	Daily Tu-Sa	Monthly	Monthly First Sunday	Monthly 15th	Monthly Last Sunday	Once per FY
1	Legacy CCR FOUO 4082	X	X	X			
2	Legacy CCR FOUO 40822	X	X	X			
3	Legacy CCR MPIN	X	X	X			
4	Legacy CCR Proprietary 4082	X	X	X			
5	Legacy CCR Proprietary 40822	X	X	X			
6	Legacy CCR Sensitive 4082	X	X	X			
7	Legacy CCR Sensitive 40822	X	X	X			
8	Legacy CCR Complete 4082	X	X	X			
9	Legacy CCR Complete 40822	X	X	X			
10	Legacy CCR GSA Complete		X			X	
11	Legacy CCR FOIA		X		X		
12	Legacy FedReg Extract	X					
13	SAM Public (Currently NOT being posted due to D&B/GSA discussions)	X	X	X			
14	SAM FOUO	X	X	X			
15	SAM Sensitive	X	X	X			
16	SAM System-Only	X	X	X			
17	SAM MPIN	X	X	X			
18	SAM FSRS	X	X	X			
19	SAM Reps and Certs (NOT being posted until GSA testing is complete)		X	X			
20	SAM Exclusion Public Extract (Full volume daily file)	X					
21	SAM IRS Exclusion Extract (Full volume daily file)	X					
22	Bio-Preferred Fiscal Year Report (Posted once per FY)						X

1.1.22 Measure #26: Data Quality - Extract Provision Consistency

Performance Requirement:	Extract Provision Consistency
Acceptable Quality Level (AQL):	**Less than 12 Extracts Missed per Year**
Data Source:	Stakeholder manual identification and interface monitoring
How It Is Measured:	Number of times on which the **monthly** extracts are not delivered timely due to technical or data quality issues. Any extract not posted within 4 hours of the specification will be considered a miss.
IBM's Approach for Achieving:	Monthly files are generated from the ETL servers and graphs are run throughout the night to produce the extract of the most current data in SAM. The interfaces that run the graphs are monitored for execution throughout the night. Any failure in the graph creation of the extract can cause a delay in posting of the extract in a timely manner. Additionally, GSA will conduct acceptance testing and provide disposition of extract posting. Any failure to post or delay in posting, the IBM team will notify a GSA POC for communication to stakeholders.
Data Accessibility:	Interface tracking spreadsheet is maintained by the IBM data and interface team. Any breach to SLAs will be reported on the monitoring spreadsheet.
Restrictions:	Monthly Extracts listed at the time of approval of this document will be considered for this metric
IBM Owner:	Extracts & Interfaces Lead

There are 18 monthly files that are currently part of the SAM extracts:

Extract Name	Monthly	Monthly First Sunday	Monthly 15th	Monthly Last Sunday	Once per FY
Legacy CCR FOUO 4082	X	X			
Legacy CCR FOUO 40822	X	X			
Legacy CCR MPIN	X	X			
Legacy CCR Proprietary 4082	X	X			
Legacy CCR Proprietary 40822	X	X			
Legacy CCR Sensitive 4082	X	X			
Legacy CCR Sensitive 40822	X	X			
Legacy CCR Complete 4082	X	X			
Legacy CCR Complete 40822	X	X			
Legacy CCR GSA Complete	X			X	
Legacy CCR FOIA	X		X		
SAM Public (Currently NOT being posted due to D&B/GSA discussions)	X	X			
SAM FOUO	X	X			
SAM Sensitive	X	X			
SAM System-Only	X	X			
SAM MPIN	X	X			
SAM FSRS	X	X			
SAM Reps and Certs (NOT being posted until GSA testing is complete)	X	X			

1.1.23 Measure #27: Program Management - Deliverable Timeliness

Performance Requirement:	Deliverable Timeliness
Acceptable Quality Level (AQL):	**100.00%**
Data Source:	Stakeholder manual identification
How It Is Measured:	Percentage of deliverables and scheduled items available and accepted on schedule.
IBM's Approach for Achieving:	Program deliverables are listed in the deliverables tracking spreadsheet within the Connections website. The IBM team will follow the policies documented within the QCP to address the accuracy and timeliness of deliverables.
Data Accessibility:	GSA to acknowledge receipt of deliverables on the same day. Deliverables are posted on the Connections website that can be accessed by anyone with an approved account.
Restriction:	None
IBM Owner:	PMO Lead

Any missed deliverable in a month will result in a failure of this metric.

1.1.24 Measure #28: Program Management - Risk Management

Performance Requirement:	Risk Management
Acceptable Quality Level (AQL):	**There are no unmitigated or unaccepted High-level risks to the program**
Data Source:	Stakeholder manual identification
How It Is Measured:	Risks identified in the monthly risk log delivered within the Monthly Steward Report will have a mitigation strategy for all items marked as high.
IBM's Approach for Achieving:	Items are added to the risk log as issues / risks arise. The team conducts monthly risk reviews and updates the risk log. Only current known risks that are documented for consideration of mitigation will be counted within this metric.
Data Accessibility:	GSA and IBM to meet at least quarterly to review current risk log which is also delivered in the monthly Steward Report.
Restriction:	None
IBM Owner:	PMO Lead

1.1.25 Measure #29: Release Quality - Defects Per Release

Performance Requirement:	Defects Per Release
Acceptable Quality Level (AQL):	**Less than 5 Serious defects per 100 RTC Items**
Data Source:	Rational Team Concert
How It Is Measured:	Less than 5 Serious software defects as a result of the production deployment. (1 Serious defect for every 20 RTC delivered items)
IBM's Approach for Achieving:	Items that can be traced to a requirement such as Defect, Enhancement and O&M make up the RTC count. 5 Serious defects identified within 30 days after the release.
Data Accessibility:	All defects are maintained in the Rational Team Concert (RTC) tool. Items are marked for delivery in the due date field and may be tracked to completion. Once an item is successfully implemented in production, it is closed.
Restrictions	None
IBM Owner:	Program Manager

Pass Example: A release contained 120 items. 5 serious defects were opened in the first 30 days after the release.

Fail Example: A release contained 120 items. 6 serious defects were opened in the first 30 days

1.1.26 Measure #30: Release Quality - Production Scope

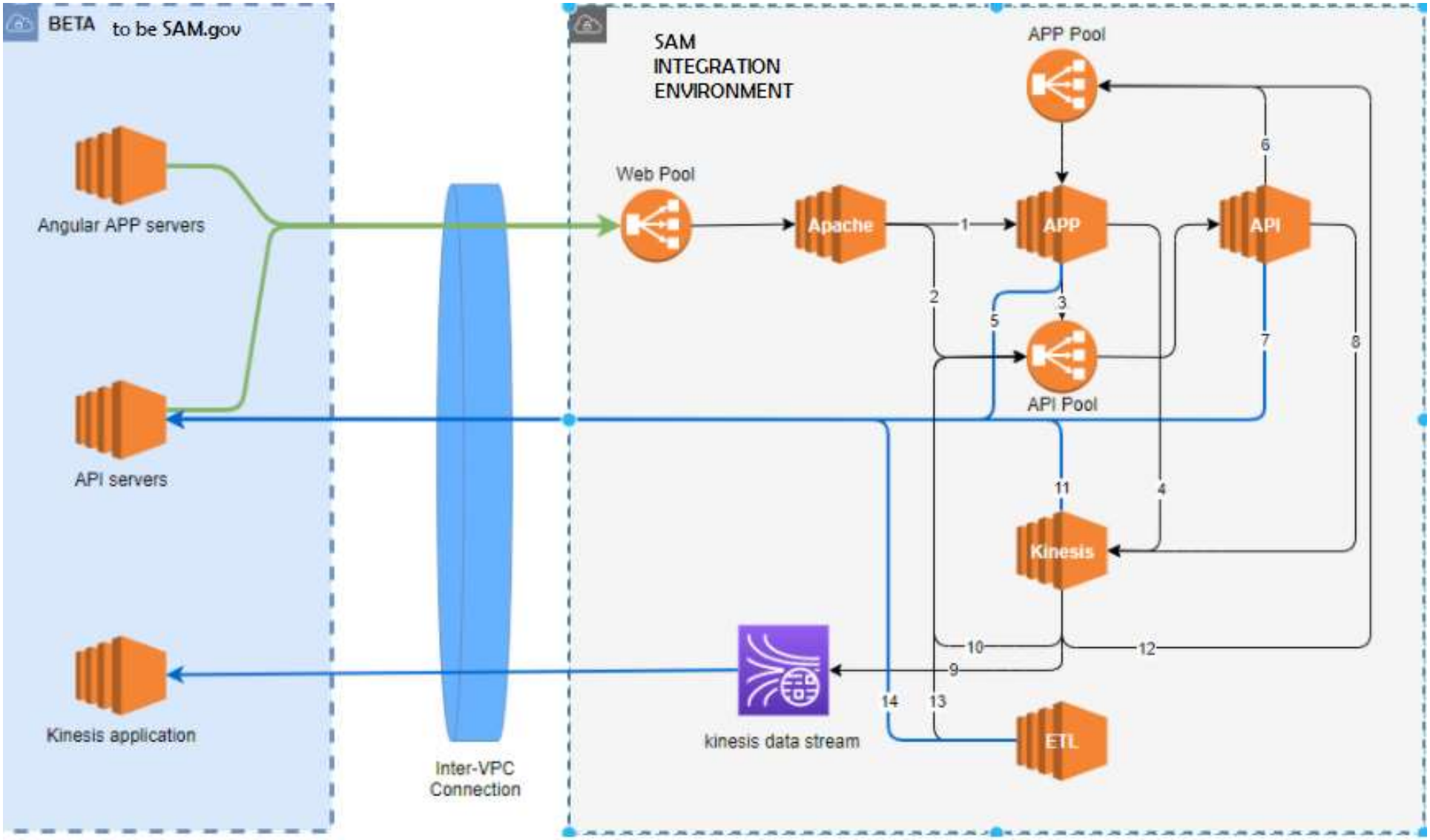
Performance Requirement:	Production Releases contain the agreed / scheduled scope
Acceptable Quality Level (AQL):	**95% of requirements scheduled have been delivered**
Data Source:	Stakeholder manual identification
How It Is Measured:	Missed functionality as indicated by the approved requirements specifications not implemented.
IBM's Approach for Achieving:	Approved system specifications added to a release scope prior to end of requirements phase. Requirements that are agreed upon will be developed and delivered to testing for validation. Per the System Engineering plan, approved requirements are designed and developed according to specification and reviewed accordingly. System testing including GAT and UAT will validate proper and complete incorporation of the requirements.
Data Accessibility:	Requirements are maintained in the Rational Team Concert (RTC) Requirements Composer tool. These requirements are linked to individual RTC numbers. Once a requirement is approved for a release, it is tracked to completion within the RTC item.
Restriction:	This is effective for quarterly releases only.
IBM Owner:	Program Manager

During the months when no release is added to production or no new requirements are implemented, the previous score will carry over to the current month.

1.1.27 Measure #31: Release Quality - Production Releases on Schedule

Performance Requirement:	Production Releases are delivered on schedule
Acceptable Quality Level (AQL):	**Delivered on schedule**
Data Source:	Stakeholder manual identification
How It Is Measured:	Release date is met as agreed upon by GSA and IBM.
IBM's Approach for Achieving:	GSA and IBM will work together to develop and work towards a quarterly release scope and plan. Once the release date is set and the items for delivery are agreed upon, the teams will have regularly scheduled meetings to discuss progress of the release. The teams will target to have the release date agreed upon at least 90 days prior to the release. Any change to a release date, due to a dependency on GSA, will not count against IBM as a missed schedule delivery.
Data Accessibility:	Release items are maintained in the Rational Team Concert (RTC) tool. Items are marked for delivery in the due date field and may be tracked to completion. Once an item is successfully implemented in production, it is closed.
Restriction:	This is effective for quarterly releases only. This measure will not be counted due to reasons beyond failure of a passing test disposition or incomplete delivery of agreed upon scope.
IBM Owner:	Program Manager

During the months when no release is added to production, the previous score will carry over to the current month.


BETA
to be SAM.gov
SAM
INTEGRATION
ENVIRONMENT
APP Pool
Web Pool
Angular APP servers
Apache
APP
API
API Pool
API servers
Kinesis
Kinesis application
kinesis data stream
ETL
Inter-VPC
Connection
1
2
3
4
5
6
7
8
9
10
11
12
13
14

ID16210006 PWS Att M

IT Policy Requirements Guide

CIO-12-2018

Office of the Chief Information Officer

Table of Contents

1.0 Introduction ……2

1.1 Scope……2

1.2 Purpose……2

2.0 Contracting Life Cycle……2

2.1 Contracting Life Cycle Graphic……3

2.2 Contracting Phase Activities for COR ……3

3.0 Non-Security & Non-Privacy IT Policies……..4-10

4.0 Internal GSA Resources……..10

5.0 External GSA Resources……..10

1.0 Introduction

The U.S. General Services Administration (GSA) has implemented various federal policies for providing direction, and constituting uniform rules and accountability for governing the acquisition and usage of information technology (IT). This document identifies GSA information technology policies other than security and privacy policies and provides guidance to help GSA employees and applicable contractors fulfill them. Having one comprehensive Guide identify policies will assist the GSA workforce's understanding and implementation of policies. As policies are updated this guide will be updated.

1.1 Scope

This IT Policy Requirements Guide covers IT policies other than security and privacy because GSA CIO 09-48 IT Security Procedural Guide covers all security and privacy IT policies. As a result of the close association of IT systems and IT governance processes in some cases one may be able to detect a relationship between the listed policies and what could be referred to as explicit IT security policy. However the primary scope of this guide is on IT policies outside of security and privacy.

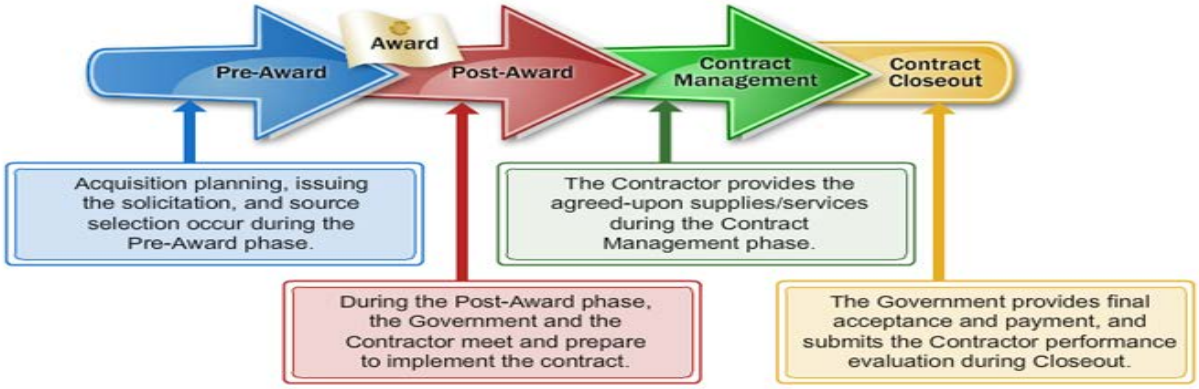
1.2 Purpose

The purpose of this Guide is to identify applicable non-security and non-privacy IT policies and provide guidance on implementing these policies. The applicability of IT policy to the contracting phases is used to help highlight critical requirements that the acquisition professional must adhere to. There is emphasis given to the Contracting Officer's Representative (COR) due to his or her unique viewpoint in contract management. In addition, this guide identifies what IT policies a contractor must comply with when this guide has been incorporated into their contract. Section 3 specifies which policies are applicable for a contractor based on the products or services being acquired in the contract.

2.0 Contracting Life Cycle

Every acquisition, and its resulting contract, follows a four phase contracting life cycle. The Contracting Officer's Representative (COR) has significant supporting involvement in each phase.

2.1 Contracting Life Cycle Graphic



Source: Graphic is from DAU University's "FCR 100 Contracting Officer Level 1" 2017 online course.

2.2 Contracting Phase Activities for COR

The following list *some* primary activities performed by the COR during the four contracting phases. The Contracting Officer (CO) has the actual authority to act as an agent for the Government and can delegate responsibilities to the COR. The COR oversees technical aspects of the contracts and performs most of the administrative functions required to ensure acceptable service or product. The CO relies on the COR to be his or her "eyes and ears" to help manage the contract.

(1.) Pre-Award • **Conducting Market Research** • **Defining Requirements** • **Support determining the Acquisition Strategy**	**(2.) Post-Award** • **Supporting creation of the Management Plan & contract kick off meeting** • **Creating of a COR Checklist** • **Maintaining a COR Contract File** • **Liaison/Communicating Concerns and Information** • **Ongoing Market Research to stay current with market conditions, technology advances, and industry trends**
(3.) Contract Administration • **Monitoring Performance/Providing technical direction** • **Managing Contract Changes** • **Inspecting and accepting supplies and/or services** • **Reviewing invoices and processing payments**	**(4.) Closeout** • **Supporting contract closeout procedures**** • **Providing contract evaluation in CPARS** • **Completing contract file** ****NOTE: Final invoice & payment, deobligation of funds, etc..**

3.0 Non-Security & Non-Privacy IT Policies

The chart below identifies which policies apply to GSA employees and the contractors. To determine if a policy applies, first check if there is a green check mark in the column with the heading, "*Who has primary responsibilities?*". If there is a checkmark for an employee or contractor, then identify if the policy must be followed based on the scope of the policy as detailed in the column with the heading, *"When does it apply?"*.

Policy	Who has primary responsibilities?		When does it apply?	Which contracting phase does it apply?
	GSA	Contractor		
CIO IL-16-03 GSA Open Source Software (OSS) Policy This Instructional Letter (IL) establishes GSA policies for OAuth 2.0 integration of GSA.gov accounts with third party services including but not limited to Websites, Software as a Service (SaaS), mobile applications, and Google Apps Scripts.	✅ See 5. Responsibilities a. b. c. d. e. f.	❌	When there is a development requirement for new or existing software, component or functionality	- Pre-Award - Contract Administration
CIO 2101.1 GSA Enterprise Information Technology Management (ITM) Policy This policy reinforces several existing IT management processes; integrates GSA IT in all implementation, procurement, workforce, and IT-related budget matters; and strengthens our partnerships across GSA.	✅ See 3. Applicability c. See 4. Responsibilities a. (1), (2), (3)(a)(b) b. (1),(2),(3),(4)	❌	When engaging with business lines, reviewing business plans, and/or conducting reviews (acquisition, budget, or post-implementation)	- Pre-Award - Contract Administration - Closeout
CIO 2102.1 Information Technology (IT) Integration Policy Establishes GSA's privacy policies and procedures, provides guidance and direction on implementing program requirements, defines privacy related contracting requirements, and assigns responsibilities to ensure compliance with the Privacy Act of 1974.	✅ See 5. Scope and applicability a. b. c.	❌	When acquiring any: 1.) new internal GSA IT solution 2.) major enhancement to existing project that has criteria of either: a.) over $150k b.) cloud acquisition c.) BPA d.) RFI & market research e.) or high-priority IT acquisitions	-Pre-Award -Post-Award -Contract Administration -Closeout

3.0 continued

Policy	Who has primary responsibilities?		When does it apply?	Which contracting phase does it apply?
	GSA	Contractor		
CIO 2104.1A CIO CHGE 1 GSA Information Technology IT General Rules of Behavior This Order sets forth the General Services Administration's (GSA's) policy on IT General Rules of Behavior.	✅ See 4. Applicability	✅ See 4. Applicability	When accessing GSA IT resources to conduct business on behalf of, or with, GSA or GSA supported Government organizations, and to all GSA IT resources which process or store GSA data, whether leased or owned.	- Contract Administration
CIO 2105.1C CHGE 1 GSA Section 508: Managing Information and Communications Technology (ICT) for Individuals with Disabilities This Order provides direction and guidance for ensuring information and communications technology allow persons with disabilities to have access to information and data that is comparable to the access of individuals without disabilities.	✅ See 5. Responsibilities a. Heads of Services and Staff Offices (HSSO) (1), (2), (3) (4)(a)(b)(c)(d) (e)(f)(g)	❌	When developing, procuring, maintaining, or using information and communications technology	- Pre-Award - Contract Administration
CIO 2105.2 P GSA Section 508 Procedures Handbook This Order issues and transmits Handbook (HB), GSA Section 508 Procedures. Section 508 prohibits Federal agencies from procuring, developing, maintaining, or using EIT that is not accessible to people with disabilities, subject to an undue burden defense. If it is properly determined by the agency that meeting the Section 508 standards would impose an undue burden, GSA must provide individuals with disabilities with information and data involved by an alternative means of access that allows the individual to use the information and data.	✅ See 3. Applicability	✅ See 3. Applicability	When developing, procuring, maintaining, or using electronic and information technology	- Pre-Award - Contract Administration

3.0 continued

Policy	Who has primary responsibilities?		When does it apply?	Which contracting phase does it apply?
	GSA	Contractor		
CIO 2108.1 Software License Management GSA is consolidating software license management and establishing a software license management program. This Order establishes software license management roles, responsibilities, and procedures.	✅ See 3. Scope and applicability a. b. c. d. See 4. Responsibilities a. (1)(2) (3) (4)(5)(6)(7) b.(1)(2)	✅ See 3. Scope and applicability a. b. c. d. See 4. Responsibilities a. (1)(2) (3) (4)(5)(6)(7) b.(1)(2)	When there is a requirement to acquire software	- Pre-Award - Contract Administration - Closeout
CIO 2110.4 GSA Enterprise Architecture Policy This Order establishes agency-wide policy, principles, roles and responsibilities for the establishment and implementation of the General Services Administration (GSA) Enterprise Architecture (EA).	✅ See 4. Applicability a. b. c. See 5. Roles and responsibilities a. b. c. d. e. f.	❌	When building EA or when there is a requirement to purchase new software	- Pre-Award - Contract Administration
CIO 2130.2 Enterprise IT Governance This policy provides direction and guidance on GSA Enterprise IT Governance (EIG). EIG is a structured decision-making framework for identifying, selecting, prioritizing, and tracking all IT investments and initiatives for the GSA enterprise. EIG integrates new business-driven approaches to investment evaluation and selection with existing agency activities and programs (e.g., Spend Tracker and legacy PBS IT governance).	✅ See 3. Applicability	❌	When EIG approval is needed	- Pre-Award

3.0 continued

Policy	Who has primary responsibilities?		When does it apply?	Which contracting phase does it apply?
	GSA	Contractor		
CIO 2135.2B GSA Information Technology (IT) Capital Planning and Investment Control This Order establishes agency-wide policies, roles and responsibilities for GSA's IT Capital Planning and Investment Control process (CPIC). CPIC is an integrated management process for the continuous selection, control, and evaluation of IT investments over their life cycles and is focused on achieving desired outcomes in support of GSA's missions, goals, and objectives.	✅ See 4. Applicability See 8. CPIC responsibilities a.b.c.d. e.(1)(2)(3)(4)(5)(6)(7) f.Program/ Project Manager 1)(2)(3)(4)(5)(6)(7)(8)	❌	When evaluating IT investments over their life cycles	- Pre-Award - Post-Award - Contract Administration - Closeout
CIO 2140.4 Information Technology (IT) Solutions Life Cycle (SLC) Policy This Order sets forth policy for planning and managing IT solutions developed for or operated by GSA. This policy has been developed to ensure the Solutions Life Cycle (SLC) discipline used is consistent with SLC guiding principles, acquisition planning requirements, and capital planning and investment control requirements. The term SLC replaces the term Software Development Life Cycle (SDLC) which was used in the past.	✅ See 5. Applicability and scope a. b. c. d. e. f.	❌	This policy applies to acquisition development, maintenance, enhancement, operation, and disposal of IT systems and solutions of any size, complexity, or significance that are part of the agency's' IT portfolio as defined in CIO 2135.2B GSA Information Technology (IT) Capital Planning and Investment Control	- Pre-Award - Post-Award - Contract Administration - Closeout
CIO 2142.1 P GSA Information and Data Quality Handbook This order issues and transmits Handbook (HB), General Services Administration (GSA) Information and Data Quality Guidelines.	✅ See 2. Applicability	❌	When acquisition will result in a new asset or data update to an existing asset	- Contract Administration

3.0 continued

Policy	Who has primary responsibilities?		When does it apply?	Which contracting phase does it apply?
	GSA	Contractor		
CIO 2141.2 General Services Administration (GSA) Web Domain Names This GSA Order sets forth GSA's internal guidance to assist organizations desiring to obtain unique website identifications. This Order provides domain name guidance for GSA staff organizations, including service, geographical, and operational areas.	✅ See 4. Coverage	❌	Applicable if an acquisition involves the need for a new domain name	- Pre-Award
CIO 2160.1F CHGE 2 GSA information Technology (IT) Standards Profile To ensure acquisition and use of standard information technologies and proper maintenance of the IT Standards Profile. The IT Standards Profile is the official GSA repository of all approved software applications. It is managed by GSA IT and can be found at ea.gsa.gov.	✅ See 2. Applicability a. b. c. d. e. See 5. Responsibilities a. b. c. d. e. f. g. See 6. Compliance a. b. (1)(2)(3)(4) c. d. (1)(2)	❌	When acquiring or using information technologies in the conduct of GSA business	- Pre-Award
CIO 2160.2B CHGE 1 GSA Electronic Messaging and Related Services This Order updates GSA's directive on electronic messaging due to the move from a server-based messaging system to cloud-based e-mail and collaboration tools and additional federal requirements for managing electronic mail records. This directive addresses security, appropriate use, and recordkeeping of the GSA Enterprise Messaging Services (GEMS) in a cloud-based environment.	✅ See 3. Applicability	✅ See 3. Applicability	All authorized users who are granted access to GEMS and to all communications sent or received via GEMS	- Pre-Award

3.0 continued

Policy	Who has primary responsibilities?		When does it apply?	Which contracting phase does it apply?
	GSA	Contractor		
CIO 2160.4A Provisioning of Information Technology (IT) Devices This Order provides direction and guidance on the deployment of computer workstations, mobile devices, and printers for agency and designated contractor personnel.	✅ See 4. Applicability a. See 5. Roles and responsibilities a.(1)(2) b.(1)(2)	✅ See 4. Applicability a.	When writing SOW. Compliance with policy should be addressed in Statements of Work (SOWs) for contractors.	- Pre-Award - Contract Administration - Closeout
CIO 2164.1 Internal Clearance Process for GSA Data Assets This Order provides the internal clearance process that the General Services Administration (GSA) must follow before releasing GSA data assets. GSA IT's Office of Enterprise Information & Data Management (IDM) established this process in collaboration with the Office of General Counsel (OGC), the Freedom of Information Act (FOIA) Division, the Privacy Officer in GSA IT, and the Executive Secretariat Division. The established clearance process ensures that the privacy, security, and confidentiality of GSA's critical data assets are protected from unauthorized access, release, and dissemination.	✅ See 4. Applicability	❌	Before releasing GSA data assets	- Contract Administration
CIO P 2165.2 GSA Telecommunications Policy This policy establishes the policy for General Services Administration (GSA) authorized users for utilization of GSA-provided telecommunications equipment, systems and services (hereafter, GSA telecommunications).	✅ See 2. Applicability	✅ See 2. Applicability	When creating any agreement (e.g. MOU) that results in that process or handle of any GSA-owned information, data, or IT system equipment	- Pre-Award

3.0 continued

Policy	Who has primary responsibilities?		When does it apply?	Which contracting phase does it apply?
	GSA	Contractor		
CIO 7000.3 Information Technology Standards for Internal GSA Workplaces This Order transmits the information technology (IT) standards for all new workplace projects, including new construction or alterations to existing space, for all GSA offices.	✅ See 5. Scope and applicability	✅ See 5. Scope and applicability	When there is a requirement to purchase IT equipment for an internal GSA workplace	- Pre-Award
CIO 9297.1 GSA Data Release Policy This Order provides GSA's policy on releasing information relating to GSA employees, contractors, and others on whom GSA maintains information described in this document.	✅ See 4. Applicability	❌	When releasing information to the public as through FOIA or other official requests and who collect, maintain, use, manage, or come in contact with personally identifiable or sensitive information owned by GSA	- Contract Administration - Contract Closeout

4.0 Internal GSA Resources

- GSA Acquisition Policy
  https://insite.gsa.gov/portal/content/510990

- GSA IT Policy Management
  https://insite.gsa.gov/portal/content/626370

- GSA IT Vendor Management
  https://insite.gsa.gov/portal/category/535534

5.0 External GSA Resources

- GSA Directives Library
  https://www.gsa.gov/directives-library

IT Security Procedural Guide:

Security and Privacy Requirements for IT Acquisition Efforts

CIO-IT Security-09-48

Revision 4

January 25, 2018

Office of the Chief Information Security Officer

IMPORTANT!

This guide defines security and privacy requirements for GSA IT acquisition contracts involving externally hosted contractor information systems that do not connect to the GSA network; information systems hosted in GSA facilities that directly connect to the GSA network; cloud information systems; or mobile applications. The security and privacy requirements are appropriately formatted to allow the respective security and privacy contract requirements to be placed in-line within a statement of work for each system type. Alternatively, this entire document can be incorporated into the statement of work or contract.

NOTE: Throughout this guide there are highlighted SELECT statements. The requirements office, in coordination with the contracting officer, will complete the selections prior to their incorporation into a contract or statement of work.

VERSION HISTORY/CHANGE RECORD

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
Revision 1 – November 6, 2009				
1	Bo Berlas	Minor Changes to GSA 800-53 R3 Control Tailoring workbook in Appendix A	GSA 800-53 Control Tailoring Workbook Update	17
Revision 2 – November 7, 2014				
1	John Sitcharing/ Blanche Heard	Minor changes to verbiage regarding Penetration Testing	Update Penetration Testing verbiage	9
2	John Sitcharing/ Blanche Heard	CISO mandated change in Penetration Testing requirement/ naming conventions based on consolidation efforts	CISO Mandate	Entire document
Revision 3 – February 2, 2017				
1	Bo Berlas	Added Essential Security controls to Section 2	Security Controls Update	9
2	Bo Berlas	Added sections 3-5	Updated to Provide Requirements for Internal Systems, Cloud Systems, and Mobile Applications	22-55
Revision 4 – January 25, 2018				
1	Bryon Feliksa/ John Klemens	Incorporated security references from MV 16-01 and additional references. Added a section on LiSaaS, Privacy controls, and updated Privacy and other sections to align with GSA policy and procedures.	Incorporate MV 16-01 and consolidate GSA Cybersecurity and Privacy Guidance.	Throughout

APPROVAL

IT Security Procedural Guide 09-48, *"Security and Privacy Requirements for IT Acquisition Efforts,"* Revision 4, is hereby approved for distribution.

1/26/2018

X Kurt Garbars

Kurt Garbars
CISO
Signed by: KURT GARBARS

This guide will be available on the OCIO Webpage and GSA.gov when revised.

Table of Contents

1 Introduction 1

1.1 Scope 1
1.2 Purpose 2

2 External Information Systems – IT Security and Privacy Requirements 3

2.1 Required Policies and Regulations for GSA Contracts 3
2.2 GSA Security Compliance Requirements 4
2.3 Essential Security Controls 5
2.4 Assessment and Authorization (A&A) Activities 9
2.5 Reporting and Continuous Monitoring 11
2.6 GSA Privacy Requirements 15
2.7 Additional Stipulations 17

3 Internal Information Systems - IT Security and Privacy Requirements 19

3.1 Required Policies and Regulations for GSA Contracts 19
3.2 GSA Security Compliance Requirements 20
3.3 Essential Security Controls 21
3.4 Assessment and Authorization (A&A) Activities 26
3.5 Reporting and Continuous Monitoring 28
3.6 GSA Privacy Requirements 32
3.7 Additional Stipulations 33

4 Low Impact Software as a Service (LiSaaS) – IT Security and Privacy Requirements 36

4.1 Assessment of the System 36
4.2 Authorization of the System 37
4.3 Reporting and Continuous Monitoring 37
4.4 Protection of Information 37
4.5 Data Ownership and Unrestricted Rights to Data 37
4.6 Personally Identifiable Information 38
4.7 Data Availability 38
4.8 Data Release 38
4.9 Confidentiality and Nondisclosure 39
4.10 Section 508 Compliancy 39
4.11 Additional Stipulations 39
4.12 Terms of Service 41
4.13 References 41

5 Cloud Information Systems – IT Security and Privacy Requirements 42

5.1 Assessment and Authorization 42
5.2 Assessment of the System 42
5.3 Authorization of the System 44
5.4 Reporting and Continuous Monitoring 46
5.5 Personnel Security Requirements 47
5.6 Sensitive Information Storage 47
5.7 Protection of Information 48
5.7.1 Unrestricted Rights to Data 48

5.7.2 Personally Identifiable Information 48
5.7.3 Data Availability 48
5.7.4 Data Release 48
5.8 Data Ownership 49
5.9 Confidentiality and Nondisclosure 49
5.10 GSA Non-Disclosure Agreement 49
5.11 Additional Stipulations 50
5.12 References 52

6 Mobile Application - IT Security and Privacy Requirements 53

6.1 General Mobile Application Guidelines 53
6.2 Mobile Device Security 53
6.3 Application Sources 54
6.4 Terms of Service (ToS) 55
6.5 GSA Privacy Requirements 55
6.6 GSA App Development, Assessment, Authorization and Deployment 56
6.7 Intellectual Property 58
6.8 Confidentiality and Nondisclosure 58
6.9 GSA Non-Disclosure Agreement 59
6.10 Personnel Security Requirements 59
6.11 Additional Stipulations 60

Appendix A: GSA Tailoring of NIST 800-53 Controls 63

1 Introduction

The U.S. General Services Administration (GSA) must provide information security for the information systems that support the operations and assets of the agency, including those provided or managed by GSA, another agency, contractor, or other source. The Federal Information Security Modernization Act of 2014 (FISMA of 2014) describes Federal agency security and privacy responsibilities as including "information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency." This includes services which are either fully or partially provided; including other agency hosted, outsourced, and cloud computing solutions. Agency information security programs apply to all organizations (sources) which possess or use Federal information – or which operate, use, or have access to Federal information systems (whether automated or manual) – on behalf of a Federal agency, information systems used or operated by an agency or other organization on behalf of an agency.

Office of Management and Budget (OMB) Memorandum M-14-04 asserts that agencies are responsible for ensuring information technology acquisitions comply with the information technology security requirements in FISMA of 2014, OMB's implementing policies including OMB Circular A-130 and guidance and standards from the National Institute of Standards and Technology (NIST).

1.1 Scope

This guide provides security and privacy requirements for the GSA information system types outlined below:

- **External Information Systems.** External information systems reside in contractor facilities and typically do not connect to the GSA network. External information systems may be government owned and contractor operated or contractor owned and operated on behalf of GSA or the Federal Government (when GSA is the managing agency).
- **Internal Information Systems.** Internal information systems reside on premise in GSA facilities AND directly connect to the GSA network. Internal systems are operated on behalf of GSA or the Federal Government (when GSA is the managing agency).
- **Low Impact Software as a Service (LiSaaS) Systems.** LiSaaS systems must adhere to GSA IT Security Procedural Guide 17-75, "*Security Reviews for Low Impact Software as a Service (SaaS) Solutions*." LiSaaS systems are cloud applications that are implemented for a limited duration, considered low impact and would cause limited harm to GSA, and cost less than $100,000 to deploy.
- **Cloud Information Systems**. Includes Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or SaaS. Requires FedRAMP.
- **Mobile Application.** A mobile application, most commonly referred to as an app, is a type of application software designed to run on a mobile device, such as a smartphone or tablet computer.

1.2 Purpose

The purpose of this document is to define and establish consistent security and privacy requirements for GSA IT acquisition contracts involving externally hosted information systems that do not connect to the GSA network; information systems hosted in GSA facilities that directly connect to the GSA network; LiSaaS systems, cloud information systems; or mobile applications. The security and privacy requirements are appropriately formatted to allow the respective security and privacy contract language to be placed in-line within a statement of work for each system type. The security and privacy requirements identified in this guide will ensure compliance with the appropriate provisions of FISMA of 2014, OMB Circular A-130, and NIST Special Publication (SP) 800-53, Revision 4.

2 External Information Systems – IT Security and Privacy Requirements

2.1 Required Policies and Regulations for GSA Contracts

Federal Laws and Regulations:

The contractor shall comply with all applicable Federal Laws and Regulations.

- 40 U.S.C. 11331, "*Responsibilities for Federal Information Systems Standards*"
- FISMA of 2014, "*The Federal Information Security Modernization Act of 2014*"
- HSPD 12, "*Homeland Security Presidential Directive 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*"
- OMB Circular No. A-130, "*Managing Information as a Strategic Resource*"
- OMB M-08-23, "*Securing the Federal Government's Domain Name System Infrastructure (Submission of Draft Agency Plans Due by September 5, 2008)*"
- OMB M 14-03, "*Enhancing the Security of Federal Information and Information Systems*"
- OMB M-10-23, "*Guidance for Agency Use of Third-Party Websites and Applications*"
- OMB M-15-13, "*Policy to Require Secure Connections across Federal Websites and Web Services*"
- OMB M-17-12, "*Preparing for and Responding to a Breach of Personally Identifiable Information*"
- Privacy Act of 1974, "*5 USC, § 552a*"
- OMB Memoranda, location of current fiscal year guidance on Federal Information Security and Privacy Management Requirements, including FISMA reporting

Federal Standards and Guidance:

The contractor shall comply with all applicable Federal Information Processing Standards (FIPS). NIST Special Publications (800 Series) are guidance, unless required by a FIPS publication, in which case usage is mandatory.

- FIPS PUB 199, "*Standards for Security Categorization of Federal Information and Information Systems*"
- FIPS PUB 200, "*Minimum Security Requirements for Federal Information and Information Systems*"
- FIPS PUB 140-2, "*Security Requirements for Cryptographic Modules*"
- NIST SP 800-18, Revision 1, "*Guide for Developing Security Plans for Federal Information Systems*"
- NIST SP 800-30, Revision 1, "*Guide for Conducting Risk Assessments*"
- NIST SP 800-34, Revision 1, "*Contingency Planning Guide for Federal Information Systems*"
- NIST SP 800-37, Revision 1, "*Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Lifecycle Approach*"
- NIST SP 800-47, "*Security Guide for Interconnecting Information Technology Systems*"
- NIST SP 800-53, Revision 4, "*Security and Privacy Controls for Federal Information Systems and Organizations*"

- NIST SP 800-53A, Revision 4, *"Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*"
- NIST SP 800-63-3, "*Digital Identity Guidelines*"
- NIST SP 800-122, "*Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*"
- NIST SP 800-137, "*Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*"

GSA Policies:

The contractor shall comply with the following GSA Directives/Policies.

- GSA Order CIO 1878.1, "*GSA Privacy Act Program*"
- GSA Order CIO 1878.2, "*Conducting Privacy Impact Assessments (PIAs) in GSA*"
- GSA Order CIO 2100.1, "*GSA Information Technology (IT) Security Policy*"
- GSA Order CIO 9297.2, "*GSA Information Breach Notification Policy*"

The GSA policies listed in this paragraph must be followed, if applicable.

- GSA Order CIO 2103.1, "*Controlled Unclassified Information (CUI) Policy*"
- GSA Order CIO 2104.1, "*GSA Information Technology (IT) General Rules of Behavior*"
- GSA Order CIO 2182.2, "*Mandatory Use of Personal Identity Verification (PIV) Credentials*"

GSA Procedural Guides:

GSA IT Procedural Guides are guidance, unless required by a GSA Directive/Policy, in which case usage is mandatory.

Note: GSA's Procedural Guides are updated frequently; to make sure you have the most recent version of publicly available procedural guides, visit GSA.gov. If a non-publicly available guide is needed, contact the contracting officer who will coordinate with the GSA Office of the Chief Information Security Officer to determine if it can be made available.

2.2 GSA Security Compliance Requirements

FIPS PUB 200, *"Minimum Security Requirements for Federal Information and Information Systems*," is a mandatory federal standard that defines the minimum security requirements for federal information and information systems in seventeen security-related areas. Information systems supporting GSA must meet the minimum security and privacy requirements through the use of security controls in accordance with NIST Special Publication 800-53, Revision 4 (hereafter described as NIST 800-53), *"Security and Privacy Controls for Federal Information Systems and Organizations."*

To comply with the Federal standard, GSA must determine the security category of the information and information system in accordance with FIPS PUB 199, *"Standards for Security Categorization of Federal Information and Information Systems,"* and then the contractor shall

apply the appropriately tailored set of Low, Moderate, or High impact baseline security controls in NIST 800-53, as determined by GSA. NIST 800-53 controls requiring organization-defined parameters (i.e., password change frequency) shall be consistent with GSA specifications. The GSA-specified control parameters and supplemental guidance defining more specifically the requirements per FIPS PUB 199 impact level are available in the GSA Control Tailoring Workbook referenced in Appendix A of this document.

The Contractor shall use GSA technical guidelines, NIST guidelines, Center for Internet Security (CIS) guidelines (Level 1), or industry best practice guidelines in hardening their systems.

2.3 Essential Security Controls

All NIST 800-53 controls must be implemented as per the applicable FIPS PUB 199 Low, Moderate, or High baseline. The following table identifies essential security controls from the respective baselines to highlight their importance and ensure they are implemented. The Contractor shall make the proposed system and security architecture of the information system available to the Security Engineering Division, in the Office of the Chief Information Security Officer for review and approval before commencement of system build (architecture, infrastructure, and code).

Control ID	Control Title	Baseline	GSA Implementation Guidance
AC-2	Account Management	L, M, H	
AC-17 (3)	Remote Access | Managed Access Control Points	M, H	All remote accesses from internal users/systems to the external information system must be routed through GSA's managed network access control points, subjecting them to security monitoring.
AU-2	Audit Events	L, M, H	Information systems shall implement audit configuration requirements as documented in applicable GSA IT Security Technical Hardening Guides (i.e., hardening and technology implementation guides); for web applications see GSA IT Security Procedural Guide 07-35, Section 2.8.10, What to Log. For technologies where a Technical Guide and Standard does not exist, events from an industry source such as vendor guidance or Center for Internet Security benchmark, recommended by the GSA S/SO or Contractor to be approved and accepted by the GSA AO shall be used.
CM-6	Configuration Settings	L, M, H	Information systems, including vendor owned/operated systems on behalf of GSA, shall configure their systems in agreement with GSA technical guidelines, NIST guidelines, Center for Internet Security guidelines (Level 1), or industry best practice guidelines, as deemed appropriate.

Control ID	Control Title	Baseline	GSA Implementation Guidance
CP-7	Alternative Processing Site	M, H	FIPS PUB 199 Moderate and High impact systems must implement processing across geographically-disparate locations to ensure fault tolerance. Amazon Web Services based architectures must implement a multi-region strategy (multiple availability zones in a single region are not sufficient).
CP-8	Telecom Services	M, H	FIP PUB 199 Moderate and High impact information systems must implement alternate telecom services to support resumption when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.
IA-2 (1)	Identification and Authentication (Organizational Users) | Network Access to Privileged Accounts	L, M, H	All information systems shall implement multi-factor authentication for privileged accounts.
IA-2 (2)	Identification and Authentication (Organizational Users) | Network Access to Non-Privileged Accounts	M, H	FIPS PUB 199 Moderate and High impact information systems must implement multi-factor authentication for non-privileged accounts.
IA-7	Cryptographic Module Authentication	L, M, H	The information system shall implement FIPS PUB 140-2 compliant encryption modules for authentication functions. Reference: https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules
MP-4	Media Storage	M, H	Digital media including magnetic tapes, external/removable hard drives, flash/thumb drives, diskettes, compact disks and digital video disks shall be encrypted using a FIPS PUB 140-2 certified encryption module.
MP-5	Media Transport	M, H	Digital media including magnetic tapes, external/removable hard drives, flash/thumb drives and digital video disks shall be encrypted using a FIPS PUB 140-2 certified encryption module during transport outside of controlled areas.

Control ID	Control Title	Baseline	GSA Implementation Guidance
PL-8	Information Security Architecture	M, H	All information system security architectures must be formally reviewed and approved by the Office of the Chief Information Security Officer, Security Engineering Division during the system develop/design stages of the SDLC and prior to Security Assessment and Authorization.
RA-5	Vulnerability Scanning	L, M, H	All systems must complete weekly operating system (OS) and monthly web application vulnerability scans. The most recent vulnerability scanning results shall be provided to GSA together with the quarterly POA&M submission.
SA-22	Unsupported System Components	GSA Required	All systems must be comprised of software and hardware components that are fully supported in terms of security patching for the anticipated life of the system; software must be on GSA's Enterprise Architecture IT Standards List.
SC-8 / SC-8(1)	Transmission Confidentiality and Integrity / Transmission Confidentiality and Integrity | Cryptographic or Alternate Physical Protection	M, H	Implemented encryption algorithms and cryptographic modules shall be FIPS-approved and FIPS PUB 140-2 validated, respectively. ○ Digital signature encryption algorithms - Reference: https://csrc.nist.gov/Projects/Cryptographic-Algorithm-Validation-Program/Validation/Validation-List/DSA ○ Block cypher encryption algorithms - Reference: https://csrc.nist.gov/Projects/Cryptographic-Algorithm-Validation-Program/Block-Ciphers ○ Secure hashing algorithms – Reference: https://csrc.nist.gov/Projects/Cryptographic-Algorithm-Validation-Program/Secure-Hashing Internet accessible Websites shall implement HTTPS Only and HTTP Strict Transport Security (HSTS), reference OMB Memorandum M-15-13. SSL/TLS implementations shall align with GSA IT Security Procedural Guide 14-69, *"SSL/TLS Implementation."*
SC-13	Cryptographic Protection	L, M, H	Implemented encryption algorithms and cryptographic modules shall be FIPS-approved and FIPS PUB 140-2 validated, respectively. ○ Digital signature encryption algorithms - Reference: https://csrc.nist.gov/Projects/Cryptographic-Algorithm-Validation-Program/Validation/Validation-List/DSA ○ Block cypher encryption algorithms - Reference: https://csrc.nist.gov/Projects/Cryptographic-Algorithm-Validation-Program/Block-Ciphers ○ Secure hashing algorithms – Reference: https://csrc.nist.gov/Projects/Cryptographic-Algorithm-Validation-Program/Secure-Hashing

Control ID	Control Title	Baseline	GSA Implementation Guidance
SC-17	PKI Certificates	M, H	Implement appropriate creation, use, and signing of crypto certs in agreement with GSA IT Security Procedural Guide 14-69, *"SSL/TLS Implementation,"* and NIST Special Publications 800-32, NIST 800-63.
SC-18	Mobile Code	M, H	
SC-22	Architecture and Provisioning for Name / Address Resolution Service	L, M, H	Information systems shall be Domain Name System Security Extensions (DNSSEC) compliant. Reference OMB Memorandum M-08-23, which requires all Federal Government departments and agencies that have registered and are operating second level .gov to be DNSSEC.
SC-28 (1)	Protection of Information at Rest | Cryptographic Protection	GSA Required – For systems with Personally Identifiable Information Only	Systems bearing PII must implement protect information at rest. At a minimum, fields bearing PII data must be encrypted with field level encryption. Encryption algorithms shall be FIPS-approved; implemented encryption modules shall be FIPS PUB 140-2 validated.
SI-2	Flaw Remediation	L, M, H	All projects and systems must be adequately tested for flaws; all Critical, High, and Moderate risk findings must be remediated prior to go-live. Post go-live, all critical and high vulnerabilities identified must be mitigated within 30 days and all moderate vulnerabilities mitigated within 90 days.
SI-3	Malicious Code Protection	L, M, H	
SI-4	Information System Monitoring	L, M, H	
SI-10	Information Input Validation	M, H	All system accepting input from end users must validate the input in accordance to industry best practices and published guidelines, including GSA IT Security Procedural Guide 07-35, *"Web Application Security,"* and OWASP Top 10 Web Application Security Vulnerabilities.
AR-2	Privacy Impact and Risk Assessment	See note below	The contractor shall conduct a Privacy Threshold Analysis (PTA) and, if applicable, a Privacy Impact Assessment (PIA) identifying the categories of information and addressing potential risks to PII. The contractor also shall coordinate with the GSA Privacy Office concerning these documents.
AR-8	Accounting of Disclosures	See note below	The contractor shall keep an accurate accounting of disclosures of information held in any system of records under its control.

Control ID	Control Title	Baseline	GSA Implementation Guidance
TR-2	System of Records Notices and Privacy Act Statements	See note below.	The contractor shall coordinate with the GSA Privacy Office to ensure System of Records Notices (SORNs) and Privacy Act notices on forms that collect Personally Identifiable Information (PII) are established and kept current.
UL-1	Internal Use	See note below	The contractor shall ensure that PII is shared internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices.
UL-2	Information Sharing with Third Parties	See note below	The contractor shall coordinate with the GSA Privacy Office to ensure PII is shared in accordance with GSA requirements and agreements with third parties.

Note: Privacy controls are not associated with a baseline. Controls are applicable/not applicable based on PII data being collected, stored, or transmitted.

2.4 Assessment and Authorization (A&A) Activities

The implementation of a new Federal Government IT system requires a formal approval process known as Assessment and Authorization (A&A). NIST Special Publication 800-37, Revision 1 (hereafter described as NIST 800-37) and GSA IT Security Procedural Guide 06-30, "*Managing Enterprise Risk,*" provide guidelines for performing the A&A process. The Contractor system/application must have a valid assessment and authorization, known as an Authority to Operate (ATO) (signed by the Federal government) before going into operation and processing GSA information. The failure to obtain and maintain a valid ATO will result in the termination of the contract. The system must have a new A&A conducted (signed by the Federal government) at least every three (3) years or at the discretion of the Authorizing Official when there is a significant change to the system's security posture or via continuous monitoring based on GSA CIO IT Security 12-66, "*Information Security Continuous Monitoring Strategy*" that is reviewed and accepted by the GSA CISO.

Assessing the System

1. The Contractor shall comply with Assessment and Authorization (A&A) requirements as mandated by Federal laws and policies, including making available any documentation, physical access, and logical access needed to support this requirement. The Level of Effort for the A&A is based on the System's NIST Federal Information Processing Standard (FIPS) Publication 199 categorization. The contractor shall create, maintain and update the following A&A documentation:

    - System Security Plan (SSP) completed in agreement with NIST Special Publication 800-18, Revision 1, *"Guide for Developing Security Plans for Federal Information Systems."* The SSP shall include as appendices required policies and procedures across 17 control families mandated per FIPS PUB 200, Rules of Behavior, and Interconnection Agreements (in agreement with NIST Special Publication 800-47,

"Security Guide for Interconnecting Information Technology Systems"). The SSP shall include; as an appendix, a completed GSA Control Tailoring Workbook identified in Appendix A of this guide. The column in the workbook titled "GSA Defined Values," shall be used to document all contractor implemented settings that are different from the GSA defined setting and where the GSA defined setting allows a contractor determined setting.

- Contingency Plan (including Disaster Recovery Plan) completed in agreement with NIST Special Publication 800-34.
- Contingency Plan Test Report completed in agreement with GSA IT Security Procedural Guide 06-29, *"Contingency Planning."*
- Incident Response Plan completed in agreement with NIST Special Publication 800-61, "Computer Security Incident Handling Guide" and GSA IT Security Procedural Guide 01-02, "*Incident Response*."
- Incident Response Test Report completed in agreement NIST Special Publication 800-61, "Computer Security Incident Handling Guide" and GSA IT Security Procedural Guide 01-02, "*Incident Response*."
- Configuration Management Plan completed in agreement with GSA IT Security Procedural Guide 01-05, "*Configuration Management*."
- Plan of Actions & Milestones completed in agreement with GSA IT Security Procedural Guide 09-44, *"Plan of Action and Milestones (POA&M)."*
- Penetration Test Reports documenting the results of vulnerability analysis and exploitability of identified vulnerabilities. Note: Penetration testing is required for all FIPS PUB 199 Low impact and Moderate impact Internet accessible information systems, and all FIPS PUB 199 High impact information systems are required to complete an independent penetration test and provide an Independent Penetration Test Report documenting the results of the exercise as part of the A&A package. Reference GSA IT Security Procedural Guide 06-30, *"Managing Enterprise Risk"* and GSA IT Security Procedural Guide 11-51, *"Conducting Penetration Test Exercises"* for penetration testing guidance.

2. Information systems must be assessed and authorized every three (3) years or whenever there is a significant change to the system's security posture in accordance with NIST Special Publication 800-37, Revision 1, *"Guide for the Security Certification and Accreditation of Federal Information Systems,"* and CIO IT Security 06-30, "*Managing Enterprise Risk*" or via continuous monitoring based on GSA CIO IT Security 12-66, "*Information Security Continuous Monitoring Strategy*" that is reviewed and accepted by the GSA CISO.

3. At the Moderate impact level and higher, the **<SELECT: contractor or Government>** is responsible for providing an independent Security Assessment/Risk Assessment in accordance with GSA IT Security Procedural Guide 06-30, *"Managing Enterprise Risk."*

4. If the Government is responsible for providing a Security Assessment/Risk Assessment and Penetration Test, the Contractor shall allow GSA employees (or GSA designated third party contractors) to conduct A&A activities to include control reviews in

accordance with NIST 800-53/NIST 800-53A and GSA IT Security Procedural Guide 06-30, *"Managing Enterprise Risk."* Review activities include but are not limited to operating system vulnerability scanning, web application scanning, and database scanning of applicable systems that support the processing, transportation, storage, or security of GSA information. This includes the general support system infrastructure.

5. Identified gaps between required NIST 800-53 controls and the contractor's implementation as documented in the Security Assessment/Risk Assessment report shall be tracked for mitigation in a Plan of Action and Milestones (POA&M) document completed in accordance with GSA IT Security Procedural Guide 09-44, *"Plan of Action and Milestones (POA&M)."* Depending on the severity of the gaps, the Government may require them to be remediated before an Authorization to Operate is issued.
6. The Contractor is responsible for mitigating all security risks found during the A&A and continuous monitoring activities. All high-risk vulnerabilities must be mitigated within 30 days and all moderate risk vulnerabilities must be mitigated within 90 days from the date vulnerabilities are formally identified. The Government will determine the risk rating of vulnerabilities.

Authorization of the System

1. Upon receipt of the documentation (Security Authorization Package (SAP)) described in GSA IT Security Procedural Guide 06-30, *"Managing Enterprise Risk"* and NIST Special Publication 800-37 as documented above, the GSA Authorizing Official (AO) for the system (in coordination with the GSA Chief Information Security Officer (CISO), system Program Manager (PM), Information System Security Manager (ISSM), and Information System Security Officer (ISSO) will render an authorization decision to:
    - Authorize system operation w/out any restrictions or limitations on its operation;
    - Authorize system operation w/restriction or limitation on its operation, or;
    - Not authorize for operation.
2. The Contractor shall provide access to the Federal Government, or their designee acting as their agent, when requested, in order to verify compliance with the requirements for an Information Technology security program. At its option, the Government may choose to conduct on site surveys. The Contractor shall make appropriate personnel available for interviews and documentation during this review. If documentation is considered proprietary or sensitive, these documents may be reviewed on-site under the hosting Contractor's supervision.

2.5 Reporting and Continuous Monitoring

Maintenance of the security authorization to operate will be through continuous monitoring of security controls of the external system and its environment of operation to determine if the security controls in the information system continue to be effective over time in light of changes that occur in the system and environment. Through continuous monitoring, security

controls and supporting deliverables are updated and submitted to GSA per the schedules below. The submitted deliverables (or lack thereof) provide a current understanding of the security state and risk posture of the information systems. They allow GSA AOs to make credible risk-based decisions regarding the continued operations of the information systems and initiate appropriate responses as needed when changes occur.

Deliverables to be provided to the GSA COR/ISSO/ISSM Quarterly

1. Vulnerability Scanning
   Reference: NIST 800-53 control RA-5
   Provide the most recent Web Application and Operating System vulnerability scan reports.

2. Plan of Action & Milestones (POA&M) Update
   Reference: NIST 800-53 control CA-5
   Provide POA&M updates in accordance with requirements and the schedule set forth in GSA CIO IT Security Procedural Guide 09-44, "*Plan of Action and Milestones (POA&M).*"

Deliverables to be provided to the GSA COR/ISSO/ISSM Annually

1. Updated A&A documentation including the System Security Plan and Contingency Plan
   a. System Security Plan
      Reference: NIST 800-53 control PL-2
      Review and update the System Security Plan annually to ensure the plan is current and accurately describes implemented system controls and reflects changes to the contractor system and its environment of operation. The System Security Plan must be in accordance with NIST 800-18, Revision 1, *"Guide for Developing Security Plans."*
   b. Contingency Plan
      Reference: NIST 800-53 control CP-2
      Provide an annual update to the contingency plan completed in accordance with NIST 800-34, *"Contingency Planning Guide."*

2. User Certification/Authorization Review Documents
   Reference: NIST 800-53 control AC-2
   Provide the results of the annual review and validation of system users' accounts to ensure the continued need for system access. The user certification and authorization documents will illustrate the organization establishes, activates, modifies, reviews, disables, and removes information system accounts in accordance with documented account management procedures.

3. Separation of Duties Matrix
   Reference: NIST 800-53 control AC-5

Develop and furnish a separation of duties matrix reflecting proper segregation of duties for IT system maintenance, management, and development processes. The separation of duties matrix will be updated or reviewed on an annual basis.

4. Information Security Awareness and Training Records
   Reference: NIST 800-53 control AT-4
   Provide the results of security awareness (AT-2) and role-based information security technical training (AT-3). AT-2 requires basic security awareness training for employees and contractors that support the operation of the contractor system. AT-3 requires information security technical training to information system security roles. Training shall be consistent with the requirements contained in C.F.R. Part 5 Subpart C (5 C.F.R 930.301) and conducted at least annually.

5. Annual FISMA Self-Assessment
   Reference: NIST 800-53 control CA-2
   Deliver the results of the annual FISMA self-assessment conducted per GSA IT Security Procedural Guide 04-26, "*Federal Information Security Modernization Act (FISMA) Implementation."* Based on the controls selected for self-assessment, the GSA OCISO will provide the appropriate test cases for completion.

6. System(s) Baseline Configuration Standard Document
   Reference: NIST 800-53 control CM-2/CM-2(1)
   Provide a well-defined, documented, and up-to-date specification to which the information system is built.

7. System Configuration Settings Verification
   Reference: NIST 800-53 control CM-6/CM-6(1)
   Establish and document mandatory configuration settings for information technology products employed within the information system that reflect the most restrictive mode consistent with operational requirements. Configuration settings are the configurable security-related parameters of information technology products that compose the information system. Systems should be configured in agreement with GSA technical guidelines, NIST guidelines, Center for Internet Security guidelines (Level 1), or industry best practice guidelines in hardening their systems, as deemed appropriate by the Authorizing Official.

   Provide the most recent operating system Configuration Settings Compliance scan report.

8. Configuration Management Plan
   Reference: NIST 800-53 control CM-9
   Provide an annual update to the Configuration Management Plan for the information system.

9. Contingency Plan Test Report
   Reference: NIST 800-53 control CP-4
   Provide a contingency plan test report completed in accordance with GSA IT Security Procedural Guide 06-29, *"Contingency Planning."* A continuity test shall be

conducted annually prior to mid-July of each year. The continuity test can be a table top test while the system is at the FIPS PUB 199 Low Impact level. The table top test must include Federal and hosting Contractor representatives. Functional exercises must be completed once every three years for FIPS PUB 199 Moderate impact systems and annually for FIPS PUB 199 High impact systems.

10. Incident Response Test Report
    Reference: NIST 800-53 control IR-3
    Provide an incident response plan test report documenting results of incident reporting process per GSA IT Security Procedural Guide 01-02, *"Incident Response."*

11. Information System Interconnection Agreements
    Reference: NIST 800-53 control CA-3
    Provide Interconnection Security Agreements (ISA) and supporting Memoranda of Agreement/Understanding (MOA/U), completed in accordance with NIST 800-47, *"Security Guide for Connecting Information Technology Systems,"* for existing and new interconnections. Per NIST 800-47, an interconnection is the direct connection of two or more IT systems for the purpose of sharing data and other information resources through a pipe, such as ISDN, T1, T3, DS3, VPN, etc. ISAs shall be submitted as appendices as part of the annual System Security Plan submission. ISAs shall include, if applicable, any changes since the last submission; updated ISAs are required at least every three years.

12. Rules of Behavior
    Reference: NIST 800-53 control PL-4
    Define and establish Rules of Behavior for information system users. Rules of Behavior shall be submitted as an appendix to the System Security Plan.

13. Penetration Testing Report
    Reference: NIST 800-53 control CA-8
    All Internet accessible systems, and all FIPS PUB 199 High impact systems are required to complete an independent penetration test and provide a Penetration Test Report documenting the results of the exercise as part of their A&A package. Annual penetration tests are required for these same systems in accordance with GSA Order CIO 2100.1 and CIO-IT Security-11-51, "*Conducting Penetration Test Exercises.*"

14. Personnel Screening and Security
    Reference: NIST 800-53 control PS-3, NIST 800-53 control PS-7
    Furnish documentation reflecting favorable adjudication of background investigations for all personnel (including subcontractors) supporting the system. Contractors shall comply with GSA Order CIO 2100.1, *"GSA Information Technology (IT) Security Policy"* and GSA Order, CIO P 2181.1, "*Homeland Security Presidential Directive-12 (HSPD-12) Personal Identity Verification and Credentialing Handbook*." GSA separates the risk levels for personnel working on Federal computer systems into three categories: Low Risk, Moderate Risk, and High Risk.

- Those contract personnel (hereafter known as "Applicant") determined to be in a Low Risk position will require a National Agency Check with Written Inquiries (NACI) investigation.
- Those Applicants determined to be in a Moderate Risk position will require either a Limited Background Investigation (LBI) or a Minimum Background Investigation (MBI) based on the Contracting Officer's (CO) determination.
- Those Applicants determined to be in a High Risk position will require a Background Investigation (BI).

Applicants will not be reinvestigated if a prior favorable adjudication is on file with FPS or GSA, there has been less than a one year break in service, and the position is identified at the same or lower risk level.

Once a favorable FBI Criminal History Check (Fingerprint Check) has been returned, Applicants may receive a GSA identity credential (if required) and initial access to GSA information systems. The HSPD-12 Handbook contains procedures for obtaining identity credentials and access to GSA information systems as well as procedures to be followed in case of unfavorable adjudications.

Deliverables to be provided to the GSA COR/ISSO/ISSM Biennially

1. Policies and Procedures
   Develop and maintain current the following policies and procedures:
   a. Access Control Policy and Procedures (NIST 800-53 AC-1)
   b. Security Awareness and Training Policy and Procedures (NIST 800-53 AT-1)
   c. Audit and Accountability Policy and Procedures (NIST 800-53 AU-1)
   d. Identification and Authentication Policy and Procedures (NIST 800-53 IA-1)
   e. Incident Response Policy and Procedures (NIST 800-53 IR-1, reporting timeframes are documented in GSA IT Security Procedural Guide 01-02, "*Incident Response*"
   f. System Maintenance Policy and Procedures (NIST 800-53 MA-1)
   g. Media Protection Policy and Procedures (NIST 800-53 MP-1)
   h. Physical and Environmental Policy and Procedures (NIST 800-53 PE-1)
   i. Personnel Security Policy and Procedures (NIST 800-53 PS-1)
   j. System and Information Integrity Policy and Procedures (NIST 800-53 SI-1)
   k. System and Communication Protection Policy and Procedures (NIST 800-53 SC-1)
   l. Key Management Policy (NIST 800-53 SC-12)

2.6 GSA Privacy Requirements

Personally identifiable information (PII) **<SELECT: is or is not>** in the scope of the acquisition and PII **<SELECT: is or is not>** expected to be stored, processed, or transmitted in the vendor's information system. The collection, maintenance or dissemination of any PII that is subject to the Privacy Act and/or the E-Government Act will be handled in full accordance with all GSA rules of conduct and in accordance with GSA Privacy Program requirements.

The contractor shall prepare a Privacy Threshold Analysis (PTA) to confirm and document PII is not in scope, or to determine which categories of information will be stored, processed, or transmitted by the system. The PTA must be completed before development begins and whenever a change with a privacy impact (e.g., a new category of information is collected) is made to an existing system. PTAs are required as part of GSA's process to determine whether a Privacy Impact Assessment (PIA) and/or a System of Records Notice (SORN) is required, and if any other privacy requirements apply to the information system. Instructions for the PTA and PIA forms can be found at https://www.gsa.gov/reference/gsa-privacy-program/privacy-impact-assessments-pia.

PII (should it come into scope) will require the following guidelines be adhered to.

- The vendor's information system must be authorized at least at the FIPS PUB 199 Moderate level.
- For any system that collects, maintains or disseminates PII, a PIA must be completed by the contractor and provided to the GSA Privacy Office for review along with the other authorization to operate (ATO) documents.
- If the system retrieves information using PII, the Privacy Act applies and it must have a system of records notice (SORN) published in the Federal Register.
- If PII is collected from individuals by the system, a Privacy Act Statement (i.e., Privacy Notice) must be provided to users prior to their use of the application on what data is being collected and why, as well as the authority for the collection and the impact of not providing some or all of it. The Privacy Act Statement must be available to the individual directly on the form used to collect the information. Providing a link back to the Statement from the form is acceptable.

Provided below is a template for an acceptable Privacy Act Statement, when bracketed sections are completed. A completed example is available at https://www.gsa.gov/reference/gsa-privacy-program/privacy-act-statement-for-design-research.

Privacy Act Statement

This (insert voluntary or mandatory) collection of personal information in authorized by (insert legal authority). We collect (developer insert categories of PII collected, e.g., name, email, etc.). Your personal information is collected so we can (developer insert purpose of collection and what effect on the individual, if any, not providing any or all of the information may have). Your personal information is stored in (developer insert GSA system name). GSA may use this information pursuant to its published Privacy Act system of records notice (insert link to applicable GSA Privacy Act SORN).

Note: Systems that access data a user creates must assume a user may include privacy data/PII in the system unless the data creation is restricted to data controlled by the system.

All contractor staff who have significant privacy information responsibilities must complete GSA's specialized Privacy 201 Training. This includes contractors who work with PII as part of their work duties (e.g.; Human Resource staff, Finance staff, and managers/supervisors).

2.7 Additional Stipulations

1. Deliverables shall be labeled Sensitive But Unclassified (SBU) or contractor selected designation per document sensitivity. External transmission/dissemination of SBU to or from a Government computer must be encrypted. Certified encryption modules must be used in accordance with FIPS PUB 140-2, *"Security Requirements for Cryptographic Modules."*
2. The Contractor shall certify applications are fully functional and operate correctly as intended on systems using the United States Government Configuration Baseline (USGCB). This includes Internet Explorer configured to operate on Windows. The standard installation, operation, maintenance, update, and/or patching of software shall not alter the configuration settings from the approved USGCB configuration. The information technology should also use the Windows Installer Service for installation to the default "program files" directory and should be able to silently install and uninstall. Applications designed for normal end users shall run in the standard user context without elevated system administration privileges. The contractor shall use Security Content Automation Protocol (SCAP) validated tools with USGCB Scanner capability to certify their products operate correctly with USGCB configurations and do not alter USGCB settings.
3. The Contractor shall cooperate in good faith in defining non-disclosure agreements that other third parties must sign when acting as the Federal government's agent.
4. The Government has the right to perform manual or automated audits, scans, reviews, or other inspections of the vendor's IT environment being used to provide or facilitate services for the Government. The Contractor shall be responsible for the following privacy and security safeguards:
    a. The Contractor shall not publish or disclose in any manner, without the Contracting Officer's written consent, the details of any safeguards either designed or developed by the Contractor under this contract or otherwise provided by the Government. Exception - Disclosure to a Consumer Agency for purposes of A&A verification or to the MAX.Gov portal. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours of the request. Access to support incident investigations, shall be provided as soon as possible but not longer than 72 hours after request.

    The program of inspection shall include, but is not limited to:

    - Authenticated and unauthenticated operating system/network vulnerability scans
    - Authenticated and unauthenticated web application vulnerability scans

- Authenticated and unauthenticated database application vulnerability scans
- Automated scans can be performed by Government personnel, or agents acting on behalf of the Government, using Government operated equipment, and Government specified tools. If the vendor chooses to run its own automated scans or audits, results from these scans may at the Government's discretion, be accepted in lieu of Government performed vulnerability scans. In these cases, scanning tools and their configuration shall be approved by the Government. In addition, the results of vendor-conducted scans shall be provided in full to the Government.

b. If new or unanticipated threats or hazards are discovered by either the Government or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.

5. The Contractor shall comply with Section 1634 of Public Law 115-91 that prohibits use of any hardware, software, or services developed or provided, in whole or in part, by— (1) Kaspersky Lab (or any successor entity); (2) any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or (3) any entity of which Kaspersky Lab has majority ownership.

3 Internal Information Systems - IT Security and Privacy Requirements

3.1 Required Policies and Regulations for GSA Contracts

Federal Laws and Regulations:

The contractor shall comply with all applicable Federal Laws and Regulations.

- 40 U.S.C. 11331, "*Responsibilities for Federal Information Systems Standards*"
- FISMA of 2014, "*The Federal Information Security Modernization Act of 2014*"
- HSPD 12, "*Homeland Security Presidential Directive 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*"
- OMB Circular No. A-130, "*Managing Information as a Strategic Resource*"
- OMB M-08-23, "*Securing the Federal Government's Domain Name System Infrastructure (Submission of Draft Agency Plans Due by September 5, 2008)*"
- OMB M 14-03, "*Enhancing the Security of Federal Information and Information Systems*"
- OMB M-10-23, "*Guidance for Agency Use of Third-Party Websites and Applications*"
- OMB M-15-13, "*Policy to Require Secure Connections across Federal Websites and Web Services*"
- OMB M-17-12, "*Preparing for and Responding to a Breach of Personally Identifiable Information*"
- Privacy Act of 1974, "*5 USC, § 552a*"
- OMB Memoranda, location of current fiscal year guidance on Federal Information Security and Privacy Management Requirements, including FISMA reporting

Federal Standards and Guidance:

The contractor shall comply with all applicable Federal Information Processing Standards (FIPS). NIST Special Publications (800 Series) are guidance, unless required by a FIPS publication, in which case usage is mandatory.

- FIPS PUB 199, "*Standards for Security Categorization of Federal Information and Information Systems*"
- FIPS PUB 200, "*Minimum Security Requirements for Federal Information and Information Systems*"
- FIPS PUB 140-2, "*Security Requirements for Cryptographic Modules*"
- NIST SP 800-18, Revision 1, "*Guide for Developing Security Plans for Federal Information Systems*"
- NIST SP 800-30, Revision 1, "*Guide for Conducting Risk Assessments*"
- NIST SP 800-34, Revision 1, "*Contingency Planning Guide for Federal Information Systems*"
- NIST SP 800-37, Revision 1, "*Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Lifecycle Approach*"
- NIST SP 800-47, "*Security Guide for Interconnecting Information Technology Systems*"
- NIST SP 800-53, Revision 4, "*Security and Privacy Controls for Federal Information Systems and Organizations*"

- NIST SP 800-53A, Revision 4, *"Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*"
- NIST SP 800-63-3, "*Digital Identity Guidelines*"
- NIST SP 800-122, "*Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*"
- NIST SP 800-137, "*Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*"

GSA Policies:

The contractor shall comply with the following GSA Directives/Policies.

- GSA Order CIO 1878.1, "*GSA Privacy Act Program*"
- GSA Order CIO 1878.2, "*Conducting Privacy Impact Assessments (PIAs) in GSA*"
- GSA Order CIO 2100.1, "*GSA Information Technology (IT) Security Policy*"
- GSA Order CIO 9297.2, "*GSA Information Breach Notification Policy*"

The contractor shall comply with the following GSA policies listed below when inside a GSA building or inside a GSA firewall.

- GSA Order CIO 2100.3, "*Mandatory Information Technology (IT) Security Training Requirement for Agency and Contractor Employees with Significant Security Responsibilities*"
- GSA Order 9732.1 ADM P, "*Suitability and Personnel Security*"

The GSA policies listed in this paragraph must be followed, if applicable.

- GSA Order CIO 2103.1, "*Controlled Unclassified Information (CUI) Policy*"
- GSA Order CIO 2104.1, "*GSA Information Technology (IT) General Rules of Behavior*"
- GSA Order CIO 2182.2, "*Mandatory Use of Personal Identity Verification (PIV) Credentials*"

GSA Procedural Guides:

GSA IT Procedural Guides are guidance, unless required by a GSA Directive/Policy, in which case usage is mandatory.

Note: GSA's Procedural Guides are updated frequently; to make sure you have the most recent version of publicly available procedural guides, visit GSA.gov. If a non-publicly available guide is needed, contact the contracting officer who will coordinate with GSA Office of the Chief Information Security Officer to determine if it can be made available.

3.2 GSA Security Compliance Requirements

FIPS PUB 200, *"Minimum Security Requirements for Federal Information and Information Systems,"* is a mandatory federal standard that defines the minimum security requirements for federal information and information systems in seventeen security-related areas. Information

systems supporting GSA must meet the minimum security and privacy requirements through the use of the security controls in accordance with NIST Special Publication 800-53, Revision 4 (hereafter described as NIST 800-53), *"Security and Privacy Controls for Federal Information Systems and Organizations."*

To comply with the federal standard, GSA must determine the security category of the information and information system in accordance with FIPS PUB 199, *"Standards for Security Categorization of Federal Information and Information Systems,"* and then the contractor shall apply the appropriately tailored set of Low, Moderate, or High impact baseline security controls in NIST 800-53, as determined by GSA. NIST 800-53 controls requiring organization-defined parameters (i.e., password change frequency) shall be consistent with GSA specifications. The GSA-specified control parameters and supplemental guidance defining more specifically the requirements per FIPS PUB 199 impact level are available in the GSA Control Tailoring Workbook referenced in Appendix A of this document.

The Contractor shall use GSA technical guidelines, NIST guidelines, Center for Internet Security (CIS) guidelines (Level 1), or industry best practice guidelines in hardening their systems. Where a GSA security hardening benchmark exists, it must be used. GSA security hardening benchmarks may be exceeded but not lowered. GSA benchmarks are available on the GSA Intranet and will be provided by GSA upon request.

3.3 Essential Security Controls

All NIST 800-53 controls must be implemented as per the applicable FIPS PUB 199 Low, Moderate, or High baseline. The following table identifies essential security controls from the respective baselines to highlight their importance; ensure they are implemented; and identify integration requirements with GSA's IT and IT Security environment (if any). Contractor systems shall ensure these essential security controls are implemented. Further, the Contractor shall make the proposed system and security architecture of the information system available to the Security Engineering Division, in the Office of the Chief Information Security Officer for review and approval before commencement of system build (architecture, infrastructure, and code).

Control ID	Control Title	Baseline	GSA Implementation Guidance
AC-2	Account Management	L, M, H	Account management systems must leverage or integrate seamlessly with an existing GSA Access and Identity Management Solution such as GAMS, PIV-based authentication, or other GSA-supported Single-Sign-On solution.
AC-17 (3)	Remote Access | Managed Access Control Points	M, H	All remote accesses to the internal information system must be routed through GSA's managed network access control points, subjecting them to security monitoring.

Control ID	Control Title	Baseline	GSA Implementation Guidance
AU-2	Audit Events	L, M, H	Information systems shall implement audit configuration requirements as documented in applicable GSA IT Security Technical Hardening Guides (i.e., hardening and technology implementation guides); for web applications see GSA IT Security Procedural Guide 07-35, Section 2.8.10, What to Log. For technologies where a Technical Guide and Standard does not exist, events from an industry source such as vendor guidance or Center for Internet Security (CIS) benchmark, recommended by the GSA S/SO or Contractor to be approved by the GSA AO shall be used. Internal Information systems shall transmit OS audit log events to GSA's Enterprise Logging Platform (ELP) when possible. OS audit logs not able to be transmitted o the ELP, web application, database, and other logs will be will be retained by the system owner.
CM-6	Configuration Settings	L, M, H	Information systems shall implement GSA benchmarks for system hardening. GSA benchmarks may be exceeded but not lowered. Where a GSA benchmark does NOT exist, GSA technical guidelines, NIST guidelines, Center for Internet Security guidelines (Level 1), or industry best practice guidelines, as deemed appropriate, may be used. Further, all workstations and servers connected to the GSA network shall have BigFix and have agents installed.
CP-7	Alternative Processing Site	M, H	FIPS PUB 199 Moderate and High impact systems must implement processing across geographically-disparate locations to ensure fault tolerance. Amazon Web Services based architectures must implement a multi-region strategy (multiple availability zones in a single region are not sufficient).
CP-8	Telecom Services	M, H	FIP PUB 199 Moderate and High impact information systems must implement alternate telecom services to support resumption when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.
IA-2 (1)	Identification and Authentication (Organizational Users) | Network Access to Privileged Accounts	L, M, H	Information systems shall implement multi-factor authentication for privileged accounts. Information systems shall technically integrate with a GSA supported enterprise identification and authentication solution (e.g., SAML 2.0 with SSO integration (following 2FA with HSPD-12 PIV card)).

Control ID	Control Title	Baseline	GSA Implementation Guidance
IA-2 (2)	Identification and Authentication (Organizational Users) | Network Access to Non-Privileged Accounts	M, H	Information systems at the FIPS PUB 199 Moderate and High impact levels must implement multi-factor authentication for non-privileged accounts. Information systems shall technically integrate with a GSA supported enterprise identification and authentication solution (e.g., SAML 2.0 with SSO integration (following 2FA with HSPD-12 PIV card)).
IA-7	Cryptographic Module Authentication	L, M, H	The information system shall implement FIPS PUB 140-2 compliant encryption modules for authentication functions. Reference: https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules
MP-4	Media Storage	M, H	Digital media including magnetic tapes, external/removable hard drives, flash/thumb drives, diskettes, compact disks and digital video disks shall be encrypted using a FIPS PUB 140-2 certified encryption module.
MP-5	Media Transport	M, H	Digital media including magnetic tapes, external/removable hard drives, flash/thumb drives and digital video disks shall be encrypted using a FIPS PUB 140-2 certified encryption module during transport outside of controlled areas.
PL-8	Information Security Architecture	M, H	All information system security architectures must be formally reviewed and approved by the Office of the Chief Information Security Officer, Security Engineering Division during the system develop/design stages of the SDLC and prior to Security Assessment and Authorization.
RA-5	Vulnerability Scanning	L, M, H	All systems must integrate with the GSA vulnerability scanning tool set managed by the Security Operations Division in the Office of the Chief Information Security Officer. Information systems shall coordinate integration with the scanning program by contacting SecOps@gsa.gov.
SA-22	Unsupported System Components	GSA Required	All systems must be comprised of software and hardware components that are fully supported in terms of security patching for the anticipated life of the system; software must be on GSA's Enterprise Architecture IT Standards List.

Control ID	Control Title	Baseline	GSA Implementation Guidance
SC-8/ SC-8(1)	Transmission Confidentiality and Integration	M, H	Implemented encryption algorithms and cryptographic modules shall be FIPS-approved and FIPS PUB 140-2 validated, respectively. ○ Digital signature encryption algorithms - Reference: https://csrc.nist.gov/Projects/Cryptographic-Algorithm-Validation-Program/Validation/Validation-List/DSA ○ Block cypher encryption algorithms - Reference: https://csrc.nist.gov/Projects/Cryptographic-Algorithm-Validation-Program/Block-Ciphers ○ Secure hashing algorithms – Reference: https://csrc.nist.gov/Projects/Cryptographic-Algorithm-Validation-Program/Secure-Hashing Internet accessible Websites shall implement HTTPS Only and HTTP Strict Transport Security (HSTS), reference OMB Memorandum M-15-13. SSL/TLS implementations shall align with GSA IT Security Procedural Guide 14-69, *"SSL/TLS Implementation."*
SC-13	Cryptographic Protection	L, M, H	Implemented encryption algorithms and cryptographic modules shall be FIPS-approved and FIPS PUB 140-2 validated, respectively. ○ Digital signature encryption algorithms - Reference: https://csrc.nist.gov/Projects/Cryptographic-Algorithm-Validation-Program/Validation/Validation-List/DSA ○ Block cypher encryption algorithms - Reference: https://csrc.nist.gov/Projects/Cryptographic-Algorithm-Validation-Program/Block-Ciphers ○ Secure hashing algorithms – Reference: https://csrc.nist.gov/Projects/Cryptographic-Algorithm-Validation-Program/Secure-Hashing
SC-17	PKI Certificates	M, H	Implement appropriate creation, use, and signing of crypto certs in agreement with GSA IT Security Procedural Guide 14-69, *"SSL/TLS Implementation,"* and NIST Special Publications 800-32, NIST 800-63.
SC-18	Mobile Code	M, H	iOS and Android app creation, usage restrictions. Mobile applications shall undergo assessment and authorization practices as documented in GSA IT Security Procedural Guide 12-67, *"Securing Mobile Devices and Applications."*
SC-22	Architecture and Provisioning for Name / Address Resolution Service	L, M, H	Information systems shall be Domain Name System Security Extensions (DNSSEC) compliant. Reference OMB Memorandum M-08-23, which requires all Federal Government departments and agencies that have registered and are operating second level .gov to be DNSSEC.

Control ID	Control Title	Baseline	GSA Implementation Guidance
SC-28 (1)	Protection of Information at Rest | Cryptographic Protection	GSA Required – For systems with Personally Identifiable Information Only	Systems bearing PII must implement protect information at rest. At a minimum, fields bearing PII data must be encrypted with field level encryption. Encryption algorithms shall be FIPS-approved; implemented encryption modules shall be FIPS PUB 140-2 validated.
SI-2	Flaw Remediation	L, M, H	All projects and systems must be adequately tested for flaws; all Critical, High, and Moderate risk findings must be remediated prior to go-live. Post go-live, all critical and high vulnerabilities identified must be mitigated within 30 days and all moderate vulnerabilities mitigated within 90 days.
SI-3	Malicious Code Protection	L, M, H	All internal information systems must incorporate Bit9 and FireEye HX agents on supported operating systems. These agents will be provided.
SI-4	Information System Monitoring	L, M, H	All information systems must be monitored internally and across ingress/egress points for potentially malicious activity. In addition, all internal information systems must incorporate Bit9 and FireEye HX agents on supported operating systems. These agents will be provided.
SI-10	Information Input Validation	M, H	All system accepting input from end users must validate the input in accordance to industry best practices and published guidelines, including GSA IT Security Procedural Guide 07-35, *"Web Application Security,"* and OWASP Top 10 Web Application Security Vulnerabilities.
AR-2	Privacy Impact and Risk Assessment	See note below	The contractor shall conduct a Privacy Threshold Analysis (PTA) and, if applicable, a Privacy Impact Assessment (PIA) identifying the categories of information and addressing potential risks to PII. The contractor also shall coordinate with the GSA Privacy Office concerning these documents.
AR-8	Accounting of Disclosures	See note below	The contractor shall keep an accurate accounting of disclosures of information held in any system of records under its control.
TR-2	System of Records Notices and Privacy Act Statements	See note below	The contractor shall coordinate with the GSA Privacy Office to ensure System of Records Notices (SORNs) and Privacy Act notices on forms that collect Personally Identifiable Information (PII) are established and kept current.
UL-1	Internal Use	See note below	The contractor shall ensure that PII is shared internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices.

Control ID	Control Title	Baseline	GSA Implementation Guidance
UL-2	Information Sharing with Third Parties	See note below	The contractor shall coordinate with the GSA Privacy Office to ensure PII is shared in accordance with GSA requirements and agreements with third parties.

Note: Privacy controls are not associated with a baseline. Controls are applicable/not applicable based on PII data being collected, stored, or transmitted.

3.4 Assessment and Authorization (A&A) Activities

The implementation of a new Federal Government IT system requires a formal approval process known as Assessment and Authorization (A&A). NIST Special Publication 800-37, Revision 1 (hereafter described as NIST 800-37) and GSA IT Security Procedural Guide 06-30, "*Managing Enterprise Risk,"* provide guidelines for performing the A&A process. The Contractor system/application must have a valid assessment and authorization, known as an Authority to Operate (ATO) (signed by the Federal government) before going into operation and processing GSA information. The failure to obtain and maintain a valid ATO will result in the termination of the contract. The system must have a new A&A conducted (signed by the Federal government) at least every three (3) years or at the discretion of the Authorizing Official when there is a significant change to the system's security posture or via continuous monitoring based on GSA IT Security Procedural Guide 12-66, "*Information Security Continuous Monitoring Strategy*" that is reviewed and accepted by the GSA CISO.

Assessing the System

1. The Contractor shall comply with Assessment and Authorization (A&A) requirements as mandated by Federal laws and policies, including making available any documentation, physical access, and logical access needed to support this requirement. The Level of Effort for the A&A is based on the System's NIST Federal Information Processing Standard (FIPS) Publication 199 categorization. The contractor shall create, maintain and update the following A&A documentation:
    - System Security Plan (SSP) completed in agreement with NIST Special Publication 800-18, Revision 1, *"Guide for Developing Security Plans for Federal Information Systems.*" The SSP shall include as appendices required policies and procedures across 17 control families mandated per FIPS PUB 200, Rules of Behavior, and Interconnection Agreements (in agreement with NIST Special Publication 800-47, *"Security Guide for Interconnecting Information Technology Systems"*). The SSP shall include; as an appendix, a completed GSA Control Tailoring Workbook identified in Appendix A of this guide. The column in the workbook titled "GSA Defined Values," shall be used to document all contractor implemented settings that are different from the GSA defined setting and where the GSA defined setting allows a contractor determined setting.
    - Contingency Plan (including Disaster Recovery Plan) completed in agreement with NIST Special Publication 800-34.

- Contingency Plan Test Report completed in agreement with GSA IT Security Procedural Guide 06-29, *"Contingency Planning*."
- Plan of Actions & Milestones completed in agreement with GSA IT Security Procedural Guide 09-44, *"Plan of Action and Milestones (POA&M)*."
- Penetration Test Reports documenting the results of vulnerability analysis and exploitability of identified vulnerabilities. Note: Penetration testing is required for all FIPS PUB 199 Low impact and Moderate impact Internet accessible information systems, and all FIPS PUB 199 High impact information systems are required to complete an independent penetration test and provide an Independent Penetration Test Report documenting the results of the exercise as part of the A&A package. Reference GSA IT Security Procedural Guide 06-30, *"Managing Enterprise Risk"* and GSA IT Security Procedural Guide 11-51, *"Conducting Penetration Test Exercises"* for penetration testing guidance.

2. Information systems must be assessed and authorized every three (3) years or whenever there is a significant change to the system's security posture in accordance with NIST Special Publication 800-37 Revision 1, "*Guide for the Security Certification and Accreditation of Federal Information Systems,*" and GSA IT Security 06-30, "*Managing Enterprise Risk*" or via continuous monitoring based on GSA CIO IT Security 12-66, "*Information Security Continuous Monitoring Strategy*" that is reviewed and accepted by the GSA CISO.
3. At the Moderate impact level and higher, the **<SELECT: contractor or Government>** is responsible for providing an independent Security Assessment/Risk Assessment in accordance with GSA IT Security Procedural Guide 06-30, *"Managing Enterprise Risk*."
4. If the Government is responsible for providing a Security Assessment/Risk Assessment and Penetration Test, the Contractor shall allow GSA employees (or GSA designated third party contractors) to conduct A&A activities to include control reviews in accordance with NIST 800-53/NIST 800-53A and GSA IT Security Procedural Guide 06-30, *"Managing Enterprise Risk*." Review activities include but are not limited to operating system vulnerability scanning, web application scanning, and database scanning of applicable systems that support the processing, transportation, storage, or security of GSA information. This includes the general support system infrastructure.
5. Identified gaps between required NIST 800-53 controls and the contractor's implementation as documented in the Security Assessment/Risk Assessment report shall be tracked for mitigation in a Plan of Action and Milestones (POA&M) document completed in accordance with GSA IT Security Procedural Guide 09-44, *"Plan of Action and Milestones (POA&M)."* Depending on the severity of the gaps, the Government may require them to be remediated before an Authorization to Operate is issued.
6. The Contractor is responsible for mitigating all security risks found during the A&A and continuous monitoring activities. All high-risk vulnerabilities must be mitigated within 30 days and all moderate risk vulnerabilities must be mitigated within 90 days from the date vulnerabilities are formally identified. The Government will determine the risk rating of vulnerabilities.

Authorization of the System

1. Upon receipt of the documentation (Security Assessment Package, (SAP)) described in GSA IT Security Procedural Guide 06-30, *"Managing Enterprise Risk."* and NIST Special Publication 800-37 as documented above, the GSA Authorizing Official (AO) for the system (in coordination with the GSA Chief Information Security Officer (CISO), system Program Manager (PM), Information System Security Manager (ISSM), and Information System Security Officer (ISSO)) will render an authorization decision to:
    - Authorize system operation w/out any restrictions or limitations on its operation;
    - Authorize system operation w/ restriction or limitation on its operation, or
    - Not authorize for operation.
2. The Contractor shall provide access to the Federal Government, or their designee acting as their agent, when requested, in order to verify compliance with the requirements for an Information Technology security program. At its option, the Government may choose to conduct on site surveys. The Contractor shall make appropriate personnel available for interviews and documentation during this review. If documentation is considered proprietary or sensitive, these documents may be reviewed on-site under the hosting Contractor's supervision.

3.5 Reporting and Continuous Monitoring

Maintenance of the security authorization to operate will be through continuous monitoring of security controls of the contractors system and its environment of operation to determine if the security controls in the information system continue to be effective over time in light of changes that occur in the system and environment. Through continuous monitoring, security controls and supporting deliverables are updated and submitted to GSA per the schedules below. The submitted deliverables (or lack thereof) provide a current understanding of the security state and risk posture of the information systems. They allow GSA AOs to make credible risk-based decisions regarding the continued operations of the information systems and initiate appropriate responses as needed when changes occur.

Deliverables to be provided to the GSA COR/ISSO/ISSM Quarterly

1. Plan of Action & Milestones (POA&M) Update
   Reference: NIST 800-53 control CA-5
   Provide POA&M updates in accordance with requirements and the schedule set forth in GSA CIO IT Security Procedural Guide 09-44, "*Plan of Action and Milestones (POA&M).*"

Deliverables to be provided to the GSA COR/ISSO/ISSM Annually

1. Updated A&A documentation including the System Security Plan and Contingency Plan
    a. System Security Plan

Reference: NIST 800-53 control PL-2
Review and update the System Security Plan annually to ensure the plan is current and accurately describes implemented system controls and reflects changes to the contractor system and its environment of operation. The System Security Plan must be in accordance with NIST 800-18, Revision 1, *"Guide for Developing Security Plans."*

b. Contingency Plan
Reference: NIST 800-53 control CP-2
Provide an annual update to the contingency plan completed in accordance with NIST 800-34, *"Contingency Planning Guide."*

2. User Certification/Authorization Review Documents
Reference: NIST 800-53 control AC-2
Provide the results of the annual review and validation of system users' accounts to ensure the continued need for system access. The user certification and authorization documents will illustrate the organization establishes, activates, modifies, reviews, disables, and removes information system accounts in accordance with documented account management procedures.

3. Separation of Duties Matrix
Reference: NIST 800-53 control AC-5
Develop and furnish a separation of duties matrix reflecting proper segregation of duties for IT system maintenance, management, and development processes. The separation of duties matrix will be updated or reviewed on an annual basis.

4. Information Security Awareness and Training Records
Reference: NIST 800-53 control AT-4
Provide the results of security awareness (AT-2) and role-based information security technical training (AT-3). AT-2 requires basic security awareness training for employees and contractors that support the operation of the contractor system. AT-3 requires information security technical training to information system security roles. Training shall be consistent with the requirements contained in C.F.R. Part 5 Subpart C (5 C.F.R 930.301) and conducted at least annually.

5. Annual FISMA Self-Assessment
Reference: NIST 800-53 control CA-2
Deliver the results of the annual FISMA self-assessment conducted per GSA IT Security Procedural Guide 04-26, "*Federal Information Security Modernization Act (FISMA) Implementation."* Based on the controls selected for self-assessment, the GSA OCISO will provide the appropriate test cases for completion.

6. System(s) Baseline Configuration Standard Document
Reference: NIST 800-53 control CM-2/CM-2(1)
Provide a well-defined, documented, and up-to-date specification to which the information system is built.

7. System Configuration Settings

Reference: NIST 800-53 control CM-6
Establish and document mandatory configuration settings for information technology products employed within the information system that reflect the most restrictive mode consistent with operational requirements. Configuration settings are the configurable security-related parameters of information technology products that compose the information system. Systems shall implement GSA benchmarks for system hardening. GSA benchmarks may be exceeded but not lowered. Where a GSA benchmark does NOT exist, GSA technical guidelines, NIST guidelines, Center for Internet Security guidelines (Level 1), or industry best practice guidelines, as deemed appropriate, may be used.

All workstations and servers connected to the GSA network integrate with BigFix and have agents installed. Provide the most recent operating system Configuration Settings Compliance scan report.

8. Configuration Management Plan
   Reference: NIST 800-53 control CM-9
   Provide an annual update to the Configuration Management Plan for the information system.

9. Contingency Plan Test Report
   Reference: NIST 800-53 control CP-4
   Provide a contingency plan test report completed in accordance with GSA IT Security Procedural Guide 06-29, *"Contingency Planning."* A continuity test shall be conducted annually prior to mid-July of each year. The continuity test can be a table top test while the system is at the FIPS PUB 199 Low Impact level. The table top test must include Federal and hosting Contractor representatives. Functional exercises must be completed once every three years for FIPS PUB 199 Moderate impact systems and annually for FIPS PUB 199 High impact systems.

10. Incident Response Test Report
    Reference: NIST 800-53 control IR-3
    Provide an incident response plan test report documenting results of incident reporting process per GSA IT Security Procedural Guide 01-02, *"Incident Response*."

11. Information System Interconnection Agreements
    Reference: NIST 800-53 control CA-3
    Provide Interconnection Security Agreements (ISA) and supporting Memoranda of Agreement/Understanding (MOA/U), completed in accordance with NIST 800-47, *"Security Guide for Connecting Information Technology Systems,"* for existing and new interconnections. Per NIST 800-47, an interconnection is the direct connection of two or more IT systems for the purpose of sharing data and other information resources through a pipe, such as ISDN, T1, T3, DS3, VPN, etc. ISAs shall be submitted as appendices as part of the annual System Security Plan submission. ISAs shall include, if applicable, any changes since the last submission; updated ISAs are required at least every three years.

12. Rules of Behavior
    Reference: NIST 800-53 control PL-4
    Define and establish Rules of Behavior for information system users. Rules of Behavior shall be submitted as an appendix to the System Security Plan.

13. Penetration Testing Report
    Reference: NIST 800-53 control CA-8
    All Internet accessible systems, and all FIPS PUB 199 High impact systems are required to complete an independent penetration test and provide a Penetration Test Report documenting the results of the exercise as part of their A&A package. Annual penetration tests are required for these same systems in accordance with GSA Order CIO 2100.1 and CIO-IT Security-11-51, "*Conducting Penetration Test Exercises.*"

14. Personnel Screening and Security
    Reference: NIST 800-53 control PS-3, NIST 800-53 control PS-7
    Furnish documentation reflecting favorable adjudication of background investigations for all personnel (including subcontractors) supporting the system. Contractors shall comply with GSA Order CIO 2100.1, "*GSA Information Technology (IT) Security Policy"* and GSA Order CIO P 2181.1, "*Homeland Security Presidential Directive-12 (HSPD-12) Personal Identity Verification and Credentialing Handbook."* GSA separates the risk levels for personnel working on Federal computer systems into three categories: Low Risk, Moderate Risk, and High Risk.

    - Those contract personnel (hereafter known as "Applicant") determined to be in a Low Risk position will require a National Agency Check with Written Inquiries (NACI) investigation.
    - Those Applicants determined to be in a Moderate Risk position will require either a Limited Background Investigation (LBI) or a Minimum Background Investigation (MBI) based on the Contracting Officer's (CO) determination.
    - Those Applicants determined to be in a High Risk position will require a Background Investigation (BI).

    Applicants will not be reinvestigated if a prior favorable adjudication is on file with FPS or GSA, there has been less than a one year break in service, and the position is identified at the same or lower risk level.

    Once a favorable FBI Criminal History Check (Fingerprint Check) has been returned, Applicants may receive a GSA identity credential (if required) and initial access to GSA information systems. The HSPD-12 Handbook contains procedures for obtaining identity credentials and access to GSA information systems as well as procedures to be followed in case of unfavorable adjudications.

Deliverables to be provided to the GSA COR/ISSO/ISSM Biennially

1. Policies and Procedures
   Develop and maintain current the following policies and procedures:
   a. Access Control Policy and Procedures (NIST 800-53 AC-1)
   b. Security Awareness and Training Policy and Procedures (NIST 800-53 AT-1)
   c. Audit and Accountability Policy and Procedures (NIST 800-53 AU-1)
   d. Identification and Authentication Policy and Procedures (NIST 800-53 IA-1)
   e. Incident Response Policy and Procedures (NIST 800-53 IR-1, reporting timeframes are documented in GSA IT Security Procedural Guide 01-02, "*Incident Response*"
   f. System Maintenance Policy and Procedures (NIST 800-53 MA-1)
   g. Media Protection Policy and Procedures (NIST 800-53 MP-1)
   h. Physical and Environmental Policy and Procedures (NIST 800-53 PE-1)
   i. Personnel Security Policy and Procedures (NIST 800-53 PS-1)
   j. System and Information Integrity Policy and Procedures (NIST 800-53 SI-1)
   k. System and Communication Protection Policy and Procedures (NIST 800-53 SC-1)
   l. Key Management Policy (NIST 800-53 SC-12)

3.6 GSA Privacy Requirements

Personally identifiable information (PII) **<SELECT: is or is not>** in the scope of the acquisition and PII **<SELECT: is or is not>** expected to be stored, processed, or transmitted in the vendor's information system. The collection, maintenance or dissemination of any PII that is subject to the Privacy Act and/or the E-Government Act will be handled in full accordance with all GSA rules of conduct and in accordance with GSA Privacy Program requirements.

The contractor shall prepare a Privacy Threshold Analysis (PTA) to confirm and document PII is not in scope, or to determine which categories of information will be stored, processed, or transmitted by the system. The PTA must be completed before development begins and whenever a change with privacy impact (e.g., a new category of information is collected) is made to an existing system. PTAs are required as part of GSA's process to determine whether a Privacy Impact Assessment (PIA) and/or a System of Records Notice (SORN) is required, and if any other privacy requirements apply to the information system. Instructions for the PTA and PIA forms can be found at https://www.gsa.gov/reference/gsa-privacy-program/privacy-impact-assessments-pia.

PII (should it come into scope) will require the following guidelines be adhered to.

- The vendor's information system must be authorized at least at the FIPS PUB 199 Moderate level.
- For any system that collects, maintains or disseminates PII, a PIA must be completed by the contractor and provided to the GSA Privacy Office for review along with the other authorization to operate (ATO) documents.

- If the system retrieves information using PII, the Privacy Act applies and it must have a system of records notice (SORN) published in the Federal Register.
- If PII is collected from individuals by the system, a Privacy Act Statement (i.e., Privacy Notice) must be provided to users prior to their use of the application on what data is being collected and why, as well as the authority for the collection and the impact of not providing some or all of it. The Privacy Act Statement must be available to the individual directly on the form used to collect the information. Providing a link back to the Statement from the form is acceptable.

Provided below is a template for an acceptable Privacy Act Statement, when bracketed sections are completed. A completed example is available at https://www.gsa.gov/reference/gsa-privacy-program/privacy-act-statement-for-design-research.

Privacy Act Statement

This (insert voluntary or mandatory) collection of personal information in authorized by (insert legal authority). We collect (developer insert categories of PII collected, e.g. name, email, etc.). Your personal information is collected so we can (developer insert purpose of collection and what effect on the individual, if any, not providing any or all of the information may have). Your personal information is stored in (developer insert GSA system name). GSA may use this information pursuant to its published Privacy Act system of records notice (insert link to applicable GSA Privacy Act SORN).

Note: Systems that access data a user creates must assume a user may include privacy data/PII in the system unless the data creation is restricted to data controlled by the system.

All contractor staff who have significant privacy information responsibilities must complete GSA's specialized Privacy 201 Training. This includes contractors who work with PII as part of their work duties (e.g.; Human Resource staff, Finance staff, and managers/supervisors).

3.7 Additional Stipulations

1. Deliverables shall be labeled Sensitive But Unclassified (SBU) or contractor selected designation per document sensitivity. External transmission/dissemination of SBU to or from a Government computer must be encrypted. Certified encryption modules must be used in accordance with FIPS PUB 140-2, *"Security Requirements for Cryptographic Modules."*
2. The Contractor shall certify applications are fully functional and operate correctly as intended on systems using the United States Government Configuration Baseline (USGCB). This includes Internet Explorer configured to operate on Windows. The standard installation, operation, maintenance, update, and/or patching of software shall not alter the configuration settings from the approved USGCB configuration. The information technology should also use the Windows Installer Service for installation to the default "program files" directory and should be able to silently install and uninstall. Applications designed for normal end users shall run in the standard user context

without elevated system administration privileges. The contractor shall use Security Content Automation Protocol (SCAP) validated tools with USGCB Scanner capability to certify their products operate correctly with USGCB configurations and do not alter USGCB settings.

3. The Contractor shall cooperate in good faith in defining non-disclosure agreements that other third parties must sign when acting as the Federal government's agent.
4. The Government has the right to perform manual or automated audits, scans, reviews, or other inspections of the vendor's IT environment being used to provide or facilitate services for the Government. The Contractor shall be responsible for the following privacy and security safeguards:
    a. The Contractor shall not publish or disclose in any manner, without the Contracting Officer's written consent, the details of any safeguards either designed or developed by the Contractor under this contract or otherwise provided by the Government. Exception - Disclosure to a Consumer Agency for purposes of A&A verification or to the MAX.Gov portal. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours of the request. Access to support incident investigations, shall be provided as soon as possible but not longer than 72 hours after request.

        The program of inspection shall include, but is not limited to:

        - Authenticated and unauthenticated operating system/network vulnerability scans.
        - Authenticated and unauthenticated web application vulnerability scans
        - Authenticated and unauthenticated database application vulnerability scans.
        - Automated scans can be performed by Government personnel, or agents acting on behalf of the Government, using Government operated equipment, and Government specified tools. If the vendor chooses to run its own automated scans or audits, results from these scans may at the Government's discretion, be accepted in lieu of Government performed vulnerability scans. In these cases, scanning tools and their configuration shall be approved by the Government. In addition, the results of vendor-conducted scans shall be provided in full to the Government.

    b. If new or unanticipated threats or hazards are discovered by either the Government or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.

5. The Contractor shall comply with Section 1634 of Public Law 115-91 that prohibits use of any hardware, software, or services developed or provided, in whole or in part, by— (1) Kaspersky Lab (or any successor entity); (2) any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or (3) any entity of which Kaspersky Lab has majority ownership.

4 Low Impact Software as a Service (LiSaaS) – IT Security and Privacy Requirements

To be considered for award, the contractor must comply with GSA IT's Low-Impact SaaS (LiSaaS) review. The successful vendor will need to ensure any software-as-a-service provided under this contract meets GSA security and privacy requirements prior to invoicing the government for services received under this contract. This includes working with GSA to ensure the Software-as-a-Service (SaaS) passes the current Low-impact-software-as-a-service (LiSaaS) approval process, as outlined in GSA IT Security Procedural Guide 17-75, "*Security Reviews for Low Impact Software as a Service (SaaS) Solutions*." The review process is made up of two main parts: Voluntary Product Accessibility Template (VPAT) for 508 accessibility and security scanning/process reviews. Once this process is complete and the software-as-a-service tool is approved for use by GSA, the CSP will have one year to achieve a FedRAMP authorization. This will either require the software as a service to undergo the FedRAMP Tailored approval process or the standard FedRAMP process for low impact systems. Without a LiSaaS approval, GSA will not be able to use the tool for the base year of the contract, and without FedRAMP approval, GSA will be unable to use the product for the option years of the contract.

The contractor's agreement to the LiSaaS and FedRAMP requirements are required. If the contractor does not agree, no contract award will be made.

If at any time, the vendor is either unwilling or unable to meet any of the process requirements, GSA may choose to cancel the contract and terminate any outstanding orders.

4.1 Assessment of the System

Maintenance of the security authorization to operate will be through continuous monitoring of security controls of the contractors system and its environment of operation to determine if the security controls in the information system continue to be effective over time in light of changes that occur in the system and environment. Through continuous monitoring, security controls and supporting deliverables are updated and submitted to GSA per the schedules below. The submitted deliverables (or lack thereof) provide a current understanding of the security state and risk posture of the information systems. They allow GSA AOs to make credible risk-based decisions regarding the continued operations of the information systems and initiate appropriate responses as needed when changes occur.

The contractor shall provide evidence in support of meeting the requirements for the review activities stated in GSA IT Security Procedural Guide 17-75 and as listed below.

- Unique IDs for each person using the SaaS. Two factor authentication should be used.
- System and security parameters deferred to customers, default settings must be changed.
- Encryption of authentication credentials during transmission.
- Results of web application vulnerability scans.
- Results of operating system vulnerability scans.

- Vendor's flaw remediation process.
- Results of one of the following audits/certifications:
  - Service Organization Control (SOC) 2/Statements on Standards for Attestation Engagements (SSAE) 18
  - SysTrust/WebTrust
  - ISO/IEC 27001
  - Payment Card Industry Data Security Standard (PCI DSS)

4.2 Authorization of the System

The LiSaaS ATO will be valid for no longer than one (1) year. The contractor shall maintain its LiSaaS ATO while pursuing a FedRAMP ATO (i.e., FedRAMP Tailored or the standard FedRAMP process for low impact systems) for its SaaS offering. Without a LiSaaS approval, GSA will not be able to use the tool for the base year of the contract, and without FedRAMP approval, GSA will be unable to use the product for the option years of the contract. If at any time, the vendor is either unwilling or unable to meet any of the process requirements, GSA may choose to cancel the contract and terminate any outstanding orders.

4.3 Reporting and Continuous Monitoring

In support of continuous monitoring the vendor shall maintain its audit report/certification, perform web application and operating system scans, and remediate flaws per the vendor's flaw remediation process. The vendor shall report if its audit report/certification renews or expires and if any of the other required activities cannot be supported.

4.4 Protection of Information

The contractor shall be responsible for properly protecting all information used, gathered, disclosed, or developed as a result of work under this contract. The contractor shall also protect all Government data, etc. by treating the information as sensitive. All information gathered or created under this contract should be considered as confidential information. It is anticipated that this information will be gathered, created and stored within the primary work location. If contractor personnel must remove any information from the primary work area they should protect it to the same extent they would their proprietary data and/or company trade secrets. The use of any information that is subject to the Privacy Act will be utilized in full accordance with all rules of conduct as applicable to Privacy Act Information. Personnel shall adhere to the Privacy Act, Title 5 of the U. S. Code, Section 552a and applicable agency rules and regulations.

4.5 Data Ownership and Unrestricted Rights to Data

All Government data collected in the system is the property of the Federal Government. The Government will retain unrestricted rights to government data. The ordering activity retains All data collected by the system shall be provided by the Contractor (system provider) as requested during the contract period and at the completion of the contract period.

Government data rights of software deliverables shall be in accordance with FAR 52. 227-19 Commercial Computer Software License and/or FAR 52. 227-14 Rights in Data - General. Ownership of data entered into any and all systems, system documentation, all deliverables produced in the performance of this contract, and other related system information shall reside with the Government.

The Contractor shall place the following copyright notice on all materials, documents, deliverables, etc. developed during the performance of this contract:

For purposes of clarity, the intent of the government is for intellectual property to be vested in the federal government for work paid for by the federal government. All documents, graphics, and code created under this contract are the intellectual property of the federal government including, but not limited to, plans, reports, schedules, software code, software designs, graphics, etc. In the event that the federal government implements under this contract open-source software and pays for the cost of the implementation of open-source software, the final changes and edits to the code and configuration (such as work to integrate plug-ins) are the intellectual property of the federal government.

4.6 Personally Identifiable Information

Personally identifiable information (PII) data **is not** in the scope of the acquisition and PII data **is not** expected to be stored in the vendor's SaaS solution. The contractor shall prepare a Privacy Threshold Analysis (PTA) to either document PII is not in scope, or determine which caetgories of information will be stored, processed, or transmitted by the system. The use of any information that is subject to the Privacy Act will be utilized in full accordance with all rules of conduct as applicable to Privacy Act Information.

Privacy data (should it come into scope) will require that the vendor’s SaaS solution be FedRAMP authorized at least at the FIPS PUB 199 Moderate level.

4.7 Data Availability

The data must be available to the Government upon request within one business day or within the timeframe negotiated with the Contractor, and shall not be used for any other purpose other than that specified herein. The contractor shall provide requested data at no additional cost to the government.

4.8 Data Release

Contractor will not disclose Customer Data to any government or third party or access or use Customer Data; except in each case as necessary to maintain the SaaS solution or to provide the SaaS solution to Customer in accordance with this contract, or as necessary to comply with the law or a valid and binding order of a governmental or regulatory body (such as a subpoena or court order). Unless it would be in violation of a court order or other legal requirement, Contractor will give Government reasonable notice of any such legal requirement or order, to allow Government to seek a protective order or other appropriate remedy.

4.9 Confidentiality and Nondisclosure

Personnel (contractor/subcontractor employee)working on any of the described tasks, may at Government request, be required to sign formal non-disclosure and/or conflict of interest agreements to guarantee the protection and integrity of Government information and documents. The Contractor shall submit to the COR a completed confidentiality and non-disclosure agreement form for each individual contractor/subcontractor.

Additionally, any information made available to the Contractor by the Government shall be used only for the purpose of carrying out the provisions of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of the contract. In performance of this contract, the Contractor assumes responsibility for protection of the confidentiality of Government records and shall ensure that all work performed by its subcontractors shall be under the supervision of the Contractor or the Contractor's responsible employees. Each officer or employee of the Contractor or any of its subcontractors to whom any Government record may be made available or disclosed shall be notified in writing by the Contractor that information disclosed to such officer or employee can be used only for that purpose and to the extent authorized herein. Further disclosure of any such information, by any means, for a purpose or to an extent unauthorized herein, may subject the offender to criminal sanctions imposed by 18 U. S. C. §§ 1030.

4.10 Section 508 Compliancy

The Contractor(s) shall provide accessibility based on Section 508 of the Rehabilitation Act of 1973 (29 U. S. C. 794d). All electronic and information technology (EIT) delivered must meet the applicable accessibility standards at 36 CFR 1194, unless an agency exception to this requirement exists. The 36 CFR 1194 implements Section 508 of the Rehabilitation Act of 1973, as amended. All deliverables will be Section 508 compliant, and will be reviewed for compliance by the government which reserves the right to reject the deliverable(s) until remediation of deficiencies has been successfully completed by the Contractor. Complete technical descriptions are provided on the following website: http://www.section508.gov.

Where appropriate, the Contractor(s) shall indicate whether each product or service is compliant or noncompliant with the accessibility standards at 36 CFR 1194. Further, the quote must indicate where full details of compliance can be found (e. g., vendor's website or other exact location).

4.11 Additional Stipulations

1. Deliverables shall be labeled Sensitive But Unclassified (SBU) or contractor selected designation per document sensitivity. External transmission/dissemination of SBU to or from a Government computer must be encrypted. Certified encryption modules must be used in accordance with FIPS PUB 140-2, "*Security Requirements for Cryptographic Modules*."
2. The contractor shall cooperate in good faith in defining non-disclosure agreements that

other third parties must sign when acting as the Federal government's agent.

3. The Government has the right to perform manual or automated audits, scans, reviews, or other inspections of the vendor's IT environment being used to provide or facilitate services for the Government. The Contractor shall be responsible for the following privacy and security safeguards:

    a. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours of the request. Access to support incident investigations, shall be provided as soon as possible but not longer than 72 hours after request.

    b. Physical Access Considerations – If the SaaS provider is operated within an IaaS that is FedRAMP authorized (e. g., AWS); physical access to the physical datacenter environment will be governed by the terms of access allowed by the underlying infrastructure provider as defined in the FedRAMP A&A authorization package.

    c. The program of inspection shall include, but is not limited to:

        - Authenticated and unauthenticated operating system/network vulnerability scans
        - Authenticated and unauthenticated web application vulnerability scans
        - Authenticated and unauthenticated database application vulnerability scans
        - Automated scans can be performed by Government personnel, or agents acting on behalf of the Government, using Government operated equipment, and Government specified tools. If the vendor chooses to run its own automated scans or audits, results from these scans may at the Government's discretion, be accepted in lieu of Government performed vulnerability scans. In these cases, scanning tools and their configuration shall be approved by the Government. In addition, the results of vendor-conducted scans shall be provided in full to the Government.

    d. If new or unanticipated threats or hazards are discovered by either the Government or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.

4. The Contractor shall comply with Section 1634 of Public Law 115-91 that prohibits use of any hardware, software, or services developed or provided, in whole or in part, by— (1) Kaspersky Lab (or any successor entity); (2) any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or (3) any entity of which Kaspersky Lab has majority ownership.

4.12 Terms of Service

Many terms found in commercial ToS or End User License Agreements (EULA) are not acceptable when the Government is the end user. Office of Chief Information Officer (OCIO) requires that software and services within the GSA Enterprise have approved ToS or EULA.

The Contractor's SaaS will undergo a formal review by GSA as part of the review/approval process. The Contractor's ToS shall be found to be acceptable to the government or a modified ToS negotiated as part of the approval review, prior to final authorization.

4.13 References

GSA IT Security Procedural Guide 17-75, "*Security Reviews for Low Impact Software as a Service (SaaS) Solutions*"

FIPS PUB 199, *"Standards for Security Categorization of Federal Information and Information Systems"*

Guide to Understanding FedRAMP

5 Cloud Information Systems – IT Security and Privacy Requirements

The contractor shall implement the controls contained within the FedRAMP Cloud Computing Security Requirements Baseline and FedRAMP Continuous Monitoring Requirements for **<SELECT Low, Moderate, or High>** impact systems (as defined in FIPS PUB 199). These documents define requirements for compliance to meet minimum Federal information security and privacy requirements for **<SELECT Low, Moderate, or High>** impact systems. The FedRAMP baseline controls are based on NIST Special Publication 800-53, Revision 4, *"Security and Privacy Controls for Federal Information Systems and Organizations"* (as amended), and also includes a set of additional controls for use within systems providing cloud services to the federal government.

The contractor shall generally, substantially, and in good faith follow FedRAMP guidelines and Security guidance. In situations where there are no procedural guides, the contractor shall use generally accepted industry best practices for IT security.

GSA may choose to cancel the contract and terminate any outstanding orders if the contractor has its FedRAMP authorization (Joint Authorization Board [JAB] Provisional or Agency) revoked and the deficiencies are greater than agency risk tolerance thresholds.

5.1 Assessment and Authorization

5.2 Assessment of the System

1. The contractor shall comply with FedRAMP requirements as mandated by Federal laws and policies, including making available any documentation, physical access, and logical access needed to support this requirement. The Level of Effort for the A&A is based on the System's FIPS PUB 199 categorization. The contractor shall create, maintain and update the following documentation using FedRAMP requirements and templates, which are available at https://www.fedramp.gov/:
    - Privacy Impact Assessment (PIA)
    - FedRAMP Test Procedures and Results
    - Security Assessment Report (SAR)
    - System Security Plan (SSP)
    - Contingency Plan (CP)
    - Contingency Plan (CP) Test Results
    - Plan of Action and Milestones (POA&M)
    - Continuous Monitoring Plan (CMP)
    - FedRAMP Control Tailoring Workbook
    - Control Implementation Summary Table
    - Results of Penetration Testing
    - Software Code Review

- Interconnection Agreements/Service Level Agreements/Memorandum of Agreements

2. Information systems must be assessed by an accredited FedRAMP Third Party Assessment Organization (3PAO) initially and whenever there is a significant change to the system's security posture in accordance with the FedRAMP Continuous Monitoring Plan.
3. The Government reserves the right to perform Security Assessment and Penetration Testing (of its instance). If the Government exercises this right, the contractor shall allow Government employees (or designated third parties) to conduct Security Assessment and Penetration Testing activities to include control reviews in accordance with FedRAMP requirements. Penetration shall be supported by mutually agreed upon Rules of Engagement (RoE). Review activities include but are not limited to manual penetration testing; automated scanning of operating systems, web applications; wireless scanning; network device scanning to include routers, switches, and firewall, and IDS/IPS; databases and other applicable systems, including general support structure, that support the processing, transportation, storage, or security of Government information for vulnerabilities.
4. The contractor shall provide access to the Federal Government, or their designee acting as their agent, when requested, in order to verify compliance with the requirements for an Information Technology security program. The Government reserves the right to conduct on-site inspections. The contractor shall make appropriate personnel available for interviews and provide all necessary documentation during this review.
5. Physical Access Considerations – If the Cloud Service Provider (CSP) is operated within an Infrastructure as a Service (IaaS) that is FedRAMP authorized (e.g., AWS); physical access to the physical datacenter environment will be governed by the terms of access allowed by the underlying infrastructure provider as defined in the FedRAMP A&A authorization package.
6. Identified gaps between required FedRAMP Security Control Baselines and Continuous Monitoring controls and the contractor's implementation as documented in the Security Assessment Report shall be tracked by the contractor for mitigation in a Plan of Action and Milestones (POA&M) document. Depending on the severity of the gaps, the Government may require them to be remediated before a GSA authorization is issued.
7. The contractor is responsible for mitigating all security risks found during A&A and continuous monitoring activities. All high-risk vulnerabilities must be mitigated within 30 days and all moderate risk vulnerabilities must be mitigated within 90 days from the date vulnerabilities are formally identified. The Government will determine the risk rating of vulnerabilities.

5.3 Authorization of the System

1. If the CSP Software as a Service (SaaS) or Platform as a Service (PaaS) is FedRAMP authorized (i.e., listed as FedRAMP authorized on the FedRAMP website:

   https://marketplace.fedramp.gov/index.html#/products?sort=productName&status=Compliant

   GSA will leverage the CSP's FedRAMP Assessment and Authorization package to document and assess the customer controls for which GSA has responsibility and issue a GSA ATO for the agency's instance of the CSP's SaaS or PaaS offering. The CSP shall work with the GSA to facilitate documentation and assessment of required customer controls, as necessary.

2. If the CSP SaaS or PaaS offering is NOT already FedRAMP authorized, it shall:

   a. Operate on an CSP IaaS environment that is FedRAMP authorized; AND

   b. Be listed as FedRAMP In Process on the FedRAMP Website - https://marketplace.fedramp.gov/index.html#/products?sort=productName&status=In%20Process

      OR be listed as FedRAMP Ready on the FedRAMP website - https://marketplace.fedramp.gov/index.html#/products?sort=productName&status=FedRAMP%20Ready

   c. Shall deliver within 90 days of contract award a FedRAMP Readiness Assessment Review completed by a FedRAMP 3PAO following the FedRAMP Readiness Assessment Guidelines. The FedRAMP Readiness Assessment Review demonstrates the CSPs overall readiness for FedRAMP authorization and whether it has a viable path to achieve a FedRAMP authorization within one (1) year of the contract award. If the CSP does not provide a FedRAMP Readiness Assessment as prescribed or the assessment demonstrates a significant gap in capabilities that will preclude achievement of a FedRAMP authorization within 1 year of the contract award, then, GSA will terminate the contract.

   If requirements a-c, as defined above, are met the CSP will have one (1) year from the date of contract award to achieve FedRAMP authorization. During this transitional period, GSA may issue an agency specific authorization (i.e., not FedRAMP) not to exceed one (1) year (to allow the CSP to achieve FedRAMP compliance) leveraging an existing ATO with another Federal Department/Agency (D/A) (with supporting A&A Package). The CSP may have a non-FedRAMP ATO with another D/A or be based on the GSA Moderate Impact SaaS Solutions process as described in GSA IT Security Procedural Guide 06-30, "*Managing Enterprise Risk.*" The CSP shall make available any existing assessment and authorization package for GSA review and provide necessary documentation and access to facilitate the GSA Moderate Impact SaaS A&A process. Without a FedRAMP authorization within 1 year of contract award; GSA will not be able to use the product for the option years and shall terminate the contract.

3. CSP shall ensure these essential security controls are implemented. CSP shall implement FedRAMP control parameters and implementation guidance, as applicable. Further, the CSP shall make the proposed system and security architecture of the information system available to the Security Engineering Division, in the Office of the Chief Information Security Officer for review and approval before commencement of system build (architecture, infrastructure, and code (as applicable)) and/or the start as A&A activities.

Control ID	Control Title	FedRAMP Baseline
AC-2	Account Management	L, M, H
AU-2	Audit Events	L, M, H
CM-6	Configuration Settings	L, M, H
CP-7	Alternative Processing Site	M, H
CP-8	Telecom Services	M, H
IA-2 (1)	Identification and Authentication (Organizational Users) | Network Access to Privileged Accounts	L, M, H
IA-2 (2)	Identification and Authentication (Organizational Users) | Network Access to Non-Privileged Accounts	M, H
IA-2 (12)	Identification and Authentication (Organizational Users) | Acceptance of PIV Credentials	L, M, H
IA-7	Cryptographic Module Authentication	L, M, H
MP-4	Media Storage	M, H
MP-5	Media Transport	M, H
PL-8	Information Security Architecture	M, H
RA-5	Vulnerability Scanning	L, M, H
SC-8 / SC-8(1)	Transmission Confidentiality and Integrity / Transmission Confidentiality and Integrity | Cryptographic or Alternate Physical Protection	M, H
SC-13	Cryptographic Protection	L, M, H
SC-17	PKI Certificates	M, H
SC-18	Mobile Code	M, H
SC-22	Architecture and Provisioning for Name / Address Resolution Service	L, M, H

Control ID	Control Title	FedRAMP Baseline
SC-28 (1)	Protection of Information at Rest | Cryptographic Protection	M, H
SI-2	Flaw Remediation	L, M, H
SI-3	Malicious Code Protection	L, M, H
SI-4	Information System Monitoring	L, M, H
SI-10	Information Input Validation	M, H

5.4 Reporting and Continuous Monitoring

Maintenance of the FedRAMP Authorization will be through continuous monitoring and periodic audit of the operational controls within a contractor's system, environment, and processes to determine if the security controls in the information system continue to be effective over time in light of changes that occur in the system and environment. Through continuous monitoring, security controls and supporting deliverables are updated in agreement with FedRAMP guidelines and submitted to the MAX.Gov Portal or repository designated by the FedRAMP program.

The submitted deliverables (or lack thereof) provide a current understanding of the security state and risk posture of the information systems. The deliverables will allow the Federal Departments/Agencies leveraging the services providers' cloud offering to make credible risk-based decisions regarding the continued operations of the information systems and initiate appropriate responses as needed when changes occur. Contractors will be required to provide updated deliverables and automated data feeds as defined in the FedRAMP Continuous Monitoring Plan.

The contractor shall provide continuous monitoring deliverables in support of a one (1) year conditional authorization (if necessary) to achieve FedRAMP authorization. Deliverables shall include:

- Quarterly OS, web, and database vulnerability scans (deliverable shall include raw results and findings shall be included in the POA&M document);
- Quarterly Plan of Action and Milestones (POA&M);
- Annual A&A Package updates including the System Security Plan, Contingency Plan, Configuration Management Plan, Contingency Plan Test Report, and Annual FISMA Assessment.

Upon achievement of FedRAMP authorization, GSA will accept the FedRAMP A&A and continuous monitoring documentation made available on the MAX.Gov Portal or a repository designated by the FedRAMP program in agreement with FedRAMP guidelines to satisfy the continuous monitoring requirement.

5.5 Personnel Security Requirements

Contractor shall furnish documentation reflecting favorable adjudication of background investigations for all personnel (including subcontractors) supporting the system. Contractors shall comply with GSA Order CIO 2100.1, "*GSA Information Technology (IT) Security Policy,"* and GSA Order CIO P 2181.1, "*HSPD-12 Personal Identity Verification and Credentialing Handbook*." GSA separates the risk levels for personnel working on Federal computer systems into three categories: Low Risk, Moderate Risk, and High Risk.

- Those contract personnel (hereafter known as "Applicant") determined to be in a Low Risk position will require a National Agency Check with Written Inquiries (NACI) investigation.
- Those Applicants determined to be in a Moderate Risk position will require either a Limited Background Investigation (LBI) or a Minimum Background Investigation (MBI) based on the Contracting Officer's (CO) determination.
- Those Applicants determined to be in a High Risk position will require a Background Investigation (BI).

Applicants will not be reinvestigated if a prior favorable adjudication is on file with FPS or GSA, there has been less than a one year break in service, and the position is identified at the same or lower risk level.

Once a favorable FBI Criminal History Check (Fingerprint Check) has been returned, Applicants may receive a GSA identity credential (if required) and initial access to GSA information systems. The HSPD-12 Handbook contains procedures for obtaining identity credentials and access to GSA information systems as well as procedures to be followed in case of unfavorable adjudications.

GSA shall sponsor the investigation when deemed necessary. No access shall be given to government computer information systems and government sensitive information without a background investigation being verified or in process. If results of background investigation are not acceptable, then access shall be terminated.

The Contractor shall provide a report of separated staff on a monthly basis, beginning 60 days after execution of the option period.

5.6 Sensitive Information Storage

Sensitive But Unclassified (SBU) information, data, and/or equipment will only be disclosed to authorized personnel on a need-to-know basis. The contractor shall ensure that appropriate administrative, technical, and physical safeguards are established to ensure the security and confidentiality of this information, data, and/or equipment is properly protected. When no longer required, this information, data, and/or equipment will be returned to Government control, destroyed, or held until otherwise directed. Destruction of items shall be accomplished by following NIST Special Publication 800-88, *"Guidelines for Media Sanitization."* The

destruction, purging or clearing of media specific to the CSP will be recorded and supplied upon request of the Government.

5.7 Protection of Information

The contractor shall be responsible for properly protecting all information used, gathered, or developed as a result of work under this contract. The contractor shall also protect all Government data, equipment, etc. by treating the information in accordance with its FISMA system categorization.

All information about the systems gathered or created under this contract should be considered as SBU information. If contractor personnel must remove any information from the primary work area that is included in the ATO boundary, they should protect it to the same FedRAMP requirements. The use of any information that is subject to the Privacy Act will be utilized in full accordance with all rules of conduct as applicable to Privacy Act Information.

5.7.1 Unrestricted Rights to Data

The government will retain unrestricted rights to government data. The ordering activity retains ownership of any user created/loaded data and applications hosted on vendor's infrastructure, as well as maintains the right to request full copies of these at any time.

5.7.2 Personally Identifiable Information

Personally identifiable information (PII) **<SELECT: is or is not>** in the scope of acquisition and PII **<SELECT: is or is not>** expected to be stored in the vendor's cloud solution. The collection, maintenance or dissemination of any PII that is subject to the Privacy Act and/or the E-Government Act will be handled in full accordance with all GSA rules of conduct and in accordance with GSA Privacy Program requirements.

PII (should it come into scope) will require that the vendor's cloud solution be FedRAMP authorized at least at the FIPS PUB 199 Moderate level.

5.7.3 Data Availability

The data must be available to the Government upon request within one business day or within the timeframe negotiated with the Contractor, and shall not be used for any other purpose other than that specified herein. The contractor shall provide requested data at no additional cost to the government.

5.7.4 Data Release

Any information made available to the Contractor by the Government shall be used only for the purpose of carrying out the provisions of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of the contract. In performance of this contract, the Contractor assumes responsibility for protection of the confidentiality of Government records and shall ensure that all work performed by its subcontractors shall be under the supervision of the Contractor or the Contractor's

responsible employees. Each officer or employee of the Contractor or any of its subcontractors to whom any Government record may be made available or disclosed shall be notified in writing by the Contractor that information disclosed to such officer or employee can be used only for that purpose and to the extent authorized herein. Further disclosure of any such information, by any means, for a purpose or to an extent unauthorized herein, may subject the offender to criminal sanctions imposed by 18 U.S.C. §§ 1030.

Contractor will not disclose Customer Data to any government or third party or access or use Customer Data; except in each case as necessary to maintain the Cloud Services or to provide the Cloud Services to Customer in accordance with this contract, or as necessary to comply with the law or a valid and binding order of a governmental or regulatory body (such as a subpoena or court order). Unless it would be in violation of a court order or other legal requirement, Contractor will give Government reasonable notice of any such legal requirement or order, to allow Government to seek a protective order or other appropriate remedy.

5.8 Data Ownership

All Government data collected in the system is the property of the Federal Government. All data collected by the system shall be provided by the Contractor (system provider) as requested during the contract period and at the completion of the contract period.

5.9 Confidentiality and Nondisclosure

Personnel working on any of the described tasks, may at Government request, be required to sign formal non-disclosure and/or conflict of interest agreements to guarantee the protection and integrity of Government information and documents.

Additionally, any information made available to the Contractor by the Government shall be used only for the purpose of carrying out the provisions of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of the contract. In performance of this contract, the Contractor assumes responsibility for protection of the confidentiality of Government records and shall ensure that all work performed by its subcontractors shall be under the supervision of the Contractor or the Contractor's responsible employees. Each officer or employee of the Contractor or any of its subcontractors to whom any Government record may be made available or disclosed shall be notified in writing by the Contractor that information disclosed to such officer or employee can be used only for that purpose and to the extent authorized herein. Further disclosure of any such information, by any means, for a purpose or to an extent unauthorized herein, may subject the offender to criminal sanctions imposed by 18 U.S.C. §§ 1030.

5.10 GSA Non-Disclosure Agreement

Each individual contractor/subcontractor employee who performs work on this contract is required to sign an Employee Non-Disclosure Agreement. The Contractor shall submit to the

COR a completed confidentiality and non-disclosure agreement form for each individual contractor/subcontractor.

The Contractor and all contractor/subcontractor employees may have access to sensitive data, proprietary, or confidential business information of other companies or the Government in the course of performing official duties on this contract. The term "proprietary information" means any information considered so valuable by its owners that it is held in secret by them and their licensees and is not available to the public.

All information that is (1) obtained related to or derived from this contract, and (2) results from or derived from any actual tasks assigned to contractor employees while participating on this contract is considered proprietary.

The Contractor and all contractor/subcontractor employees will not use vendor proprietary information except as necessary to perform this contract, and shall agree not to disclose such information to third parties, including any employee of the contractor/subcontractor who has not executed this nondisclosure agreement, or use such information in any manner inconsistent with the purpose for which it was obtained. Anyone failing to comply with the agreement may be subject to disciplinary action or termination of employment by the contractor/subcontractor, and possible administrative, civil, or criminal penalties.

5.11 Additional Stipulations

1. Deliverables shall be labeled Sensitive But Unclassified (SBU) or contractor selected designation per document sensitivity. External transmission/dissemination of SBU to or from a Government computer must be encrypted. Certified encryption modules must be used in accordance with FIPS PUB 140-2, *"Security Requirements for Cryptographic Modules."*
2. The Contractor shall certify applications are fully functional and operate correctly as intended on systems using the United States Government Configuration Baseline (USGCB). This includes Internet Explorer configured to operate on Windows. The standard installation, operation, maintenance, update, and/or patching of software shall not alter the configuration settings from the approved USGCB configuration. The information technology should also use the Windows Installer Service for installation to the default "program files" directory and should be able to silently install and uninstall. Applications designed for normal end users shall run in the standard user context without elevated system administration privileges. The contractor shall use Security Content Automation Protocol (SCAP) validated tools with USGCB Scanner capability to certify their products operate correctly with USGCB configurations and do not alter USGCB settings.
3. The contractor shall cooperate in good faith in defining non-disclosure agreements that other third parties must sign when acting as the Federal government's agent.
4. The contractor shall comply with any additional FedRAMP privacy requirements.

5. The Government has the right to perform manual or automated audits, scans, reviews, or other inspections of the vendor's IT environment being used to provide or facilitate services for the Government. The Contractor shall be responsible for the following privacy and security safeguards:
    a. The Contractor shall not publish or disclose in any manner, without the Contracting Officer's written consent, the details of any safeguards either designed or developed by the Contractor under this contract or otherwise provided by the Government. Exception - Disclosure to a Consumer Agency for purposes of A&A verification or to the MAX.Gov portal. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours of the request. Access to support incident investigations, shall be provided as soon as possible but not longer than 72 hours after request.
    b. Physical Access Considerations – If the SaaS provider is operated within an IaaS that is FedRAMP authorized (e.g., AWS); physical access to the physical datacenter environment will be governed by the terms of access allowed by the underlying infrastructure provider as defined in the FedRAMP A&A authorization package.
    c. The program of inspection shall include, but is not limited to:
        - Authenticated and unauthenticated operating system/network vulnerability scans
        - Authenticated and unauthenticated web application vulnerability scans
        - Authenticated and unauthenticated database application vulnerability scans
        - Automated scans can be performed by Government personnel, or agents acting on behalf of the Government, using Government operated equipment, and Government specified tools. If the vendor chooses to run its own automated scans or audits, results from these scans may at the Government's discretion, be accepted in lieu of Government performed vulnerability scans. In these cases, scanning tools and their configuration shall be approved by the Government. In addition, the results of vendor-conducted scans shall be provided in full to the Government.
    d. If new or unanticipated threats or hazards are discovered by either the Government or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.
6. The Contractor shall comply with Section 1634 of Public Law 115-91 that prohibits use of any hardware, software, or services developed or provided, in whole or in part, by— (1)

Kaspersky Lab (or any successor entity); (2) any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or (3) any entity of which Kaspersky Lab has majority ownership.

5.12 References

Guide to Understanding FedRAMP

FedRAMP Cloud Computing Documents

FedRAMP Templates

6 Mobile Application - IT Security and Privacy Requirements

The contractor shall generally, substantially, and in good faith follow GSA IT Security Policy and Guidelines including GSA Order CIO 2100.1, "*GSA Information Technology (IT) Security Policy"* and GSA IT Security Procedural Guide 12-67, "*Securing Mobile Devices and Applications,*" or current versions. In situations where there are no procedural guides, the contractor shall use generally accepted industry best practices for IT security.

6.1 General Mobile Application Guidelines

1. The Mobile Application (App) shall be integrated with a Mobile Device Management (MDM) solution. GSA currently uses MAAS 360.
2. The contractor shall provide to the GSA IT Contracting Officer Representative (COR) the source code and all supporting artifacts of the app for security testing via the GSA Static and mobile Code Scanning program. In addition, the contractor shall actively participate in the program to remediate all findings according to the most recent Static Code Scanning Standard Operating Procedure (SOP) before the beta and production App is accepted by GSA. Once the contract is awarded, GSA will provide a copy of the Static Code Scanning SOP to the contractor.
3. The contractor shall provide clear and concise documentation so that future developers and programmers can understand the processes used and are able to enhance, edit or build upon the original App. All source code information prepared for this App is the property of GSA, Federal Acquisition Service, OCCM and GSA IT.
    - The contractor shall provide detailed process and code documentation.
    - The contractor shall provide App features documentation.
    - The contractor shall support development and updates of a security authorization package for the App following the process requirements documented in GSA IT Security Procedural Guide 12-67, "*Securing Mobile Devices and Applications,"* or current version.

6.2 Mobile Device Security

The contractor shall adhere to the following requirements and guidelines for developing mobile applications. All requirements and guidelines are found in the GSA IT Security Procedural Guide 12-67, "*Securing Mobile Devices and Applications,"* which will be provided upon contract award.

A mobile application, most commonly referred to as an app, is a type of application software designed to run on a mobile device, such as a smartphone or tablet computer. Mobile applications frequently serve to provide users with similar services to those accessed on PCs. Apps are generally small, individual software units with limited capabilities and isolated functionality. The simplest apps are developed to utilize the web browser of the mobile device to provide a feature set integration much like what is found on a user's PC. However, as mobile

app development has grown, a more sophisticated approach involves developing applications specifically for the mobile environment, taking advantage of both its limitations and advantages. For example, apps that use location-based features are inherently built from the ground up with an eye to mobile devices given that you do not have the same concept of location on a PC. With this new paradigm in both mobile platforms and the applications loaded on them, GSA will concentrate security focus on the following goals:

- That all apps loaded have an initial assessment by GSA for acceptability and then a security assessment & authorization, when required
- That all apps are deployed from only trusted sources, following their security/assessment process – This presently is the Apple ITunes store for iOS and the Google Play store for Android. MaaS360 may also be used, once retrieved from these sources, for enterprise deployment
- That Terms of Service (ToS) discipline is adhered to, based on acceptability of an app – either as an individual user or for GSA as an Agency
- That apps deemed to be unacceptable are blacklisted, using MaaS360
- That a mobile app inventory for all devices be maintained
- That GSA developed apps are assessed, evaluated and approved by the AO for the system they support before deployment

6.3 Application Sources

Allowing mobile apps to be loaded from an unknown source presents one of the greatest risks to GSA's environment when using mobile devices. "Side loading" of apps is a process where a user installs an application from a source other than the Apple ITunes store or Google Play store. If a user jailbreaks a device, side loading can occur as well. Jailbreaking, or rooting, is a process where an Operating System (OS) of a mobile device grants a user or application root level access to the OS. While iOS devices that are not jailbroken/rooted protect against sideloading, the Android OS allows a user to turn such protection on/off (allow unknown sources) if not managed by MDM.

As such, the following policies apply to all GSA devices (Government and Bring Your Own Device) used in the environment to protect against side loading of apps:

- Devices shall not be jailbroken/rooted by users or apps loaded by users. GSA's MDM solution shall immediately notify an administrator of all such incidents immediately for remediation.
- Unknown sources shall not be enabled by users or applications. GSA's MDM solution shall immediately notify an administrator of all such incidents for remediation.
- GSA developed apps may be sideloaded for testing purposes only on test devices, but production deployment of GSA developed apps may only be done via the policies outlined below for Apple iOS and Google Android.

The GSA MaaS store may be employed for enterprise deployments, but only after the app has undergone the review/approval processes outlined below:

- Apple App Review guidelines
- Google Play Store Developer Policy Center

6.4 Terms of Service (ToS)

Many terms found in commercial TOS or End User License Agreements (EULA) are not acceptable when the Government is the end user. Office of Chief Information Officer (OCIO) requires that software and services within the GSA Enterprise have approved ToS or EULA.

Apps deemed to be acceptable are loaded at the discretion of the user for either personal use or as a personal productivity tool to further enhance the work experience. As such, use of the App is not mandated by the agency. Therefore, acceptance of the ToS falls upon the user as an individual. This is true even if the App is loaded using a GSA.gov domain account or registered with a user's GSA.gov email address.

Apps that are approved after formal assessment: and include a formal review by GSA Counsel as part of the review/approval process, where the ToS was found to be acceptable to the government or a modified ToS was negotiated as part of the approval review, prior to final authorization. When loaded and activated, the user is accepting the ToS (often a technical function required of the user), not as an individual, but as an employee or contract employee assigned to perform work functions for GSA.

6.5 GSA Privacy Requirements

Personally identifiable information (PII) **<SELECT: is or is not>** in the scope of the acquisition and PII **<SELECT: is or is not>** expected to be stored, processed, or transmitted in the vendor's App. The collection, maintenance or dissemination of any PII that is subject to the Privacy Act and/or the E-Government Act will be handled in full accordance with all GSA rules of conduct and in accordance with GSA Privacy Program requirements.

The contractor shall prepare a Privacy Threshold Analysis (PTA) to confirm and document PII is not in scope, or to determine which categories of information will be stored, processed, or transmitted by the App. The PTA must be completed before development begins and whenever a change with privacy impact (e.g., a new category of information is collected) is made to an existing App. PTAs are required to determine whether a Privacy Impact Assessment (PIA) and/or a System of Records Notice (SORN) is required, and if any other privacy requirements apply to the App. Instructions for the PTA and PIA forms can be found at https://www.gsa.gov/reference/gsa-privacy-program/privacy-impact-assessments-pia.

PII (should it come into scope) will require the following guidelines be adhered to.

- The vendor's App must be authorized at least at the FIPS PUB 199 Moderate level.
- For any system that collects, maintains or disseminates PII, a PIA must be completed by the contractor and provided to the GSA Privacy Office for review along with the other authorization to operate (ATO) documents.

- If the system retrieves information using PII, the Privacy Act applies and it must have a system of records notice (SORN) published in the Federal Register.
- If PII is collected from individuals by the system, a Privacy Act Statement (i.e., Privacy Notice) must be provided to users prior to their use of the application on what data is being collected and why, as well as the authority for the collection and the impact of not providing some or all of it. The Privacy Act Statement must be available to the individual directly on the form used to collect the information. Providing a link back to the Statement from the form is acceptable.

Provided below is a template for an acceptable Privacy Act Statement when bracketed sections are completed. A completed example is available at https://www.gsa.gov/reference/gsa-privacy-program/privacy-act-statement-for-design-research.

Privacy Act Statement

This (insert voluntary or mandatory) collection of personal information is authorized by (insert legal authority). We collect (developer insert categories of PII collected, e.g. name, email, etc.). Your personal information is collected so we can (developer insert purpose of collection and what effect on the individual, if any, not providing any or all of the information may have). Your personal information is stored in (developer insert App name). GSA may use this information pursuant to its published Privacy Act system of records notice (insert link to applicable GSA Privacy Act SORN).

Note: Apps that access data a user creates must assume a user may include privacy data/PII in the application unless the data creation is restricted to data controlled by the App.

All contractor staff who have significant privacy information responsibilities must complete GSA's specialized Privacy 201 Training. This includes contractors who work with PII as part of their work duties (e.g.; Human Resource staff, Finance staff, and managers/supervisors).

6.6 GSA App Development, Assessment, Authorization and Deployment

GSA developed apps are designed to take advantage of the concept of Anytime, Any Where, Any Device (A3) to allow GSA users and customers to access GSA data while mobile. As such, as GSA business lines develop apps for use on the iOS and Android environment, these apps must undergo an assessment and authorization process before being deployed. With that in mind, the following guidelines are to be followed:

- A GSA developed app that supports a GSA FISMA system must be documented in the System Security Plan and authorized to operate as part of a current ATO letter from the respective AO before deployment. GSA IT Security Procedural Guide 06-30, *"Managing Enterprise Risk,"* is to be followed for this process. Any app that is not directly tied to an already existing system authorized to operate must have an assessment performed and subsequently approved for release by the Chief Information Security Officer (CISO).

- Any mobile app development shall result in a minimum of the release of both an iOS and Android version of the app. This ensures coverage to all users within GSA and the maximum coverage for apps released to the public. Any additional application versions for alternate OS mobile platforms may be developed for such apps, but iOS and Android shall remain as the core base OS' for GSA developed mobile apps for all releases.
- All GSA developed apps must follow the respective application review and publication guidelines for the OS to which they were developed as outlined in Section 8.2 of GSA IT Security Procedural Guide 12-67, "*Securing Mobile Devices and Applications"* and the release process documented in this section.
- Other than for testing purposes on non-user provisioned mobile devices, side loading of apps in the environment is not authorized.
- The GSA MaaS360 Store is authorized for enterprise deployment of apps to GSA user devices once that app has been assessed, authorized, and published according to the guidelines outlined in this section.
- Mobile code scanning throughout the development cycle is critical, but before release by the Mobile Device Team, a mobile app must be scanned by the Systems Engineering Division (ISE) Team within the OCISO. This scan is a source code scan using the CheckMarx platform. As with all applications in GSA, no High/Critical findings are allowed from these scan results. Moderate findings should be documented in the respective POA&M for the system by which the app is authorized and accepted by the AO; Low and Informational findings should be taken into consideration by the developers for their next iteration of app development. A detailed process for mobile app release is documented at the end of this section.
- All mobile application development should take into consideration the Open Web Application Security Project (OWASP) Mobile Security Project when developing mobile apps either within GSA or for use by the general public. The guidelines for developing OWASP is outlined below:
  - OWASP Mobile Security Testing Guide
  - OWASP Mobile Security Project Home Page
  - OWASP Security Testing Guidelines for Mobile Apps
- GSA developed mobile apps must undergo an assessment review and approval process before being released for use. These apps fall into two categories that shall have slightly different processes for approval, with many common steps.
- Mobile apps that are developed as part of another system with a current ATO and provide access to an application using a different form factor (smartphones/tablets), such apps must be documented in the System Security Plan for the system they support.
- Mobile apps designed for a specific purpose not part of a current ATO stand alone in their ATO. As these apps do not have a parent system they support, the below listed process is the complete assessment process required for these apps.

All apps must follow the approval processes outlined below:

1. Apps must be scanned prior to release by the GSA Office of the CISO using the Checkmarx Application scanner. No Critical/High findings may remain for approval to be received and any moderate/medium findings must be contained in a POA&M, either for the system the app is a part of, or a separate POA&M if a standalone mobile app.
2. The privacy requirements as stated above must be met.
3. A mobile application security assessment review in accordance with the GSA-IT Procedural Guide: CIO-IT Security-12-67, "*Securing Mobile Devices and Applications*" must be completed and signed by the mobile App owner, mobile App assessor, mobile App Information System Security Manager (ISSM), a representative of the Office of the CSIO, to denote a proper assessment and review was conducted of the mobile app prior to release.

6.7 Intellectual Property

This task order is funded by the United States Government. All intellectual property generated and/or delivered pursuant to this Firm-Fixed Price Statement of Work will be subject to appropriate federal acquisition regulations which entitle the Government to unlimited license rights in technical data and computer software developed exclusively with Government funds, a nonexclusive "paid-up" license to practice any patentable invention or discovery made during the performance of this task order, and a "paid-up" nonexclusive and irrevocable worldwide license to reproduce all works (including technical and scientific articles) produced during this task order.

6.8 Confidentiality and Nondisclosure

The preliminary and final deliverables and all associated working papers and other material deemed relevant by the agency that have been generated by the contractor in the performance of this contract, are the property of the U.S. Government and must be submitted to the COR at the conclusion of the contract. The U.S. Government has unlimited data rights to all deliverables and associated working papers and materials.

All documents produced for this project are the property of the U.S. Government and cannot be reproduced or retained by the contractor. All appropriate project documentation will be given to the agency during and at the end of this contract. The contractor shall not release any information without the written consent of the Contracting Officer.

Personnel working on any of the described tasks may, at Government request, be required to sign formal non-disclosure and/or conflict of interest agreements to guarantee the protection and integrity of Government information and documents.

Additionally, any information made available to the Contractor by the Government shall be used only for the purpose of carrying out the provisions of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the

performance of the contract. In performance of this contract, the Contractor assumes responsibility for protection of the confidentiality of Government records and shall ensure that all work performed by its subcontractors shall be under the supervision of the Contractor or the Contractor's responsible employees. Each officer or employee of the Contractor or any of its subcontractors to whom any Government record may be made available or disclosed shall be notified in writing by the Contractor that information disclosed to such officer or employee can be used only for that purpose and to the extent authorized herein. Further disclosure of any such information, by any means, for a purpose or to an extent unauthorized herein, may subject the offender to criminal sanctions imposed by 18 U.S.C. §§ 1030.

6.9 GSA Non-Disclosure Agreement

Each individual contractor/subcontractor employee who performs work on this contract is required to sign an Employee Non-Disclosure Agreement. The Contractor shall submit to the COR a completed confidentiality and non-disclosure agreement form for each individual contractor/subcontractor.

The Contractor and all contractor/subcontractor employees may have access to sensitive data, proprietary, or confidential business information of other companies or the Government in the course of performing official duties on this contract. The term "proprietary information" means any information considered so valuable by its owners that it is held in secret by them and their licensees and is not available to the public.

All information that is (1) obtained related to or derived from this contract, and (2) results from or derived from any actual tasks assigned to contractor employees while participating on this contract is considered proprietary.

The Contractor and all contractor/subcontractor employees will not use vendor proprietary information except as necessary to perform this contract, and shall agree not to disclose such information to third parties, including any employee of the contractor/subcontractor who has not executed this nondisclosure agreement, or use such information in any manner inconsistent with the purpose for which it was obtained. Anyone failing to comply with the agreement may be subject to disciplinary action or termination of employment by the contractor/subcontractor, and possible administrative, civil, or criminal penalties.

6.10 Personnel Security Requirements

Contractor shall furnish documentation reflecting favorable adjudication of background investigations for all personnel (including subcontractors) supporting the system. Contractors shall comply with GSA Order 2100.1 – "*GSA Information Technology (IT) Security Policy"* and GSA Order CIO P 2181.1 – "*HSPD-12 Personal Identity Verification and Credentialing Handbook*." GSA separates the risk levels for personnel working on Federal computer systems into three categories: Low Risk, Moderate Risk, and High Risk.

- Those contract personnel (hereafter known as "Applicant") determined to be in a Low Risk position will require a National Agency Check with Written Inquiries (NACI) investigation.
- Those Applicants determined to be in a Moderate Risk position will require either a Limited Background Investigation (LBI) or a Minimum Background Investigation (MBI) based on the Contracting Officer's (CO) determination.
- Those Applicants determined to be in a High Risk position will require a Background Investigation (BI).

Applicants will not be reinvestigated if a prior favorable adjudication is on file with FPS or GSA, there has been less than a one year break in service, and the position is identified at the same or lower risk level.

Once a favorable FBI Criminal History Check (Fingerprint Check) has been returned, Applicants may receive a GSA identity credential (if required) and initial access to GSA information systems. The HSPD-12 Handbook contains procedures for obtaining identity credentials and access to GSA information systems as well as procedures to be followed in case of unfavorable adjudications.

GSA shall sponsor the investigation when deemed necessary. No access shall be given to government computer information systems and government sensitive information without a background investigation being verified or in process. If results of background investigation are not acceptable, then access shall be terminated.

The Contractor shall provide a report of separated staff on a monthly basis, beginning 60 days after execution of the option period.

6.11 Additional Stipulations

1. Deliverables shall be labeled Sensitive But Unclassified (SBU) or contractor selected designation per document sensitivity. External transmission/dissemination of SBU to or from a Government computer must be encrypted. Certified encryption modules must be used in accordance with FIPS PUB 140-2, *"Security requirements for Cryptographic Modules."*
2. The Contractor shall certify applications are fully functional and operate correctly as intended on systems using the United States Government Configuration Baseline (USGCB). This includes Internet Explorer configured to operate on Windows. The standard installation, operation, maintenance, update, and/or patching of software shall not alter the configuration settings from the approved USGCB configuration. The information technology should also use the Windows Installer Service for installation to the default "program files" directory and should be able to silently install and uninstall. Applications designed for normal end users shall run in the standard user context without elevated system administration privileges. The contractor shall use Security

Content Automation Protocol (SCAP) validated tools with USGCB Scanner capability to certify their products operate correctly with USGCB configurations and do not alter USGCB settings.

3. The Contractor shall cooperate in good faith in defining non-disclosure agreements that other third parties must sign when acting as the Federal government's agent.
4. The Government has the right to perform manual or automated audits, scans, reviews, or other inspections of the vendor's IT environment being used to provide or facilitate services for the Government. The Contractor shall be responsible for the following privacy and security safeguards:
    a. The Contractor shall not publish or disclose in any manner, without the Contracting Officer's written consent, the details of any safeguards either designed or developed by the Contractor under this contract or otherwise provided by the Government. Exception - Disclosure to a Consumer Agency for purposes of A&A verification or to the MAX.Gov portal. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours of the request. Access to support incident investigations, shall be provided as soon as possible but not longer than 72 hours after request.

        The program of inspection shall include, but is not limited to:

        - Authenticated and unauthenticated operating system/network vulnerability scans
        - Authenticated and unauthenticated web application vulnerability scans
        - Authenticated and unauthenticated database application vulnerability scans
        - Automated scans can be performed by Government personnel, or agents acting on behalf of the Government, using Government operated equipment, and Government specified tools. If the vendor chooses to run its own automated scans or audits, results from these scans may at the Government's discretion, be accepted in lieu of Government performed vulnerability scans. In these cases, scanning tools and their configuration shall be approved by the Government. In addition, the results of vendor-conducted scans shall be provided in full to the Government.

    b. If new or unanticipated threats or hazards are discovered by either the Government or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.

5. The Contractor shall comply with Section 1634 of Public Law 115-91 that prohibits use of any hardware, software, or services developed or provided, in whole or in part, by— (1) Kaspersky Lab (or any successor entity); (2) any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or (3) any entity of which Kaspersky Lab has majority ownership.

Appendix A: GSA Tailoring of NIST 800-53 Controls

The GSA Control Tailoring Workbook contains GSA defined values for NIST SP 800-53 Security and Privacy Controls. The workbook is not publicly available; contact the contracting officer who will coordinate with the GSA Office of the Chief Information Security Officer to determine if it can be made available.

PERFORMANCE WORK STATEMENT

A procurement by the
U.S. General Services Administration
Region 5 Contracting Division

on behalf of

CLIENT AGENCY:

General Services Administration (GSA) GSA Office of Systems Management (QD)
Integrated Award Environment (IAE)/System for Award Management (SAM)
1800 F Street NW Washington, DC 20405.

PROJECT TITLE:

Operations and Maintenance of Federal Procurement Data System (FPDS) Next Generation (NG) - fpds.gov and System for Award Management (SAM) Integration Environment

PROJECT NUMBERS:

47QDCB21K0007 ID16210006

This requirement is being solicited as a Task Order under the COMET BPA

NAICS 541519 - Other Computer Related Services
Product Service Code DB02 IT and Telecom – Compute Support Services, Non-HP

ORIGINAL VERSION DATED

14 December 2020

Post Award Document Revision History

Revision Number	Description of Changes	Requested By	Date

Contents

Contents

1. INTRODUCTION 7
1.1 Requiring Organization Mission 7
Office of Systems Management (OSM), Integrated Award Environment (IAE) 7
Organizational Mission 7
IAE/SAM Program History 7
IAE/SAM Current Status 8
beta.SAM.gov / Modernized SAM.gov 8
1.2 Procurement Objective 8
1.3 Scope 9
1.4 Background 9
1.5 Applicable Documents, Definitions, Abbreviations & Acronyms 9
2A ADMINISTRATIVE OBJECTIVES AND REQUIREMENTS 11
2A.1 General Performance Requirements 11
2A.1.1 Resources 11
2A.1.2 General Communication 11
2A.1.3 Identification of Employee Affiliation 11
2A.1.4 Business Relations 12
2A.1.5 Contractor Response 12
2A.1.6 Professional Appearance 12
2A.1.7 Team Continuity and Employee Retention 12
2A.2 General Meeting Requirements 13
2A.2.1 Initial Business/Kick-off Meeting 13
2A.2.2 Ad hoc Technical / Work Status 13
2A.2.3 Contract Administration Meetings 13
2A.3 Program / Project Management Requirements 13
2A.3.1 General Program / Project Management Requirements 13
2A.3.2 Phase-In Support 14
2A.3.3 Phase-Out Support 14
2A.4 Subcontract Management 14
2B Business and Technical Objectives 14
2B.1 Business Objectives 14
2B.1.1 Operations and Maintenance 14

2B.1.2 Operate and maintain the Entity/Award data to support the Reporting/Search functionality in the modernized Beta.SAM.gov 16
2B.1.3 Help Desk Support 16
2B.1.4 Support retiring the legacy FPDS applications 16
2B.1.5 Maintain Integration code between Legacy SAM and Beta SAM 16
3. QUALITY 16
3.1 Contractor Quality Control Plan (QCP) 16
3.2 Performance Based Requirements - Service Level Agreement (SLA) 17
3.3 Government Quality Assurance Surveillance Plan (QASP) 17
4. DELIVERABLES 18
4.1 Contractor Submission 18
4.2 Government Review 18
4.3 Government Delays in Reviewing Deliverables or Furnishing Items 18
4.4 Deliverable Table 19
4.5 Data Requirements / Descriptions 20
4.5.1 Contractor Employee Non-Disclosure Agreement 20
4.5.2 Kick-off Meeting Minutes 20
4.5.3 Quality Control Plan 20
4.5.4 Staff Matrix 21
4.5.5 Funds and Expenditure Report 21
4.5.6 Monthly Status Report (MSR) (alternate) 21
4.5.7 Technical Reports 22
4.5.8 Trip Reports 22
4.5.9 Phase-In Plan 22
4.5.10 Phase-Out Plan 22
4.5.11 Monthly Invoice 23
4.5.12 Other Reports 24
5. PERFORMANCE PLACE, TIME, AND RESTRICTIONS 24
5.1 Period of Performance 24
5.2 Place of Performance 24
5.2.1 Performance at the Contractor's Facility 24
5.2.2 Performance at the Government's Facility 24
5.2.3 Applicability of Telework 24
5.2.4 Unplanned Government Facility Closures 25
5.3 Time of Performance - Hours of Work 26
5.3.1 Normal Hours 26
5.3.2 Holidays 26

5.3.3 Expedited Performance 26
5.4 Travel....26
5.5 Limitations on Contractor Performance 26
6. PERSONNEL 27
6.1 General Requirements 27
6.2 Specific Expertise and Experience 28
6.3 Training....28
6.3.1 Contractor Staff Training 28
6.3.2 Mandatory Government Training 28
6.4 Key Positions / Key Personnel 29
6.4.1 Definition & List of Key Personnel 29
6.4.2 Key Personnel Substitution 30
6.5 Personnel Retention and Recruitment....31
6.6 Non-Key Personnel Substitutions....31
6.7 Staff Maintenance 31
6.8 Contractor Employee Work Credentials. 31
7. GOVERNMENT FURNISHED PROPERTY/INFORMATION/ACCESS 32
7.1 General....32
7.2 Government Furnished items (Property) 32
7.2.1 Facilities 32
7.2.2 Equipment 32
7.2.3 Materials 32
7.2.4 Data....32
7.3 Use of Government Property....33
7.3.1 Soft Phones 33
7.3.2 Mobile/Wireless Telephones and Smart Devices 33
7.3.3 Electronic Mail (E-mail) 33
7.3.4 Copiers and Fax Machines 33
7.3.5 Computer and Internet 33
7.3.6 Canvassing, Soliciting, or Selling 33
7.3.7 Security Violations Using Government Equipment 33
7.4 Validation of Government Furnished Items (GFI) and Equipment Inventory 34
8. SECURITY 34
8.1 Non-Disclosure Statement. 34
8.2 Compliance with Security Requirements 35
8.2.1 Assessment and Authorization (A&A) 35

8.2.2 GSA Information Technology IT Security Requirements 36
8.2.3 Recurring Security Deliverables 36
8.2.4 Updated A&A documentation including the System Security Plan and Contingency Plan 36
8.2.5. User Certification/Authorization Review Documents 37
8.2.6 Separation of Duties Matrix 37
8.2.7 Information Security Awareness and Training Records 37
8.2.8 Annual FISMA Self-Assessment 37
8.2.9 System(s) Baseline Configuration Standard Document 37
8.2.10 System Configuration Settings Verification 37
8.2.11 Configuration Management Plan 38
8.2.12 Contingency Plan Test Report 38
8.2.13 Incident Response Test Report 38
8.2.14 Information System Interconnection Agreements 38
8.2.15 Rules of Behavior 38
8.2.16 Penetration Testing Report 38
8.2.17 Personnel Screening and Security 39
8.2.18 Policies and Procedures 39
8.3 Employee Security Requirements 40
8.3.1 New Contractor Personnel 40
8.3.2 Departing Contractor Personnel 40
8.4 Common Access Card & ID Badges 40
8.5 Facility Security Requirements 40
8.6 Personal Identity Verification 40
8.7 Additional Security Requirements 40
9. SPECIAL INSTRUCTIONS 41
9.1 Contractor Performance Assessment Reporting System (CPARS) Assessment 41
9.2 Personal Services 41
9.3 Privacy Act 42
9.4 Rehabilitation Act Compliance (Section 508) 42
9.5 Final Invoice and Release of Claims 42
9.6 Other Direct Costs (ODCs) 42
9.6.1 Cost of Software Maintenance Renewals 43
9.7 Avoidance and/or Mitigation of Actual or Potential Organizational Conflicts of Interest 43
9.8 Task Order Management 43
9.8.1 Contracting Officer's Representative (COR) 43
9.8.2 Government Technical Representative 43

9.9 Technical Direction 44
9.10 Data Ownership/Release/Availability/Rights....44
9.11 Data Rights....45
9.12 Limited Use of Data 45
9.13 Proprietary Data....46
9.14 Inspection and Acceptance 46
9.15 Contract Type 46
9.16 Ceiling Price Notification 46
9.17 Task Order Funding 46
Incremental Funding....46
9.18 Material and Material Handling Costs....47
9.19 Productive Direct Labor Hours 47
9.20 Invoicing and Payment....47
9.21 Payment for Unauthorized Work 48
10 ATTACHMENTS 48
Attachment A – Contractor Non-Disclosure Agreement 48
Attachment B – QASP (Quality Assurance Surveillance Plan) 48
Attachment C – FPDS SLA (Service Level Agreement) 48
Attachment D – FPDS FY20 Software Inventory....48
Attachment E – FPDS AWS Server List....48
Attachment F – FPDS NonProd Network Architecture 48
Attachment G – FPDS Production And Coop Network Architecture 48
Attachment H – FPDS Monthly Steward Report Metrics 48
Attachment I – SAM SLA (Service Level Agreement)....48
Attachment J – SAM Integration Software Inventory 48
Attachment K – SAM AWS Server List....48
Attachment L – SAM Integration Network Architecture....48
Attachment M – CIO 12-2018_ IT Policy Requirements Guide....48
Attachment N – IT Security Procedural Guide....48

1. INTRODUCTION

1.1 Requiring Organization Mission

Office of Systems Management (OSM), Integrated Award Environment (IAE)

Organizational Mission

The Integrated Award Environment (IAE) mission is to support a common, secure business environment that facilitates and supports cost-effective acquisition of, and payment for, goods and services; effective management of federal acquisition and assistance awards; and consistent transparency into federal acquisition and assistance awards.
The IAE vision is to continue to evolve and integrate the existing shared portfolio of seven (7) electronic systems used for awarding and administering federal financial assistance (i.e., grants, loans) and contracts through Scaled Agile Framework (SAFe) development processes on the FAS Cloud Services (FCS) platform, or other common platform as specified by the government in writing.
The largest and most complex of the e-Government initiatives, the IAE works on behalf of the acquisition and financial assistance communities to save money, be more efficient, reduce burdens on the communities we serve, and improve federal award management.

Any existing legacy systems shall be operated as normal before they are migrated into the modernized new system. The Contractors are expected to provide the Operations & Maintenance (O&M) support and meet the Service Level Agreement (SLA). The vendor shall also provide transition support to the modernization teams as it relates to FPDS.

IAE/SAM Program History

In 2002, the Integrated Acquisition Environment was created as an e-Government (e-Gov) initiative under the President's Management Agenda. As part of the e-Gov initiative, the Office of Management and Budget (OMB) designated GSA as the executive agent of the Integrated Acquisition Environment. In 2013, the Integrated Acquisition Environment was renamed the Integrated Award Environment (IAE) by its governance to reflect its management of procurement, grants, and federal assistance data. In 2017, the organization was renamed as The Office of Systems Management (QD), Integrated Award Environment (IAE).

The concept behind the IAE is to provide federal agencies and contractors with a shared IT system to manage the acquisition and grants-making process from solicitation through closeout. The goals of the IAE program are to (1) create a simpler, common, integrated Information Technology (IT) service that promotes competition, transparency, and integrity; (2) increase data sharing across the Government and with the public to enable better decisions in procurement, logistics, payment, and performance assessment; and (3) take a unified approach to obtaining modern tools to leverage investment costs across the federal government for award-related IT services.

The IAE enables all phases of the federal awards management lifecycle, manages the common source of entity information for acquisition and financial assistance

(grants and loans) communities, provides a market research source for contract administration to the federal acquisition community as well as private and commercial firms that are interested in doing business with the government, and stores information that the public in general seeks on how tax dollars are being spent. IAE provides subcontract reporting opportunities for agency and contractor communities. IAE provides data for government and non-government stakeholders including the general public.

IAE is governed by the Award Committee for eGov (ACE) structure which includes the Procurement Committee for eGov (PCE) and the Financial Assistance Committee for eGov (FACE). Additionally, all IAE operations are coordinated and prioritized through a Change Control Board (CCB) that consists of voting representatives from each of the 24 Chief Financial Officer (CFO) Act agencies. These same agencies contribute funding for the IAE operations.

IAE/SAM Current Status

IAE currently sees more than one trillion dollars and 3.3 million transactions in federal assistance and procurement awards across all the IAE systems. With growing numbers, IAE currently has more than 3.4 million registered users and more than 500 million hits or page views per month.

The current IAE systems were developed over several years as free-standing, web-based systems to fulfill different roles throughout the acquisition and grants-making process. Many are operated and maintained by independent contractors. Shared functional components of the application stack for these systems are limited to co-location services that cover some systems and a consolidated end-user help desk that supports a different subset of the systems.

Current IAE systems consist of the following:

1. System for Award Management (SAM)
2. Federal Procurement Data System (FPDS)
3. Electronic Subcontracting Reporting System (eSRS)
4. Federal Funding Accountability and Transparency Act (FFATA) Subaward Reporting System (FSRS)
5. Contractor Performance Assessment Reporting System (CPARS)
6. Federal Awardee Performance and Integrity Information System (FAPIIS)
7. beta.SAM.gov

beta.SAM.gov / Modernized SAM.gov

IAE is in the process of merging all seven (7) of our current operational systems into a single website known as SAM.gov (currently being built as beta.SAM.gov) with the goal of streamlining the process for our users who make, receive, and manage federal awards.

1.2 Procurement Objective

The Government's procurement object is to award a task order under ID15210002 to a highly capable company who will provide the Operations & Maintenance (O&M) support and meet the Service Level Agreements (SLA) for the FPDS system and the SAM Integration environment. The FPDS system will be supported until it is migrated into the

modernized IAE beta.SAM.gov/SAM.gov environment. SAM Integration environment support will be ongoing.

This procurement process must be completed and awarded before 2/14/2021 to reduce the risk of not having system continuity due to the existing contract reaching its end. For the SAM Integration environment, work should not start until after the April 2021 SAM cutover to beta.SAM.

1.3 Scope

The scope of this effort encompasses the following work and initiatives.

a. **Operations and Maintenance**
    1. **Operate and maintain the legacy FPDS applications hosted in AWS**
    2. **Operate and maintain all aspects of the SAM Integration Environment hosted in AWS.**
b. **Operate and maintain the Award data to support the Reporting functionality in the modernized Beta.SAM.gov**
c. **Help Desk Support**
d. **Support retiring the legacy FPDS applications**
e. **Meet all GSA and IAE security requirements**
f. **Meet Service Level Agreement (SLA) standards/metrics**
g. **Adhere to Section 508 Mandates for Government**

The details are stated in Section 2B.

This task order will be placed under the Mission Oriented Business Integrated Services (MOBIS) Federal Supply Schedule, Solicitation No.: TFTP-MC-000874-B (Refresh 16) Special Item Number (SIN) 874-1 Consulting Services or the Consolidated Federal Supply Schedule (00CORP), Special Item Number (SIN) C874-1 Consulting Services. It is anticipated that work will be performed using a Labor Hour or Time and Material type order.

Work will be performed over the period of approximately three years, with an anticipated Base Period of 12 months and four Option Periods of 12 months each.

1.4 Background

This procurement was initiated in 2020 when the FPDS system modernization was delayed and the current contract cannot continue O&M services after it expires. The SAM Integration work was added to this procurement as well to support this environment after the cutover to beta.SAM in April 2021.

A highly capable vendor shall be awarded to take over the required O&M and defined tasks in order to have a seamless transition of migrating the FPDS system into the IAE modernization system as well as to support the SAM integration Environment which will be the backend for beta.SAM where cutover is set for April 2021 (see attached network architecture diagrams).

1.5 Applicable Documents, Definitions, Abbreviations & Acronyms

The documents, if required, (i.e., certifications, specifications, standards, policies, and

procedures), current at time of contract/order award, identified in the list below, are incorporated with the same force and effect as if provided in full text. Succeeding revisions may be substituted or incorporated as required with full notice and disclosure to the contractor. The Government will provide access to available documents and technical information as required and upon contractor request, if not available via a hyperlink within this PWS.

1. Applicable Document
   a. **FPDS SLA (Service Level Agreement)**
   b. **FPDS FY20 Software Inventory**
   c. **FPDS FY20 AWS Server List**
   d. **FPDS NonProd Network Architecture**
   e. **FPDS Production And Coop Network Architecture**
   f. **FPDS Monthly Steward Report Metrics**
   g. **SAM SLA (Service Level Agreement)**
   h. **SAM Integration Environment Software Inventory**
   i. **SAM Integration Environment AWS Server List**
   j. **SAM integration Network Architecture**

2. Definitions, Abbreviations & Acronyms

CO – Government Contracting Officer

COR – Contracting Officer's Representative

FCS – FAS Cloud Services, the platform supporting the application for beta.sam.gov / Modernized SAM

FTE – Full Time Equivalent, the number of labor hours equal to those that would be worked by one employee in a year. For this procurement action 1960 hours is considered an FTE.

CPARS – Contractor Performance Assessment Reporting System – This is a system that generates reports that are created by the government evaluators to document contractor performance.

IAE – Integrated Award Environment

Normal Workweek - A work week is 40 hours

Overtime - Time worked by a contractor's employee in excess of the employee's normal workweek. (Note: Premium pay is not authorized under this contract for overtime work.)

OSM – GSA Office of Systems Management

Quality Assurance - A planned and systematic pattern of all actions necessary to provide confidence to the government that adequate technical requirements are established; products and services conform to established technical requirements; and satisfactory performance is achieved. For the purpose of this document, Quality Assurance refers to actions by the government.

Quality Assurance Personnel (QAP) - A functionally qualified government person(s) responsible for surveillance of contractor performance and providing communications to the contractor(s) and PCO.

Quality Assurance Surveillance Plan (QASP) - A plan detailing the contract surveillance procedures and containing the **Objectives, Measures and Expectations** that will be used to evaluate contractor performance of the PWS objectives.

Quality Control - Those actions taken by a contractor to control the production of outputs to ensure that they conform to the contract requirements.

2A ADMINISTRATIVE OBJECTIVES AND REQUIREMENTS

2A.1 General Performance Requirements

2A.1.1 Resources

It is the Government's objective to rely upon Contractor resources to perform this requirement. To meet this object, the Contractor shall furnish or provide all personnel, personnel management and supervision, all related internal supporting business functions (including background and "overhead" personnel), materials, supplies, equipment, and facilities to perform the full range of services required by this PWS. The team cross-training shall be managed by the Contractor to ensure the coverage of the resource changes or absence. Exceptions shall include government furnished items or data if so stipulated in Section 7, below.

2A.1.2 General Communication

It is the Government's objective that the Contractor maintain regular and direct interface with the Contracting Officer (CO); the Contracting Officer's Representative (COR), and other identified Government representatives. The contractor shall not contact nor take direction from unauthorized Government representatives, under any circumstances.

2A.1.3 Identification of Employee Affiliation

In compliance with FAR 37.144(c), contractor employees shall avoid creating an impression in the minds of members of the public or Congress that they are Government officials by taking the following measures.

- All contractor personnel shall be required to wear Government-approved or provided picture identification badges so as to distinguish themselves from Government employees when working at the Government site.
- Additionally, the contractor shall comply with all visitor identification requirements when visiting the Government site.
- When conversing with Government personnel during business meetings, over the telephone or via electronic mail, contractor personnel shall identify themselves as such to avoid situations arising where sensitive topics might be better discussed solely between Government employees.
- Contractors shall identify themselves on any attendance sheet or any coordination documents they may review.
- Electronic mail signature blocks shall identify their company affiliation.

- Where practicable, contractors occupying co-located space with the Government should identify their work space area with their name and company affiliation.

2A.1.4 Business Relations

A primary element of project success is the business relationship between the contractor and Government representatives. It is the Government's objective that a successful business relationship be maintained. The Contractor shall contribute to meeting this objective by making every effort to establish and maintain clear and constant communication channels with the Government authorized representatives for the purpose of:

- Promptly identifying PWS and/or business relationship issues of controversy and the bilateral development and implementation of corrective action plans.
- Ensuring the professional and ethical behavior of contractor personnel.
- Maintaining effective and responsive subcontractor management (if applicable).
- Ensuring the contractor support team is fully aware and engaged in strengthening the interdependency that exists between the contractors and their Government counterparts.
- Facilitating contractor–Government collaboration for continuous improvement in performing PWS tasks, reducing risks and costs, and meeting the mission needs.
- Providing meaningful feedback during discussions about project execution, when required.
-

2A.1.5 Contractor Response

The contractor shall ensure prompt response to Government inquiries, requests for information or requests for contractual actions.

2A.1.6 Professional Appearance

It is the Government's objective that all personnel involved with this project present a professional appearance. To meet this object the Contractor personnel shall present a neat and professional appearance appropriate to the work being performed at all times when interacting with Government representatives, working in Government facilities, or representing the Government at meetings or before third parties.

2A.1.7 Team Continuity and Employee Retention

The Government recognizes the benefits in maintaining the continuity of contractor team members. These benefits include but are not limited to retention of corporate knowledge, minimizing contractor familiarization, maintaining/increasing performance levels, schedule adherence and preserving organizational interfaces developed over time. These benefits also accrue to the Contractor. Within the context of effective and efficient personnel management, the Contractor shall take reasonable and appropriate steps to retain the qualified employees staffed against this contract to maintain continuity and performance while effectively reducing costs borne by the Government.

2A.2 General Meeting Requirements

The contractor shall participate in the following meetings. Nothing discussed in any meetings or discussions between the Government and the contractor shall be construed as adding, deleting, or modifying the contractual agreement without written authorization from the Contracting Officer.

2A.2.1 Initial Business/Kick-off Meeting

Within 5 business days following the contract/order award (or other time mutually agreed between the parties), the contractor and its key personnel shall meet with the GSA CO, GSA COR, and other identified Government representatives to ensure a common understanding of the requirements, goals, expectations, end products, and objectives of the contract/order. The contractor shall discuss the overall understanding of the project and review the background information and materials provided by the Government. Discussions will also include the scope of work, deliverables to be produced, how the efforts will be organized and project conducted; assumptions made/expected end results. A concerted effort shall be made to gain a thorough understanding of the Government expectations. However, nothing discussed in this or in any subsequent meetings or discussions between the Government and the contractor shall be construed as adding, deleting, or modifying any contract/order requirements, including deliverable specifications and due dates. The contractor shall also address the status of any issues that will affect contractor start-up/ramp-up toward achieving full service/support capability. The contractor will be responsible for taking minutes of this meeting. This meeting can be held at either the Contractor's or Government's location, as appropriate.

2A.2.2 Ad hoc Technical / Work Status

The contractor shall, if requested by the Government, participate in monthly status meetings or ad hoc technical meetings at a mutually agreeable time and place to discuss tasking, work progress, technical problems, performance issues, or other technical matters. During these meetings the contractor shall at least provide accomplishments, problems and issues, and planned actions. The contractor shall take minutes of these meetings and include them in the Monthly Status Report. These meetings will occur at a time and place mutually agreed upon by the parties.

2A.2.3 Contract Administration Meetings

The CO may require the authorized contractor representative to meet or participate in a teleconference with authorized Government personnel as often as deemed necessary to discuss performance or administrative issues. The contractor may also request a meeting with the CO when deemed necessary. The content of meetings shall be documented in writing, as agreed between the parties. Minutes shall be approved by both parties and shall be included in the Government contract file.

2A.3 Program / Project Management Requirements

2A.3.1 General Program / Project Management Requirements

The contractor shall be solely responsible for managing the work performed in the execution of the contract/order. This includes the responsibility to:

- Assign appropriate resources to each task.
- Maintain clear organizational lines of authority.
- Use SAFe Agile methodologies (Refer to https://www.scaledagileframework.com/) and IAE Jira and Confluence to ensure effective task management and administration, following the requirements set forth in the PWS.
- Maintain the personnel, organization, and administrative control necessary to ensure that the work delivered meets the specification requirements.
- Establish and use proven policies, processes, analyses, and best practices.
- The contractor shall be fully responsible for management, control, and performance of any subcontractor used in support of the contract/order. Use of a subcontractor on the contractor's team shall not relieve the prime contractor of responsibility nor accountability in the execution of the contract/order

Additionally, the contractor shall:

- Bring problems or potential problems affecting performance to the attention of the CO as soon as possible.
- Notify the COR, CO, and other identified Government representatives immediately of any projected, anticipated, or known delays that may impede contactor performance.
- When requested, deliver written reports to the CO to memorialize all verbal reports.
- Provide, in writing, the results of all meetings in which proposals are put forth that have the potential for affecting and/or changing contract agreements, requirements or conditions, and these shall be brought to the attention of the CO.

2A.3.2 Phase-In Support

The contractor shall provide phase-in support in accordance with the phase-in plan as required per PWS paragraph 4.5.9

2A.3.3 Phase-Out Support

The contractor shall provide phase-out support in accordance with the phase-out plan as required per PWS paragraph 4.5.10

2A.4 Subcontract Management

The Contractor shall be fully responsible for management, control, and performance of any Subcontractor used on this contract. If a Subcontractor is being used, the Prime Contractor must inform the Government. Use of a Subcontractor on the Contractor's team shall not relieve the Prime Contractor of responsibility nor accountability in the execution of this contract/order.

2B Business and Technical Objectives

2B.1 Business Objectives

2B.1.1 Operations and Maintenance

2B.1.1.1 Operate and maintain the legacy FPDS applications independent of where the application is hosted in AWS cloud

Contractor shall provide Agile project management support for FPDS. Contractor shall coordinate directly with GSA's IAE Program Manager and Program Management Office (IAE PMO) to report status, issues, and the resolution of issues on a weekly basis. As needed, Contractor shall provide input to the IAE PMO to support responses to inquiries from leadership and oversight agencies, including the Acquisition Committee for E-Government (ACE), Office of Management and Budget (OMB), Congress, and the Government Accountability Office (GAO).

During O&M, the contractor is required to provide the system update (service packs) to align the system with the procurement policy changes and minor system enhancements; apply the data management as needed. The service pack is usually once every quarter, 4 times a fiscal year.

For tasks that involve other contractors, Contractor shall establish the requirements or quality standards necessary, shall oversee the schedule of deliverables, assist with functional support as needed, and verify that deliverables meet requirements and quality standards. Contractor is responsible to support all current up and downstream interfaces. Contractor shall closely monitor the cloud infrastructure costs and implement remediation to keep costs under control. Contractor shall report to the IAE PMO, indicating any areas of concern in the weekly report, and integrate the information into the overall end-to-end performance status.

2B.1.1.2 Operate and maintain all aspects of the SAM Integration Environment hosted in the AWS cloud

Contractor shall provide Agile project management support for the SAM Integration Environment. Contractor shall coordinate directly with GSA's IAE Program Manager and Program Management Office (IAE PMO) to report status, issues, and the resolution of issues on a weekly basis. As needed, Contractor shall provide input to the IAE PMO to support responses to inquiries from leadership and oversight agencies, including the Acquisition Committee for E-Government (ACE), Office of Management and Budget (OMB), Congress, and the Government Accountability Office (GAO). All releases need to be lined up with beta.sam.gov releases once integrated.

For tasks that involve other contractors, Contractor shall establish the requirements or quality standards necessary, shall oversee the schedule of deliverables, assist with functional support as needed, and verify that deliverables meet requirements and quality standards. Contractor is responsible to support all current up and downstream interfaces. Contractor shall closely monitor the cloud infrastructure costs and implement remediation to keep costs under control. Contractor shall report to the IAE PMO, indicating any areas of concern in the weekly report, and integrate the information into the overall end-to-end performance status. The support needed for troubleshooting any functional/technical/performance related issues need to collaborate with beta.sam.gov teams.

2B.1.2 Operate and maintain the Entity/Award data to support the Reporting/Search functionality in the modernized Beta.SAM.gov

Contractor shall operate and maintain the Entity/Award data and provide the Entity/Award data as applicable to IAE modernized system for the data desimission through Contract Data reports, Search, APIs, Data Extracts, etc. Contractor shall coordinate with the IAE modernization teams and platform team (FCS) for any delay of data synchronization. When the above said has an issue, Contractor shall provide the support on the analysis or troubleshooting. Contractor shall take proper actions, such as Data Management, to correct the Award data issues.

2B.1.3 Help Desk Support

The Contractor is responsible for the escalated Tier 2 issues received from the Federal Service Desk (FSD), also referred to as the 'Help Desk'. The desired outcome is for users to have prompt access to qualified, knowledgeable IT Help Desk support during business hours (8am-6pm) and to use the Help Desk to resolve all technical and functional questions and problems.

For policy related questions, or for issues that require Government intervention (such as the deletion of Government-owned reports), the Contractor shall escalate them to the appropriate Tier 3 IAE Government Representative. The Tier 2 help desk provider is required to accept and respond to help desk issues/requests that could not be resolved by the FSD.

2B.1.4 Support retiring the legacy FPDS applications

When IAE is working on retiring the legacy FPDS applications, Contractor shall provide the adequate support when required by the Authorized Government representatives. Coordination and collaboration are critical during the process of retiring the FPDS system. Contract shall plan the work with Jira, share the schedule with IAE modernization team for a smooth FPDS decommission.

2B.1.5 Maintain Integration code between Legacy SAM and Beta SAM

The contractor will maintain the integration code between Legacy SAM and Beta SAM for SAM and FPDS.

3. QUALITY

Both the Contractor and the Government have responsibilities for providing and ensuring quality services, respectively.

3.1 Contractor Quality Control Plan (QCP)

The Contractor shall be responsible for quality assurance and quality control of all services performed and all items delivered under this contract/order.

The Contractor shall prepare and maintain a Quality Control Plan (QCP) as a guide for implementing quality assurance and quality control procedures. The Contractor shall submit the QCP to the Government for information and acceptance. The Government has the right to require revision of the Contractor's QCP should its implementation fail to control the quality of items and/or services delivered under this contract/order.

The QCP shall include an explanation of the processes and procedures for ensuring satisfactory performance and delivery of quality items and/or services. Additionally, as a minimum, the QCP shall include the following items.

- A description of the inspection system to cover all major services and deliverables. The description shall include specifics as to the areas to be inspected on both a scheduled and unscheduled basis, frequency of inspections, and the title of inspectors.
- A description of the methods to be used for identifying and preventing defects and deficiencies in the quality of service performed.
- A description of the records to be kept to document inspections and corrective or preventive actions taken.

All records of inspections performed shall be retained and made available to the Government upon request throughout the task order performance period, and for the period after task order completion, until final settlement of any claims under this task order.

The Contractor shall implement a quality program based on its QCP. In compliance with the QCP, the Contractor shall manage, surveil, assess, improve and/or correct contract performance to ensure the quality of the services and deliverable products, as a minimum, meet the level of quality required by the Government Functional Managers or Technical Representatives.

In the event of quality concerns, identified by the Government, the Contractor shall immediately take corrective action in response to Government required changes to the QCP.

The QCP shall be delivered to the Government as stipulated in the Delivery Schedule, see Paragraph 4.5.2 of this PWS, below.

3.2 Performance Based Requirements - Service Level Agreement (SLA)

This contract / order includes a Service Level Agreement (SLA)(PWS Attachment C). The SLA augments the QASP (Quality Assurance Surveillance Plan) by providing performance targets and acceptable levels of product or service quality for specific deliverables that are more detailed than the performance expectations described in the QASP. In addition to defining Acceptable Quality Levels (AQLs), the elements of the SLA provide the basis for determining Incentives and Disincentives in conjunctions with the evaluation of contractor performance.

3.3 Government Quality Assurance Surveillance Plan (QASP)

The Government will periodically evaluate Contractor performance under this contract / order in accordance with the attached Quality Assurance Surveillance Plan (QASP). The purpose of this evaluation is to ensure that Contractor performance meets Government requirements. The Government reserves the unilateral right to change the QASP at any time during contract performance provided the changes are communicated to the Contractor by the effective date of the change. The QASP along with the included “Surveillance Objectives, Measures, and Expectations” describes the evaluation procedures, PWS items to be evaluated, and the measures against which performance will be evaluated. The Government reserves the right to review services to be provided, including those developed or performed at the contractor's facilities, to determine

conformity with performance and technical requirements as prescribed in the applicable inspection clause (see Paragraph 9.14, below). The evaluation results will be documented in the Contractor's CPARS (Contractor Performance Assessment Reporting System) report. The QASP is provided as an attachment to this PWS.

4. DELIVERABLES

4.1 Contractor Submission

Deliverables are to be transmitted with a cover letter on the prime contractor's letterhead. Each deliverable shall include an introductory summary describing the contents. Deliverables shall be provided electronically through GSA's web-based procurement system, as required, and to any other destination(s) as required per the Government's request. The contractor shall provide hard copy deliverables as required per the Government's request. All deliverables shall be produced using software tools/versions as approved by the Government.

This project will be accomplished using Agile methodologies, and as such, specific deliverables, not identified here, will be identified in each sprint. Written deliverables must be concise and clearly written, using plain language guidelines. The Contractor must ensure the accuracy, functionality, completeness, professional quality, and overall compliance with Government guidelines and requirements of all deliverables.

All deliverables developed are the property of the Government and must not be used by the Contractor for any other purpose. All project-related information or documentation, with no exceptions, must be treated as confidential and proprietary during and after the completion of this effort and submitted to the project lead. Additional supplemental restrictions or qualifications or acceptance criteria may be provided at each sprint.

4.2 Government Review

Government personnel will have 10 business days to review deliverables (to include resubmissions) and provide written acceptance/rejection. Authorized Government representatives will notify the contractor of deliverable acceptance or provide comments in writing. The contractor shall incorporate Government comments, or provide rationale for not doing so within 5 business days of receipt of comments. Government acceptance of the final deliverable will be based on resolution of Government comments or acceptance of rationale for non-inclusion. Additional changes volunteered by the contractor will be considered a resubmission of the deliverable.

4.3 Government Delays in Reviewing Deliverables or Furnishing Items

If contractor performance or submission of deliverables is contingent upon receipt of Government furnished items (data, equipment, materials, facilities, and support) or input, or upon Government review and approval of interim items or draft documents (collectively referred to as Government Performance), the Government shall specify, if not already specified within this PWS, when it will provide such items or input, or the time it will need to perform reviews or give approvals. If the Government fails to meet item, input, review, or approval deadlines, contractor performance or submission of deliverables shall automatically be extended one business day for each day of government delay. The contractor shall promptly advise the Contracting Officer of any delays in receipt of Government furnished items, input, reviews, or approvals.

4.4 Deliverable Table

The contractor shall perform or deliver the items listed in the following table on the dates and to the locations specified.

PWS Ref.	Event or Item Title	Delivery Time	Delivery Place
	Project Start	Date of Award	
Sec 4, 8, 10	Contractor Employee Non-disclosure Agreement (one for each employee assigned to work on this order	After award but prior to commencement of performance by each Contractor or Subcontractor employee	Electronically to the GSA ITSS System & email to the IAE COR
Sec 2A.2	Kick-off Meeting	within 5 business days after award or as agreed by the parties	
Sec 2A.2	Kick-off Meeting Minutes	within 5 business days after the kick-off meeting	Electronically to the GSA ITSS System & email to the COR
Section 3	Quality Control Plan-Draft	10 Business Days after award.	Electronically to the GSA ITSS System & email to the COR
Section 3	Quality Control Plan-Final	30 Business Days after Government review. (The Government shall review and provide comments within 7 business days after receipt of the draft QCP.)	Electronically to the GSA ITSS System & email to the COR
Section 4, Section 2B	Deliverables on each Agile sprint	The last day of the Agile Sprint for the committed deliverables	GSA's web-based procurement system
Section 4	Staff Matrix A complete and current list of Contractor employees and the task/office/function they are supporting	Furnished at the kick-off meeting with an update furnished on or before the date of any personnel change.	Electronically to the GSA ITSS System & email to the COR
Section 4	Funds and Man-Hour Expenditure Report	NLT 10 business days after the end of the reporting period.	Electronically to the GSA ITSS System & email to the COR
Section 4	Monthly Status Report – Final	NLT 10 business days after the end of the reporting period.	Electronically to the GSA ITSS System & email to the COR

Section 4	Technical Reports / Studies - Draft	As required by Technical Directive.	Electronically to the GSA ITSS System & email to the COR
Section 4	Technical Reports / Studies - Final	10 Business Days after Government review. (The Government shall review and provide comments within 7 business days after receipt of the draft report/study.)	Electronically to the GSA ITSS System & email to the COR
Section 8	Vulnerability Scanning	NLT 10th day of each quarter	Electronically to the GSA ITSS System & email to the COR
Section 8	Plan of Action & Milestones Update	NLT 10th day of each quarter	Electronically to the GSA ITSS System & email to the COR
Section 8	System Security Plan	NLT 10 business days after the new option year starts	Electronically to the GSA ITSS System & email to the COR
Section 8	Incident report	NLT 3 business days after the incident happens	Electronically to the GSA ITSS System & email to the COR
Section 8	Contingency Plan	NLT 10 business days after the new option year starts	Electronically to the GSA ITSS System & email to the COR
Section 8	System(s) Baseline Configuration Standard Document	90 Business Days after award	Electronically to the GSA ITSS System & email to the COR
Section 8	System Configuration Settings Compliance scan report	NLT 10th day of each quarter	Electronically to the GSA ITSS System & email to the COR

4.5 Data Requirements / Descriptions

Documentation provided in response to the objectives will be in the Government's template format. If no format is prescribed, documents may be in the Contractor's preferred format using standard Microsoft Office products.

The content of all data items, if not self-explanatory from the template format, shall be agreed upon between the parties.

4.5.1 Contractor Employee Non-Disclosure Agreement

The Contractor shall furnish a signed "Contractor Employee Non-Disclosure Agreement" for each Contractor and Subcontractor employee assigned to work under this contract / order, prior to their starting work.

4.5.2 Kick-off Meeting Minutes

The Contractor shall take minutes of the kick-off meeting which shall capture the names of the attendees, the key points of the discussion, questions raised and answered, and action items.

4.5.3 Quality Control Plan

The Contractor shall deliver a QCP as defined in Paragraph 3.1, above.

4.5.4 Staff Matrix

The Contractor shall furnish a complete and current list of Contractor and Subcontractor employees who are assigned to work under this contract / order. The matrix shall include the staffing chart showing the name of each employee, his or her position in the staffing plan, job title, and the Government's task/office/function they are supporting. The lines of authority and responsibility of each staff member shall also be made clear to the Government. The matrix shall be updated with each change in personnel, job title, position in the staffing plan, or assignment of area of responsibility.

4.5.5 Funds and Expenditure Report

The contractor shall provide a Funds and Expenditure Report that provides the current task order accounting information indicated below in support of the monthly invoice. The Contractor can determine the format of the report provided it includes, at a minimum, the following information:

- Expenditures for labor, material, travel, and any other charges.
- Matrix of Actual hours expended vs. planned and/or funded hours, and an explanation of significant variances between planned and expended hours. The report shall include amounts for the current monthly reporting period and the cumulative actual vs. planned hours and amounts for the entire contract/order up to the report date.
- Burn rates for the current period and the cumulative amount for the entire contract/order up to the report date. The information shall be presented in numerical and chart format for each CLIN
- Crosswalk of costs incurred for work performed to amounts billed.
- Current and cumulative task funding status (direct labor, travel, and other direct cost funding status to be reported separately, if required).

Charges shall not exceed the authorized cost limits established for labor and support Items. The government will not pay any unauthorized charges. Original or copies of receipts, travel vouchers, etc. shall be maintained by the contractor to support charges other than labor hours and made available to government auditors upon request. Travel documents shall be furnished in accordance with government Travel Regulations

4.5.6 Monthly Status Report (MSR) (alternate)

The contractor shall provide a MSR that briefly summarizes, by task, the management and technical work conducted during the month. The contractor shall provide the following information, plus any other information that the contractor determines to be germane to the tasks.

- Status of tasks, schedules, deliverables. Status of tasks shall include a summary description and updated milestone schedule noting changes, issues and/or variances, concerning --
  - all tasks completed and deliverables made during the reporting period,
  - all tasks currently on-going during the reporting period, and

  - all known tasks assigned for future reporting periods.
- Staffing (if a separate staffing matrix is not a required deliverable)
- Status of funding and expenditures (if a separate Funds and Expenditure Report is not a required deliverable)
- Problems or issues and proposed resolutions
- Government action requested or required

4.5.7 Technical Reports

Content and format of technical reports shall be agreed upon between the parties.

4.5.8 Trip Reports

Not applicable

4.5.9 Phase-In Plan

The contractor may or may not propose a transition period, for a duration to be determined and proposed by the contractor, but shall not exceed a period of 30 calendar days. The transition period is defined as the period of time (during the phase-in) when the new contractor and the incumbent contractor will both be providing support to the client as required to support the transition to the newly awarded contract/order. If the contractor chooses to propose a transition period, such period shall be included and addressed within the below identified phase-in plan.

The contractor shall develop a phase-in plan. Such phase-in plan shall present a clear understanding of the phase-in tasks required, the issues likely to result from non-incumbent contractor performance, and the contractor's proposal to resolve such issues. The phase-in plan shall include a clear and feasible strategy for delivering services required within the periods specified by the plan and shall include a detailed plan-of-action and milestones to transition the functions identified in this PWS in a well-planned, orderly, and efficient manner. The phase-in plan shall include, at a minimum:

- Staffing plan.
- Development and submission of required deliverables.
- Interface with the Government and incumbent contractor (if applicable) during phase-in, to include meetings or status reports, as required.
- Approach to maintaining quality and minimizing disruption during phase-in.
- Development and dissemination of operating instructions, procedures, and control directives.

4.5.10 Phase-Out Plan

The FPDS system is going to be decommissioned and replaced by the modernized functionalities from the IAE's new Sam.gov system. During phase-out of the contract/order, which is determined to be a period of 30 calendar days prior to the lifecycle end date of the contract/order, a smooth and orderly close-out is necessary to ensure a minimum disruption to vital Government business. The contractor shall cooperate to the extent required to permit an orderly changeover

to the successor contractor from IAE modernization system team(s). The phase-out will be deemed completed by the COR and/or other identified Government representatives when it is determined by the Government that the transition of property, data, and information developed as a part of the contract/order have been successfully changed over from the outgoing contractor to the Government and the successor contractor as required.

For SAM Integration Environment O&M support, when Phase-Out period arrives,the contractor will abide by the phase-out activities listed below.

Phase-out activities include, but are not limited to, the tasks below.

- Submission of official comprehensive phase-out plan.
- Daily communication of staffing status (i.e. projection of when incumbent contractor employees will off-board from the incumbent contract/order and identification of additional incumbent resources, such as a transition team, that may be needed to support the transition efforts) and overall phase out status, in accordance with the accepted phase-out plan.
- Maintain the phase out schedule included within the phase-out plan.
- Transition of property.
- Transition of supporting documentation.
- Transition of accounts (e.g. user accounts and user access).
- Knowledge transfer on the stored system code, or established installation, operation, and maintenance procedures of the technologies supported. The phase out plan shall clearly describe the proposed methodologies to be utilized for such transfer (e.g., written documentation, manuals, formal classroom type training, one-on-one training sessions, etc.).
- Transition of any license keys, numbers or documentation of maintenance agreements for all software utilized for the operations of this system.
- Execution and submission of phase out checklist, to include Government acceptance.

4.5.11 Monthly Invoice

The contractor shall provide a monthly invoice, no later than the 10th calendar day of the month following the monthly reporting period, to be submitted simultaneously with the MSR. As applicable, the invoice shall include but is not limited to:

- Clear identification of all costs.
- Labor hours expended (for labor hours tasks). The labor hours expenditure information shall include the identification of the employee name, labor category, hourly labor rate, and total number of labor hours expended.
- Timecards. As required, the contractor shall provide a copy of each employee's timecard/sheet. The timesheet shall identify the contractor employee name and number of hours claimed per day.
- Travel costs.
- Supporting documentation for travel costs. Refer to PWS 5.3 for specific requirements.
- Other Direct Costs.
- Supporting documentation for other direct costs. Refer to PWS 9.6 for specific requirements.

As required, the contractor shall comply with line item (i.e., per individual positions, different programs, program areas, etc.) invoicing requests

4.5.12 Other Reports

Content of other reports is self-explanatory or should be agreed upon between the parties.

5. PERFORMANCE PLACE, TIME, AND RESTRICTIONS

5.1 Period of Performance

The anticipated period of performance(s) is/are identified below.

- Base Period: Initial 12 months from date of award
- Option Period 1: 12 months following the Base Period
- Option Period 2: 12 months following Option Period 1
- Option Period 3: 6 months following Option Period 2
- Option Period 4: 6 months following Option Period 3

5.2 Place of Performance

5.2.1 Performance at the Contractor's Facility

Work is expected to be performed primarily at the contractor's facilities. Work performed at contractor facilities shall be performed according to the contractor's standard commercial practice; however, the contractor representatives at these facilities must be available for interaction with Government employees during the core hours identified in the paragraph entitled "Time of Performance - Normal Hours", below, with the exception of Government designated holidays or facility closures.

5.2.2 Performance at the Government's Facility

The Contractor may be required to perform work at both central and regional GSA offices to attend meetings, enable the Contractor to work with GSA to understand the business needs in order to effectively use Agile principles in the continuous delivery of functionality, conduct training sessions, troubleshoot, etc. If travel is required, it will be reimbursed subject to the terms and conditions of the underlying BPA/GSA Schedule contract.

5.2.3 Applicability of Telework

All work performed at locations other than those identified as Government and/or contractor facilities shall be approved prior to performing the work. Federal contractors are not governed by Office of Personnel Management (OPM), GSA, or the individual agency policies; however, this does not prohibit contractor personnel from actually working at an alternate site, when/as appropriate and specifically authorized by the Government. The contractor shall develop telework policies to comply with the following requirements and address such requirements at a generic level within their QMP. Alternate work arrangements for contractors shall be negotiated with the contractor's own employer and the appropriate agency official, to ensure policies and procedures are in close alignment and there is a clear and concise arrangement documenting the agreement. It remains the

contractor's responsibility to ensure the services are performed in accordance with the terms and conditions of the contract/order.

The contractor shall address the pertinent facts impacting performance and ensure all affected contractor resumes and other related documentation reflects the applicable work site. The contractor shall provide justification to the Government when identifying and submitting an individual as a telecommuter and address implementation processes and procedures within the QMP. The contractor shall be responsible for ensuring the Government has the required access/details necessary for the Government to perform quality assurance responsibilities.

The contractor shall comply with all agency security telework policies. The contractor shall ensure all services provided from an alternate site comply with the Federal Information Security Management Act of 2002 (FISMA) and address the following, as a minimum:

- Controlling access to agency information and information systems;
- Protecting agency information (including personally identifiable information) and information systems;
- Limiting the introduction of vulnerabilities;
- Protecting information systems not under the control of the agency that are used for teleworking;
- Safeguarding wireless and other telecommunications capabilities that are used for teleworking; and
- Preventing inappropriate use of official time or resources that violates subpart G of the Standards of Ethical Conduct for Employees of the Executive Branch by viewing, downloading, or exchanging pornography, including child pornography.

5.2.4 Unplanned Government Facility Closures

In the event of unplanned closure of the Government facility for any reason (e.g. natural disasters, Government shut-down, or severe weather) the Contractor shall make its best effort to mitigate loss of work time. If Contractor employees are working on the Government facility, this may be done by moving employees to an off-site location. If performance under this contract/order is not possible, the Contractor shall take steps to assign employees to other projects on a temporary basis or place them in leave status to minimize non-productive costs to the Government under this contract/order. Additional instructions may be provided by the Contracting Officer on a case-by-case basis. Disagreements between the parties resulting from closures shall be settled through negotiations to the maximum extent possible or shall otherwise be settled pursuant to the provisions of the Disputes provisions of this contract/order.

All services to be performed under this contract/order have been determined to be non-essential for performance during a closure. Should the Government facility be closed, the Contractor shall be notified by either the Contracting Officer, COR, or a local television or radio station. The Contractor is responsible for notifying its employees about Government closures. Contractor employees are not to report to the Government facility if it is closed and will adhere to delays, unless otherwise specifically instructed otherwise by the CO or COR.

5.3 Time of Performance - Hours of Work

5.3.1 Normal Hours

For any Contractor employees working on Government facilities, their normal business day must include core duty hours between 9 AM through 3 PM local time, Monday through Friday, excluding holidays, to coordinate with Government operations. Actual start and end times shall be at the contractor's discretion. The Contactor shall be responsible for managing the work hours of its employees who work at Contractor facilities, provided that those employees are available when necessary to interact with Government employees.

Any Contractor employee working at Government facilities shall observe federal holidays and government closures on the same dates and during the same times as the Government personnel, since Contractor employees shall not have access to the Government facilities during these days and/or times. These holidays are as follows.

5.3.2 Holidays

The Government shall observe the following holidays.

New Year's Day	Labor Day
Martin Luther King Jr., Day	Columbus Day
Presidents' Day	Veteran's Day
Memorial Day	Thanksgiving Day
Independence Day	Christmas Day

5.3.3 Expedited Performance

In the event that individual tasks or subtasks require expedited performance or extended workdays to meet schedule constraints or work volume, the Government shall communicate that need to the Contractor's Project Manager or Team Lead who, in turn, is responsible for managing the Contractor's labor resources to meet the schedule constraints. Communications regarding expedited performance shall be documented in writing, by email or otherwise, and included in the contract administration file. If Contractor employees are working at Government facilities and task completion deadlines require extended hours, the Government will provide authorization to occupy and use Government facilities beyond normal duty hours.

5.4 Travel

Not applicable.

5.5 Limitations on Contractor Performance

In compliance with FAR 37.102(c), this task order does not require the contractor to perform any inherently governmental functions. Accordingly, the contractor shall NOT perform any of the inherently governmental functions listed in FAR 7.503. Those inherently governmental functions most applicable to this procurement action are as follows:

- Determine Government policy. [7.503(c)(5)]
- Determine Federal program priorities. [7.503(c)(6)]

- Direct or control Federal employees; [7.503(c)(7)]
- Determine acquisition, disposition, or disposal of Government property; [7.503(c)(11)]
- Determining what supplies or services are to be acquired by the Government [7.503(c)(12)(i)]
- Vote on a source selection board; [7.503(c)(12)(ii)]
- Approve any contractual document on behalf of the Government; [7.503(c)(12)(iii)]
- Award Government contracts; [7.503(c)(12)(iv)]
- Administer Government contracts; [7.503(c)(12)(v)]
- Accept or reject supplies or services; [7.503(c)(12)(v)]
- Terminate Government contracts; [7.503(c)(12)(vi)]
- Determine cost reasonableness, allowability, or allocability; [7.503(c)(12)(vii)]
- Participating as a voting member on performance evaluation boards; [7.503(c)(12)(viii)]
- Determine budget policy, guidance, and strategy [7.503(c)(16)]

6. PERSONNEL

6.1 General Requirements

%%%

NOTE: The Government, at its sole discretion, may consider substitutions and/or requests for deviation from any of the following personnel qualifications (e.g., experience in lieu of education), if to do so would be in the best interest of the Government.

%%%

All contractor personnel shall meet the minimum general requirements listed below.

- All personnel shall be capable of working independently.
- All personnel shall have training and experience that is appropriate for the tasks to which they will be assigned.
- The contractor shall provide personnel that are capable of conducting themselves in a professional manner and have proper telephone and e-mail etiquette, customer service techniques, and organizational skills.
- Contractor personnel performing in a leadership capacity shall be capable of directing contractor personnel and interfacing with the Government and customers.
- Ability to communicate applicable technical subject matter expertise to management and others.
- Strong written and oral communication skills in the English language. All contractor personnel must be able to read, write, speak and understand English.
- Exceptional customer service skills.
- Strong time-management and prioritization skills.
- If applicable, all personnel shall meet the minimum requirements set for in the Federal Supply Schedule (FSS) contract or Government-wide Acquisition Contract (GWAC) upon which this task order is based.

The Contractor shall furnish adequate documentation to substantiate compliance with this

requirement for each assigned staff member. The Contractor shall certify as to the accuracy and completeness of the supporting documentation.

6.2 Specific Expertise and Experience

The contractor shall provide personnel with the appropriate skill levels. While each individual contractor employee may not possess expertise and experience in each area of performance, the Government requires that the overall contractor staff possess the aggregate skills, expertise, and experience to successfully complete all requirements.

6.3 Training

6.3.1 Contractor Staff Training

The contractor shall provide fully trained and experienced staff. Contractor personnel are required to possess the skills necessary to support the minimum requirements of the labor category under which they are performing. Training of contractor personnel shall be performed at the contractor's expense, except when the Government changes the requirements during performance of an on-going task and it is determined to be in the best interest of the Government. This will be negotiated on a case-by-case basis. Training at Government expense will not be authorized for replacement personnel or for the purpose of keeping contractor personnel abreast of advances in the state-of-the-art, or for training contractor personnel on equipment, computer languages, and computer operating systems that are available in the commercial market.

NOTE: Unless Contractor employee training is specifically identified and authorized by the Government, in writing, the Contractor shall not bill the Government for employee time spent in training or for any costs related to or associated with Contractor employee acquired training. This applies to training of any type or for any purpose, including training that is either necessary for job or employment eligibility or a prerequisite to performance of work under this contract/order, whether general in nature or specialized and unique to this requirement.

6.3.2 Mandatory Government Training

During the course of this contract / order the Government may require Contractor employees to receive specialized training in areas necessary to allow the Contractor to fulfill the requirements of this contract / order (e.g., LAN Information Assurance Training, Government unique software or software tools, Security Training). In such cases Government mandated training shall be considered part of this contract and charged against the task(s) to which the individual Contractor employee is assigned.

Mandatory Government training shall be tracked and monitored by the contractor. All required courses must be completed by the required dates by all contractor personnel. Mandatory Government training classes may be completed during work hours. It is the intent of the Government to provide 30 calendar days written notice of annual training requirements to the designated contractor representative. The designated contractor representative will be responsible for notifying subordinate contractor personnel. Failure of Contractor employees to take mandatory Government training may impair the Contractor’s ability to perform but

will not excuse the Contractor from performing.

6.4 Key Positions / Key Personnel

6.4.1 Definition & List of Key Personnel

Key Personnel are defined as those individuals who are so essential to the work being performed that the contractor shall not divert them to other projects or replace them without receiving prior approval from the Contracting Officer. This includes substitution of those originally proposed at the time of contract/task order award*. Substituted personnel must have equal or better qualifications than the person they replace, subject to the Government's discretion.

The following Contractor personnel have been initially identified by the Government as "Key Personnel" under this contract / order.**

Project Manager

- An active PMI Project Management Professional (PMP®), PMI Program Management Professional (PgMP®) Certification, or a Bachelor, or Master degree from an accredited institution in Project Management, at the time of proposal submission
- Formal training or certification in Agile software development methods
- Demonstrated experience in the management, design, implementation, and maintenance of Services similar to the requirements of the PWS
- Demonstrated experience in managing in a continuous integration and DevOps environment.
- Demonstrated experience with the management, manpower utilization, and supervision of employees (including subcontractors) of various labor categories and skills in projects similar to the requirements of the PWS. Specifically, managing teams that will coordinate with the Government and work with other contractors to support an Agile environment with a small team of developers; managing O&M of operational systems with more than a quarter million users with one million visitors per month; managing the O&M efficiency, data quality, , service delivery and the technical support (Tier 2) to the Help Desk.
- Demonstrated ability to orchestrate the management of technology scope and risks.
- Demonstrated written and verbal communication skills, including experience in presenting material to senior Government officials.

Scrum Master

- Formal training or certification in Agile software development methods at the time of proposal submission.
- Demonstrated experience working with Agile, and/or Continuous Delivery approaches and best practices, especially those that support scaling Agile to an enterprise such as the Scaled Agile Framework (SAFe)
- Demonstrated experience in using an Agile development framework including task estimation, test automation, deployment automation and Continuous Integration to improve overall Agile activity execution and product quality.
- Demonstrated experience ensuring that the technical expectations of deliverables are met through Agile processes; additionally, support the

continuous improvement of those processes
- Demonstrated experience delivering agile software solutions using best practices such as Test-Driven Development (TDD) or Adaptable Software Design.

Technical Lead

- Minimum of 5 years experience in agile software development to include Microservices architecture using open source Java technology.
- Minimum of 3 years experience with designing and developing complex software systems on a virtualized cloud environment such as Amazon AWS.
- Formal training such as a Bachelor of Science degree in Computer Science preferred
- Minimum of 2 years experience developing and deploying microservices in a cloud environment preferred.
- Minimum of 3 years experience in DevOps and CI/CD concept using tools such as Jenkins, GitHub, Docker/Kubernetes, and testing tools such SonarQube, JMeter.
- Demonstrated experience delivering Agile software solutions using best practices such as Test-Driven Development (TDD) or Adaptable Software Design
- AWS Certified Solutions Architect

**Note: Failure of the Contractor to furnish proposed key personnel shall be viewed as a breach of contract and may be grounds for a default determination by the Government.*

***Note: Should the Contractor propose additional key personnel this provision will be modified to include those additional personnel.*

6.4.2 Key Personnel Substitution

The Contractor shall not remove or replace any personnel designated as key personnel without making a written request to and receiving written concurrence from the Contracting Officer. The Contractor's request for a change to key personnel shall be made no later than ten (10) calendar days in advance of any proposed substitution and shall include a justification for the change. The request shall (1) indicate the labor category or labor categories affected by the proposed change, (2) include resume(s) of the proposed substitute in sufficient detail to allow the Government to assess their qualifications and experience, and (3) include a statement addressing the impact of the change on the Contractor performance. Requests for substitution will not be unreasonably withheld by the Government. The Government will approve initial contactor key personnel at time of award. Replacement key personnel will be approved via modification to the contract/task order. If the Government CO and the COR determine that the proposed substitution, or non-employee initiated removal of personnel without substitution or replacement, is unacceptable or would impair the successful performance of the work, the Contracting Officer will request corrective action. Should the Contractor fail to take necessary and timely corrective action, the Government may exercise its rights under the Disputes provisions of this contract or take other action as authorized under the provisions of this task order, the Prime contract upon which this order is based, or pursue other legal remedies allowable by law.

6.5 Personnel Retention and Recruitment

The contractor shall make every effort to retain personnel in order to ensure continuity until contract/order completion. If it should become necessary to substitute or replace personnel, the contractor shall immediately notify the COR and/or other identified Government representatives in writing of any potential vacancies and shall submit the resume(s) of replacement personnel within 5 calendar days of the notification. Additionally, for all new positions identified by the Government, the contractor shall submit the resume(s) of proposed personnel within 5 business days of the Government's initial request. The contractor shall submit the resume(s) of all potential personnel selected to perform under the contract/order to the COR and/or other identified Government representatives through GSA's web-based procurement system, or any other process means identified/required, for Government review and acceptance/rejection. Upon Government acceptance of a personnel resume(s), the candidate shall be available to begin performance within 14 business days. The contractor shall ensure continuity of operations during periods of personnel turnover and long-term absences. Long-term absences are considered those longer than one week in duration.

6.6 Non-Key Personnel Substitutions

Although Government approval is not required prior to replacing any of its non-key personnel staff, the Contractor shall provide resumes or other adequate documentation to verify to the Government that all proposed replacements (temporary or permanent) meet the security and minimum educational and experience requirements of this contract/order. Additionally, the Government requests the courtesy of being immediately informed of any potential vacancy or prior to any staff member being removed, rotated, re-assigned, diverted or replaced.

6.7 Staff Maintenance

The contractor shall make every effort to retain personnel in order to ensure work continuity until contract/order completion. During any periods of turnover or temporary absence of personnel, the Contractor shall ensure continuity of operations and make every effort to maintain manning without loss of service days to the Government. This may necessitate the use of temporarily assigned employees to fill short term gaps between permanently assigned employees or prolonged (more than one week) absences of current employees.

The Contractor is required to use and/or replace all personnel with those who meet the minimum qualifications as stipulated above, in this section of the PWS and should strive to replace departing personnel with those having appropriate and/or equal qualifications. Failure on the part of the Contractor to employ an adequate number of qualified personnel to perform this work will not excuse the Contractor from failure to perform required tasks within the cost, performance, and delivery parameters of this contract / order.

6.8 Contractor Employee Work Credentials.

Contractors shall ensure their employees and those of their Subcontractors have the proper credentials allowing them to work in the United States. Persons later found to be undocumented or illegal aliens will be remanded to the proper authorities.

7. GOVERNMENT FURNISHED PROPERTY/INFORMATION/ACCESS

7.1 General

The Government shall provide, without cost to the Contractor, the data, facilities, equipment, materials and services listed below. The Government furnished property and services provided as part of the contract/order shall be used only by the contractor and only to perform under this contract/order. No expectation of personal privacy or ownership using any Government electronic information or communication equipment shall be expected. All property at Government work sites, except for contractor personal items, will be assumed to be Government property unless an inventory of contractor property is submitted and approved by the CO/COR. Contractor personal items do not include government owned computers, external drives, software, printers, and/or other office equipment (e.g., chairs, desks, file cabinets). The contractor shall maintain an accurate inventory of Government furnished property.

7.2 Government Furnished items (Property)

7.2.1 Facilities

The Government will provide facilities at the authorized primary work locations as specified in PWS paragraph 5.2. Use of the facilities by contractor personnel will include all utilities, telephone, janitorial services and furniture for contractor personnel performing tasks. The Government will provide the contractor access to buildings as required, subject to the contractor personnel obtaining the required clearances and approvals.

7.2.2 Equipment

The Government will provide the following at authorized on-site Government work locations:

- A suitable work environment (i.e., telephone, office space and furniture). Office space may include a private or shared cubicle, hoteling space (space reserved for temporary use), or other such space suitable for the work required.
- A personal desktop computer or laptop and auxiliary hardware and software required in the performance of the contract/order.
- Network connectivity required to perform work assignments. Network and computer access rights commensurate with work assignments.
- The Government will replace items that are determined to be beyond economical repair by the COR and/or other identified Government representatives unless damage or loss is determined to be due to contractor negligence.

7.2.3 Materials

Not applicable

7.2.4 Data

The Government will provide access to available documents and technical information, as required and upon contractor request, if not available via a hyperlink within this PWS.

The Government will provide documents, reports, database access, data, and other information as available and as required to facilitate accomplishment of work, as stated within this PWS.

The contractor is responsible for obtaining data necessary to perform each task if that data is in the public domain and is not otherwise furnished by the government.

7.3 Use of Government Property

7.3.1 Soft Phones

Government soft phones may be provided as an application on Government provided computers. These are provided for use in conducting official business. Contractor personnel are permitted to make calls that are considered necessary and in the interest of the Government. The contractor shall follow the same policies as Government personnel for telephone usage.

7.3.2 Mobile/Wireless Telephones and Smart Devices

Government issued mobile/wireless telephone and smart devices may be assigned to contractor personnel when the Government determines it is in the Government's best interest. Contractor personnel are prohibited from using any Government issued device for personal use.

7.3.3 Electronic Mail (E-mail)

All Government e-mail access and use by contractor personnel shall be in support of the individual's official duties and contract/order responsibilities. All information that is created, transmitted, received, obtained, or accessed in any way or captured electronically using Government e-mail systems is the property of the Government. Contractor personnel are prohibited from forwarding e-mail generated from a Government provided e-mail account to personal devices.

7.3.4 Copiers and Fax Machines

Copiers are to be used to copy material for official Government business only in the performance of the contract/order. Contractor personnel shall not use fax machines for other than official Government business in the performance of the tasks in the contract/order.

7.3.5 Computer and Internet

All Internet and electronic media access accomplished by contractor personnel (utilizing Government furnished equipment) shall be for official Government business in the performance of the tasks in the contract/order.

7.3.6 Canvassing, Soliciting, or Selling

Contractor personnel shall not engage in private activities for personal gain or any other unauthorized purpose while on Government-owned or leased property, nor may Government time or equipment be utilized for these purposes.

7.3.7 Security Violations Using Government Equipment

Any contractor violating Government security policies, guidelines, procedures, or

requirements while using Government equipment or while accessing the Government network may, without notice, have their computer and network access terminated, be escorted from their work location, and have their physical access to their work location removed at the discretion of the CO/COR. The CO/COR will notify the contractor of the security violation and request immediate removal of the contractor employee.

NOTE: All Government-provided items remain the property of the Government and shall be returned upon completion of the support services. Contractor personnel supporting this requirement shall return all items issued to them when their performance on this contract/task order is ended.

7.4 Validation of Government Furnished Items (GFI) and Equipment Inventory

The Contractor shall develop and maintain a complete GFI inventory that shall be made available to the Government upon request. Within three (3) business days of receipt of any GFI, the contractor shall validate the accuracy of the materials and notify the COR and/or other identified Government representatives, in writing, of any discrepancies, and update the GFI inventory list.

NOTE: Validation shall consist of the contractor checking for physical and logical completeness and accuracy. Physical completeness and accuracy shall be determined when all materials defined as Government furnished are provided. Logical completeness and accuracy shall be determined when all materials defined and associated with a program, system, or work package are provided.

8. SECURITY

8.1 Non-Disclosure Statement.

Due to the potentially sensitive nature of the data and information associated with this requirement, each Contractor employee (including temporary employees) assigned to work under this contract / order shall complete the attached “Contractor Employee Non-Disclosure Agreement”. (PWS Attachment A) A copy of each signed and witnessed Non-Disclosure agreement shall be submitted to the COR prior to performing any work under this contract.

The Contractor shall not release, publish, or disclose sensitive information to unauthorized personnel, and shall protect such information in accordance with provisions of the following laws and any other pertinent laws and regulations governing the confidentiality of sensitive information:

- 18 U.S.C. 641 (Criminal Code: Public Money, Property or Records)
- 18 U.S.C. 1905 (Criminal Code: Disclosure of Confidential Information)
- Public Law 96-511 (Paperwork Reduction Act)

All information that is (1) obtained related to or derived from this contract, and (2) results from or derived from any actual tasks assigned to Contractor employees while participating on this contract is considered proprietary.

8.2 Compliance with Security Requirements

The contractor is required to comply with all security regulations and directives as identified herein and other security requirements as are shown elsewhere in this contract. Please refer to the below referenced Security policy documents.

GSA Information Technology (IT) Security Requirements are included in the below Security Policy Documents

- CIO 09-48, IT Security Procedural Guide: Security and Privacy IT Acquisition Requirements
- CIO 12-2018, IT Policy Requirements Guide
- CIO IT Security 06-30, Managing Enterprise Risk
- DevSecOps OCISO Program [CIO-IT_Security_19-102] [PDF - 806 KB] - 09/13/2019

All data should be encrypted in transmission and at rest.

The Contractor shall be responsible for ensuring all employees supporting this contract comply with all security requirements imposed by the Government Security Officer at all times while in Government facilities and shall follow the instructions of the local organization pertaining to security.

The Federal Information Security Modernization Act (FISMA) of 2014 provides a comprehensive framework for ensuring the effectiveness of information security controls across Federal agencies. FISMA focuses on the program management, implementation, and evaluation aspects of the security of federal information systems. It codifies existing security policies, including Office of Management and Budget (OMB) Circular A-130, Revised, and reiterates security responsibilities provided for in the Computer Security Act of 1987, the Paperwork Reduction Act (PRA) of 1995, and the Clinger-Cohen Act (CCA) of 1996.

In order to protect against cybersecurity threats and manage GSA information systems, the Vendor shall ensure that the contract is compliant with Federal security standards and GSA requirements. The Vendor must provide security and protection for information systems that support the operations and assets of the agency, including the support activities provided or managed by a contractor. Relevant areas that GSA's policies address include:

- Security Requirements
- Cloud information system
- Mobile application
- Privacy Protection
- Controlled Unclassified Information
- Incident Reporting Requirements
- Software License Management
- Telecommunications Policy
- Social Media Policy .

8.2.1 Assessment and Authorization (A&A)

Federal agencies are required by FISMA Law to undergo a security assessment to demonstrate compliance with security requirements. Assessment and

Authorizations (A&A) are required for all new systems. The result of a successful A&A is an Authority to Operate (ATO) Memo. The ATO is required before going into operation and processing the GSA information system. The failure to obtain/maintain the ATO will result in non-compliance and possible shutdown of the system .

8.2.2 GSA Information Technology IT Security Requirements

The contractor shall deliver an IT Security Plan, as required under CIO 09-48, IT Security Procedural Guide within 30 calendar days of award that describes the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this order. The IT Security Plan shall comply with applicable Federal laws including, but not limited to, 40 U.S.C. 11331, the Federal Information Security Management Act (FISMA) of 2002, and the E-Government Act of 2002. The IT Security Plan shall meet IT security requirements in accordance with Federal and GSA policies and procedures, including General Services Administration Acquisition Regulation (GSAR) clause 552.239-71. The contractor shall submit written proof of IT security authorization six months after award, and verify that the IT Security Plan remains valid annually.

8.2.3 Recurring Security Deliverables

Deliverables to be provided to the GSA COR/ISSO/ISSM Quarterly

8.2.3.1. Vulnerability Scanning

Reference: NIST 800-53 control RA-5
Provide the most recent Web Application and Operating System vulnerability scan reports.

8.2.3.2. Plan of Action & Milestones (POA&M) Update

Reference: NIST 800-53 control CA-5
Provide POA&M updates in accordance with requirements and the schedule set forth in GSA CIO IT Security Procedural Guide 09-44, "*Plan of Action and Milestones (POA&M).*"

Deliverables to be provided to the GSA COR/ISSO/ISSM Annually

8.2.4 Updated A&A documentation including the System Security Plan and Contingency Plan

8.2.4.1 System Security Plan

Reference: NIST 800-53 control PL-2
Review and update the System Security Plan annually to ensure the plan is current and accurately describes implemented system controls and reflects changes to the contractor system and its environment of operation. The System Security Plan must be in accordance with NIST 800-18, Revision 1, *"Guide for Developing Security Plans."*

8.2.4.2 Contingency Plan

Reference: NIST 800-53 control CP-2
Provide an annual update to the contingency plan completed in accordance with NIST 800-34, *"Contingency Planning Guide."*

8.2.5. User Certification/Authorization Review Documents

Reference: NIST 800-53 control AC-2
Provide the results of the annual review and validation of system users' accounts to ensure the continued need for system access. The user certification and authorization documents will illustrate the organization establishes, activates, modifies, reviews, disables, and removes information system accounts in accordance with documented account management procedures.

8.2.6 Separation of Duties Matrix

Reference: NIST 800-53 control AC-5
Develop and furnish a separation of duties matrix reflecting proper segregation of duties for IT system maintenance, management, and development processes. The separation of duties matrix will be updated or reviewed on an annual basis.

8.2.7 Information Security Awareness and Training Records

Reference: NIST 800-53 control AT-4
Provide the results of security awareness (AT-2) and role-based information security technical training (AT-3). AT-2 requires basic security awareness training for employees and contractors that support the operation of the contractor system. AT-3 requires information security technical training to information system security roles. Training shall be consistent with the requirements contained in C.F.R. Part 5 Subpart C (5 C.F.R 930.301) and conducted at least annually.

8.2.8 Annual FISMA Self-Assessment

Reference: NIST 800-53 control CA-2
Deliver the results of the annual FISMA self-assessment conducted per GSA IT Security Procedural Guide 04-26, "*Federal Information Security Modernization Act (FISMA) Implementation."* Based on the controls selected for self-assessment, the GSA OCISO will provide the appropriate test cases for completion.

8.2.9 System(s) Baseline Configuration Standard Document

Reference: NIST 800-53 control CM-2/CM-2(1)
Provide a well-defined, documented, and up-to-date specification to which the information system is built.

8.2.10 System Configuration Settings Verification

Reference: NIST 800-53 control CM-6/CM-6(1)
Establish and document mandatory configuration settings for information technology products employed within the information system that reflect the most restrictive mode consistent with operational requirements. Configuration settings are the configurable security-related parameters of information technology products that compose the information system. Systems should be configured in agreement with GSA technical guidelines, NIST guidelines, Center for Internet Security guidelines (Level 1), or industry best practice guidelines in hardening their systems, as deemed appropriate by the Authorizing Official.
Provide the most recent operating system Configuration Settings Compliance scan report.

8.2.11 Configuration Management Plan

Reference: NIST 800-53 control CM-9
Provide an annual update to the Configuration Management Plan for the information system.

8.2.12 Contingency Plan Test Report

Reference: NIST 800-53 control CP-4
Provide a contingency plan test report completed in accordance with GSA IT Security Procedural Guide 06-29, *"Contingency Planning."* A continuity test shall be conducted annually prior to mid-July of each year. The continuity test can be a table top test while the system is at the FIPS PUB 199 Low Impact level. The table top test must include Federal and hosting Contractor representatives. Functional exercises must be completed once every three years for FIPS PUB 199 Moderate impact systems and annually for FIPS PUB 199 High impact systems.

8.2.13 Incident Response Test Report

Reference: NIST 800-53 control IR-3
Provide an incident response plan test report documenting results of incident reporting process per GSA IT Security Procedural Guide 01-02, *"Incident Response."*

8.2.14 Information System Interconnection Agreements

Reference: NIST 800-53 control CA-3
Provide Interconnection Security Agreements (ISA) and supporting Memorandum of Agreement/Understanding (MOA/U), completed in accordance with NIST 800-47, *"Security Guide for Connecting Information Technology Systems,"* for existing and new interconnections. Per NIST 800-47, an interconnection is the direct connection of two or more IT systems for the purpose of sharing data and other information resources through a pipe, such as ISDN, T1, T3, DS3, VPN, etc. ISAs shall be submitted as appendices as part of the annual System Security Plan submission. ISAs shall include, if applicable, any changes since the last submission; updated ISAs are required at least every three years.

8.2.15 Rules of Behavior

Reference: NIST 800-53 control PL-4
Define and establish Rules of Behavior for information system users. Rules of Behavior shall be submitted as an appendix to the System Security Plan.

8.2.16 Penetration Testing Report

Reference: NIST 800-53 control CA-8
All Internet accessible systems, and all FIPS PUB 199 High impact systems are required to complete an independent penetration test and provide a Penetration Test Report documenting the results of the exercise as part of their A&A package. Annual penetration tests are required for these same systems in accordance with GSA Order CIO 2100.1 and CIO-IT Security-11-51, "*Conducting Penetration Test Exercises.*"

8.2.17 Personnel Screening and Security

Reference: NIST 800-53 control PS-3, NIST 800-53 control PS-7
Furnish documentation reflecting favorable adjudication of background investigations for all personnel (including subcontractors) supporting the system. Contractors shall comply with GSA Order CIO 2100.1, *"GSA Information Technology (IT) Security Policy"* and GSA Order, CIO P 2181.1, "*Homeland Security Presidential Directive-12 (HSPD-12) Personal Identity Verification and Credentialing Handbook*." GSA separates the risk levels for personnel working on Federal computer systems into three categories: Low Risk, Moderate Risk, and High Risk.

- Those contract personnel (hereafter known as "Applicant") determined to be in a Low Risk position will require a National Agency Check with Written Inquiries (NACI) investigation.
- Those Applicants determined to be in a Moderate Risk position will require either a Limited Background Investigation (LBI) or a Minimum Background Investigation (MBI) based on the Contracting Officer's (CO) determination.
- Those Applicants determined to be in a High Risk position will require a Background Investigation (BI).

Applicants will not be reinvestigated if a prior favorable adjudication is on file with FPS or GSA, there has been less than a one year break in service, and the position is identified at the same or lower risk level.

Once a favorable FBI Criminal History Check (Fingerprint Check) has been returned, Applicants may receive a GSA identity credential (if required) and initial access to GSA information systems. The HSPD-12 Handbook contains procedures for obtaining identity credentials and access to GSA information systems as well as procedures to be followed in case of unfavorable adjudications.

Deliverables to be provided to the GSA COR/ISSO/ISSM Biennially

8.2.18 Policies and Procedures

Develop and maintain current the following policies and procedures:

a. Access Control Policy and Procedures (NIST 800-53 AC-1)
b. Security Awareness and Training Policy and Procedures (NIST 800-53 AT-1)
c. Audit and Accountability Policy and Procedures (NIST 800-53 AU-1)
d. Identification and Authentication Policy and Procedures (NIST 800-53 IA-1)
e. Incident Response Policy and Procedures (NIST 800-53 IR-1, reporting timeframes are documented in GSA IT Security Procedural Guide 01-02, "Incident Response"
f. System Maintenance Policy and Procedures (NIST 800-53 MA-1)
g. Media Protection Policy and Procedures (NIST 800-53 MP-1)
h. Physical and Environmental Policy and Procedures (NIST 800-53 PE-1)
i. Personnel Security Policy and Procedures (NIST 800-53 PS-1)
j. System and Information Integrity Policy and Procedures (NIST 800-53 SI-1)
k. System and Communication Protection Policy and Procedures (NIST 800-53 SC-1)
l. Key Management Policy (NIST 800-53 SC-12)

8.3 Employee Security Requirements

The contractor shall provide personnel who already have or are capable of attaining and maintaining a Tier 2S security fitness determination. No access will be given to the Government computer information systems and Government sensitive information before the background investigation is completed.

8.3.1 New Contractor Personnel

The full names of all contractor personnel proposed to work under this contract must be submitted to the COR and GSA Security for initiation and/or verification of an individual's security clearance investigation status. No work shall commence under the contract until GSA has received either an initial Enter on Duty Date (EoDD) or a final favorable adjudication and have been approved to work on the contract.

8.3.2 Departing Contractor Personnel

The Contractor shall notify the COR, Contracting Officer and the GSA Personnel Security Officer when Contractor personnel will no longer be working on the contract. The Contractor must then turn in all badges; Government furnished equipment, and deliverables and provide an updated listing of GFE.

8.4 Common Access Card & ID Badges

When Government facilities are utilized in performance of this contract, the Government will provide photo identification, such as Common Access Card (CAC) and Restricted Area Badge (as required). The Contractor shall comply with all requirements necessary to obtain a CAC and Restricted Area Badge. Once issued, these credentials will allow Contractor employees unescorted entry into Government facilities.

8.5 Facility Security Requirements

The contractor needs to apply for the GSA access card (PIV) so its personnels can come to government facilities for meetings or in-person activities. See section 8.4 for ID Badges.

8.6 Personal Identity Verification

The Contractor shall comply with the following Personal Identity Verification clause.

52.204-9, Personal Identity Verification of Contractor Personnel. (Jan 2006)
(a) The Contractor shall comply with agency personal identity verification procedures identified in the contract that implement Homeland Security Presidential Directive-12 (HSPD-12), Office of Management and Budget (OMB) guidance M-05-24, and Federal Information Processing Standards Publication (FIPS PUB) Number 201.
(b) The Contractor shall insert this clause in all subcontracts when the subcontractor is required to have physical access to a federally-controlled facility or access to a Federal information system.

8.7 Additional Security Requirements

"Contracts involving GSA information systems must incorporate the CIO 09-48 IT Security Procedural Guide: Security and Privacy IT Acquisition Requirements and

CIO 12-2018 IT Policy Requirements Guide. Incorporating applicable requirements from these guides will ensure GSA information systems are secure and compliant with relevant laws.

- ***GSA Information Systems: Ensure contractor implements the requirements identified in MV-19-04 [PDF - 263 KB] --***
  - ***CIO 09-48, IT Security Procedural Guide: Security and Privacy IT Acquisition Requirements [DOCX - 277 KB]***
  - ***CIO 12-2018, IT Policy Requirements Guide [PDF - 277 KB]***

End of Clause

9. SPECIAL INSTRUCTIONS

9.1 Contractor Performance Assessment Reporting System (CPARS) Assessment

Upon request by the Government, the contractor shall submit a self-evaluation of their performance at least annually utilizing a Government provided template. From time of Government request, the contractor shall have 7 business days to provide input to the GSA COR. The contractor self-assessment will then be submitted to the Government client where they will utilize this information to formulate an independent performance evaluation that will be processed through the Contractor Performance Assessment Reporting System. The requirements of the FAR and its supplements as it pertains to CPARS reporting shall be adhered to.

9.2 Personal Services

This is not a “Personal Services” contract as defined by FAR 37.104. The government has taken the following steps and precautions to ensure that “Personal Services” employer-employee relationships are not created between government and contractor employees during performance of this task order. Although Contractor employees who furnish services under this contract are subject to Government technical oversight, neither the Government nor a Government authorized third party contractor or representative shall oversee Contractor employees but shall provide all direction through the Contractor’s designated representative(s) who is/are solely responsible for supervising and managing Contractor employees. In further compliance with this regulation:

- All tasks will be initiated using approved Task Directive Forms, email, Agile tools (such as Jira) or other approved form of documentation.
- All government direction or approval of contractor initiated suggestions shall be documented using approved Task Directive Forms or other approved form, email, Agile tools of documentation
- All government contract monitors shall communicate with the contractor through the approved contractor management representative.
- All government representatives responsible for managing this task order shall be briefed on the avoidance of personal services and those actions that represent personal services, prior to assuming their contract responsibilities.

9.3 Privacy Act

Work on this project may require that contractor personnel have access to information which is subject to the Privacy Act of 1974. Personnel shall adhere to the Privacy act, Title 5 of the U.S. Code, Section 552a and applicable agency rules and regulations when handling this information. Privacy Act information is considered sensitive and appropriate safeguards shall be implemented by the contractor. The contractor is responsible for ensuring all contractor personnel are briefed on privacy Act requirements.

9.4 Rehabilitation Act Compliance (Section 508)

Unless otherwise exempt, all services and/or products provided in response to this requirement shall comply with Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d), and the Architectural and Transportation Barriers Compliance Board Electronic and Information Technology (EIT) Accessibility Standards (36 CFR part 1194).

The Contractor shall support the Government in its compliance with Section 508 throughout the development and implementation of the work to be performed. Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d) requires that when Federal agencies develop, procure, maintain, or use electronic information technology, Federal employees with disabilities have access to and use of information and data that is comparable to the access and use by Federal employees who do not have disabilities, unless an undue burden would be imposed on the agency. Section 508 also requires that individuals with disabilities, who are members of the public seeking information or services from a Federal agency, have access to and use of information and data that is comparable to that provided to the public who are not individuals with disabilities, unless an undue burden would be imposed on the agency.

Additional information regarding Section 508 can be obtained from the following web sites:

http://www.section508.gov/index.cfm?FuseAction=Content&ID=12
http://www.access-board.gov/508.htm
http://www.w3.org/WAI/Resources

9.5 Final Invoice and Release of Claims

The contractor is required as a deliverable of the contract/order to provide a final invoice no later than 30 calendar days after the end of the period of performance. Additionally, the contractor shall provide a Release of Claims no later than 90 calendar days after the end of the period of performance. The contract/order will be modified for closeout.

9.6 Other Direct Costs (ODCs)

The Government may require the contractor to purchase materials and equipment and ODCs, to include hardware, software, and related supplies critical and related to the services being acquired under the contract/order. Such requirements will be identified at the time the contract/order is issued or may be identified during the course of a contract/order by the Government or the contractor. If the contractor initiates a purchase within the scope of the contract/order and the prime contractor has an approved purchasing system, the contractor shall submit to the GSA COR a Request to Initiate Purchase (RIP) (PWS Attachment E). If the prime contractor is to lose or does not have an approved purchasing system, the contractor shall submit to the CO a Consent to Purchase (CTP) (PWS Attachment F). The RIP and CTP shall include the purpose, specific items, estimated cost, cost comparison, and rationale. The contractor shall not

make any purchases without an approved RIP from the GSA COR or an approved CTP from the CO.

9.6.1 Cost of Software Maintenance Renewals

The government shall require the contractor to purchase and maintain records and licenses of all Software Maintenance Renewals listed in the FPDS and SAM FY Inventory prior to their renewal dates. This must still follow all rules and regulations set in place above.

9.7 Avoidance and/or Mitigation of Actual or Potential Organizational Conflicts of Interest

Contractor employees may have access to sensitive government information while performing this work, may be involved in reviewing and assessing the work of other contractors, and may be involved in developing specifications and work statements for subsequent or complementary work. There is a potential for organizational conflicts of interest if the Contractor has ties with firms whose work it will review or if the Contractor is subsequently awarded a contract that uses a specification or work statement that it prepared. To avoid actual or potential organizational conflicts of interest the Contractor, in conjunction with Government scheduling and oversight controls, must be able to mitigate its relationship with a firm whose work it might review during performance of this Task Order. No specific firm is currently identified but firm may be identified during the course of contract/task order performance. Additionally, the Contractor shall refrain from seeking contracts that incorporate Contractor generated specifications or work statements until it first demonstrates, to the satisfaction of the Contracting Officer, that obtaining such other contracts will not create an actual or potential organizational conflict of interest with work performed on this task order. The Contractor shall comply with the provisions of the task order clauses entitled “Organizational Conflicts of Interest,” “Notification of Conflicts of Interest Regarding Personnel,” “Limitation of Future Contracting,” and “Annual Conflict of Interest Certification” to meet this requirement, which shall be incorporated into the Task Order.

9.8 Task Order Management

9.8.1 Contracting Officer’s Representative (COR)

The Government Contracting Officer is primarily responsible for managing this contract / order. Additionally, the work to be performed under this contract / order is subject to monitoring by an assigned Contracting Officer’s Representative (COR). The COR appointment letter, outlining the COR responsibilities under this contract/order, will be provided to the contractor under separate cover upon request. Questions concerning COR appointments should be addressed to the Contracting Officer.

9.8.2 Government Technical Representative

In addition to the COR, the Government may assign one or more Technical Representatives to monitor the technical aspects of this contract / order. The Government Technical Representative will participate in project meetings and review task order deliverables and will provide technical assistance and clarification required for contract / order performance. Refer to the attached QASP for specific information on project monitoring.

9.9 Technical Direction

All work shall be performed within the scope of this PWS and the Government will not ask or require the Contractor to perform work that is outside of the scope of this Contract/Task Order. Clarification to the work may be provided to the Contractor in writing by the Contracting Officer's Representative (COR) using a Technical Directive form or other agreed upon written documentation. The Contractor's representative shall acknowledge receipt of such technical direction in writing. If specific tasks that fall within the scope of the performance objectives of this PWS are requested, amplified, or clarified by written technical direction, the Contractor shall comply with that direction, which shall become a part of this task order. Technical direction shall be provided at the management level and Contractor employees shall perform work as specified in this Contract/Task Order as directed by the Contractor's designated project manager, who shall have full responsibility for the assignment and monitoring of Contractor employee activities.

Task directives may include deliverables that are not initially identified in this task order. If so, task directives shall include specific delivery dates and places for reports and studies or a specific completion date for support services. As an alternative, the task directives may require the Contractor to establish timelines and milestones for completion of tasks. Government specified delivery or completion dates and Government approval of Contractor proposed timelines or milestones shall be binding on the Contractor.

Technical direction does not change the total dollar value of the contract or order; however, the dollar value of specific work identified in the technical directive may be obtained from the contractor for administrative purposes (e.g. proper allocation of funds, payment of invoices).

If the Contractor believes that any technical direction requires performance of work that is outside the scope of this contract / order, the Contractor shall immediately contact the Contracting Officer.

9.10 Data Ownership/Release/Availability/Rights

All Government data collected in the system is the property of the Federal Government. All data collected by the system shall be provided by the Contractor (system provider) as requested during the contract period and at the completion of the contract period in an electronic open standard data format that is easily reusable. The data shall be provided to the Government at no additional cost. The Government shall be afforded 14 calendar days to verify and validate the data and the Contractor shall be required to correct performance if errors or omissions are found.

Any information made available to the Contractor by the Government shall be used only for the purpose of carrying out the provisions of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of the contract. In performance of this contract, the Contractor assumes responsibility for the protection of the confidentiality of Government records and shall ensure that all work performed by its subcontractors shall be under the supervision of the Contractor or the Contractor's responsible employees. Each officer or employee of the Contractor or any of its subcontractors to whom any Government record may be made available or disclosed shall be notified in writing by the Contractor that information disclosed to such officer or employee can be used only for that purpose and to the extent

authorized herein. Further disclosure of any such information, by any means, for a purpose or to an extent unauthorized herein, may subject the offender to criminal sanctions imposed by 18 U.S.C. §§ 1030.

The Contractor will not disclose Customer Data to any government or third party or access or use Customer Data; except in each case as necessary to maintain the Cloud Services or to provide the Cloud Services to Customer in accordance with this contract, or as necessary to comply with the law or a valid and binding order of a governmental or regulatory body (such as a subpoena or court order). Unless it would be in violation of a court order or other legal requirement, the Contractor will give the Government reasonable notice of any such legal requirement or order, to allow the Government to seek a protective order or other appropriate remedy.

The data must be available to the Government upon request within one business day or within the timeframe negotiated with the Contractor, and shall not be used for any other purpose other than that specified herein. The Contractor shall provide requested data at no additional cost to the government.

The Government will retain unrestricted rights to government data. GSA must own and control its data, interfaces, processes, business rules and information with the ability to export easily and readily to other applications/systems/ Contractors in readable, usable formats, without added investments as the need arises. GSA retains ownership of any user created/loaded data and applications hosted on vendor's infrastructure, as well as maintains the right to request copies of these at any time.

9.11 Data Rights

The Government shall have unlimited royalty free rights to all data originally developed, generated and delivered under this contract or order as prescribed by the clause entitled **Rights in Data—General** (FAR 52.227-14 **)** which is incorporated into this task order or into the indefinite quantity contract upon which this order is based. The Contractor shall retain all rights to data used to meet the requirements of this task order if developed solely at the Contractor's expense for their commercial applications and sales.

The Government shall have the right to use all commercially developed and privately funded data delivered under this contract or order in accordance with, and subject to, the published agreements and restrictions that accompany that data.

9.12 Limited Use of Data

All data delivered or made available to the Contractor as Government Furnished Data shall remain the property of the Government and shall only be used by the Contractor in the performance of this contract or order. The Government retains all rights to Government Furnished Data.

At the conclusion of this contract/order all Government Furnished Data shall be dealt with according to the disposition instruction provided by the Contracting Office. If the Contracting Officer fails to provide disposition instruction for Government Furnished Data within thirty days of contract/task order end, the Contractor shall return all hard copy data and delete or otherwise destroy all electronic data.

9.13 Proprietary Data

The Contractor shall not employ the use of any proprietary data or software in the performance of this contract without the advanced written consent of the Contracting Officer.

9.14 Inspection and Acceptance

Inspection and acceptance will occur in accordance with the clause entitled Inspection of Services – Time and Material and Labor Hour (FAR 52.246-6) or Inspection of Services – Fixed Price (FAR 52.246-4), or) Inspection-Supplies - Fixed Price FAR 52-246-2(I), as applicable.

Payment for the correction of defective or deficient work will be handled as follow:

The Contractor will not be paid for re-performance of defective or deficient fixed priced services per the clause FAR 52-246-4(e) Inspection of Services-FP].

The Contractor will not be paid profit associated with re-performance of any defective or deficient time and material or labor hour work per the clause FAR 52-246-6 (f) Inspectioin-T&M.

In the absence of other agreements negotiated with respect to time provided for government review or specifically stated in other parts of this PWS, deliverables will be inspected and the contractor notified of the Government's Technical Representative's findings within five (5) work days of normally scheduled review. Unacceptable or unsatisfactory work will be handled as outlined in the QASP. Acceptance of invoices shall constitute acceptance of performance.

Inspection and acceptance shall be at destination.

9.15 Contract Type

This contract / order will be awarded using a combination fixed price and labor hour contract type.

9.16 Ceiling Price Notification

Per clause 52.323-7, Payments under Time-and-Materials and Labor-Hour Contracts, the contractor is reminded – "If at any time the Contractor has reason to believe that the hourly rate payments and travel costs that will accrue in performing this contract in the next succeeding 30 days, if added to all other payments and costs previously accrued, will exceed 85 percent of the ceiling price in the Schedule, the Contractor shall notify the Contracting Officer giving a revised estimate of the total price to the Government for performing this contract with supporting reasons and documentation."

9.17 Task Order Funding

It is anticipated that the task order will be fully funded. However, if incrementally funded, the following provision applies.

Incremental Funding

(GSA 5QZA AOD Memo, Subject: Incremental Funding-3 2009 01 (revised 07-23-09)

This project may be incrementally funded. If incrementally funded, funds will be added to this task via a unilateral modification as they become available. Contractor shall not perform work resulting in charges to the government that exceed obligated funds.

The Contractor shall notify the Contracting Officer in writing, whenever it has reason to believe that in the next 60 days, when added to all costs previously incurred, will exceed 75% of the total amount so far allotted to the contract/order by the Government. The notice shall state the estimated amount of additional funds required to complete performance of the contract/order for the specified period of performance or completion of that task.

Sixty days before the end of the period specified in the Schedule, the Contractor shall notify the Contracting Officer in writing of the estimated amount of additional funds, if any, required to continue timely performance under the contract/order or for any further period specified in the Schedule or otherwise agreed upon, and when the funds will be required.

The government is not obligated to reimburse the Contractor for charges in excess of the obligated funds and the Contractor is not obligated to continue performance or otherwise incur costs that would result in charges to the government in excess of the amount obligated under this order.

End of clause

9.18 Material and Material Handling Costs

Material and material handling costs will be paid as provided in FAR 52.232-7(b) “Payments under Time-and-Materials and Labor-Hour Contracts”. Material overhead will not be authorized if the costs normally included in that overhead (purchasing staff or other material handling costs) are being directly charged to this contract/task order.

9.19 Productive Direct Labor Hours

The Contractor shall only charge for labor hours when work is actually being performed in connection with this Task Order and not for employees in a “ready” status only. For this task order 1 FTE (full time equivalent) = 1920 labor hours.

9.20 Invoicing and Payment

Payments will be made in accordance with the clause entitled Payments (FAR 52.232-1) or Payments under Time-and-Materials and Labor-Hour Contracts (FAR 52.232-7), as applicable to each task order.

The Contractor may invoice for items upon their delivery or services when rendered. Billing and payment shall be accomplished in accordance with contract terms and GSA payment procedures. Invoice submission instructions shall be provided at the time of award.

9.21 Payment for Unauthorized Work

The Contractor will not be paid for the performance of work that is not authorized under this Task Order. No payments will be made for any unauthorized supplies and/or services or for any unauthorized changes to the work specified herein. This includes any services performed by the Contractor on their own volition or at the request of an individual other than a duly appointed CO, COTR, or Government Technical Representative. Only a duly appointed CO is authorized to change the specifications, terms, or conditions under this effort.

10 ATTACHMENTS

Attachment A – Contractor Non-Disclosure Agreement

Attachment B – QASP (Quality Assurance Surveillance Plan)

Attachment C – FPDS SLA (Service Level Agreement)

Attachment D – FPDS FY20 Software Inventory

Attachment E – FPDS AWS Server List

Attachment F – FPDS NonProd Network Architecture

Attachment G – FPDS Production and Coop Network Architecture

Attachment H – FPDS Monthly Steward Report Metrics

Attachment I – SAM.gov SLA (Service Level Agreement)

Attachment J – SAM Integration Software List

Attachment K – SAM Integration Environment Prod & Non-Prod Server

Attachment L – SAM iProd VPC Environment

Attachment M – CIO 12-2018_ IT Policy Requirements Guide

Attachment N – IT Security Procedural Guide

Summary Page

47QDCB21K0007, ID16210006

Ops and Maint FPDS SAM

	Total Ceiling
Base Year	$1,550,000.00
Option Year 1	$1,550,000.00
Option Year 2	$1,550,000.00
Option Period 3 (6 months)	$1,525,000.00
Option Period 4 (6 months)	$25,000.00
Grand Total	**$6,200,000.00**

SOLICITATION NUMBER
PROJECT TITLE
Note: Blue text are calculated cells
Note: Brown text are referenced cells
Note: Quantities are estimates and may be adjusted as determined by the offeror based on understanding of the statement of work

SCHEDULE OF ITE

COMET BPA PRIC

CLIN #	Labor Category (LCAT)
101	Program Manager (Senior)
102	Program Manager (Master)
103	IT Project Manager (Senior)
104	IT Project Manager (Master)
105	Management Analyst (Senior)
106	Technical Writer (Journeyman)
107	Technical Writer (Senior)
108	Training and Development Specialist (Journeyman)
109	Training and Development Specialist (Senior)
110	Agile Coach (Senior)
111	Agile Coach (Master)
112	Information Systems Security Officer (Journeyman)
113	Information Systems Security Officer (Senior)
114	Information Systems Security Officer (Master)
115	Information Security Engineer (Senior)
116	Information Security Engineer (Master)
117	Applications Software Developer (Journeyman)
118	Applications Software Developer (Senior)
119	Applications Software Developer (Master)
120	Web Developer (Journeyman)
121	Web Developer (Senior)
122	Web Developer (Master)
123	UI/UX Designer (Journeyman)
124	UI/UX Designer (Senior)
125	UI/UX Designer (Master)

126	Business Systems Analyst (Journeyman)
127	Business Systems Analyst (Senior)
128	Business Systems Analyst (Master)
129	Solutions Architect (Senior)
130	Solutions Architect (Master)
131	Database Architect (Senior)
132	Database Architect (Master)
133	Database Administrator (Journeyman)
134	Database Administrator (Senior)
135	Database Administrator (Master)
136	Data Warehousing Specialist (Journeyman)
137	Data Warehousing Specialist (Senior)
138	Data Warehousing Specialist (Master)
139	Business Intelligence Analyst (Journeyman)
140	Business Intelligence Analyst (Senior)
141	Business Intelligence Analyst (Master)
142	Software Quality Assurance Engineer and Tester (Journeyman)
143	Software Quality Assurance Engineer and Tester (Senior)
144	Software Quality Assurance Engineer and Tester (Master)
145	Cloud Engineer (Senior)
146	Cloud Engineer (Master
147	DevOps Engineer (Journeyman)
148	DevOps Engineer (Senior)
149	DevOps Engineer (Master)
150	User Support Specialist (Journeyman)
151	User Support Specialist (Senior)
152	User Support Specialist (Master)
153	Financial Analyst (Journeyman)
154	Financial Analyst (Senior)
155	COTS Product Specialist (Senior)
156	COTS Product Specialist (Master)

BASE PERIOD TOTAL

COMET BPA PRICING - C	
CLIN #	**Labor Category (LCAT)**
201	Program Manager (Senior)
202	Program Manager (Master)
203	IT Project Manager (Senior)

204	IT Project Manager (Master)
205	Management Analyst (Senior)
206	Technical Writer (Journeyman)
207	Technical Writer (Senior)
208	Training and Development Specialist (Journeyman)
209	Training and Development Specialist (Senior)
210	Agile Coach (Senior)
211	Agile Coach (Master)
212	Information Systems Security Officer (Journeyman)
213	Information Systems Security Officer (Senior)
214	Information Systems Security Officer (Master)
215	Information Security Engineer (Senior)
216	Information Security Engineer (Master)
217	Applications Software Developer (Journeyman)
218	Applications Software Developer (Senior)
219	Applications Software Developer (Master)
220	Web Developer (Journeyman)
221	Web Developer (Senior)
222	Web Developer (Master)
223	UI/UX Designer (Journeyman)
224	UI/UX Designer (Senior)
225	UI/UX Designer (Master)
226	Business Systems Analyst (Journeyman)
227	Business Systems Analyst (Senior)
228	Business Systems Analyst (Master)
229	Solutions Architect (Senior)
230	Solutions Architect (Master)
231	Database Architect (Senior)
232	Database Architect (Master)
233	Database Administrator (Journeyman)
234	Database Administrator (Senior)
235	Database Administrator (Master)
236	Data Warehousing Specialist (Journeyman)
237	Data Warehousing Specialist (Senior)
238	Data Warehousing Specialist (Master)
239	Business Intelligence Analyst (Journeyman)
240	Business Intelligence Analyst (Senior)
241	Business Intelligence Analyst (Master)
242	Software Quality Assurance Engineer and Tester (Journeyman)
243	Software Quality Assurance Engineer and Tester (Senior)
244	Software Quality Assurance Engineer and Tester (Master)
245	Cloud Engineer (Senior)
246	Cloud Engineer (Master
247	DevOps Engineer (Journeyman)

248	DevOps Engineer (Senior)
249	DevOps Engineer (Master)
250	User Support Specialist (Journeyman)
251	User Support Specialist (Senior)
252	User Support Specialist (Master)
253	Financial Analyst (Journeyman)
254	Financial Analyst (Senior)
255	COTS Product Specialist (Senior)
256	COTS Product Specialist (Master)

OPTION PERIOD 1 TOTAL

COMET BPA PRICING - C	
CLIN #	**Labor Category (LCAT)**
301	Program Manager (Senior)
302	Program Manager (Master)
303	IT Project Manager (Senior)
304	IT Project Manager (Master)
305	Management Analyst (Senior)
306	Technical Writer (Journeyman)
307	Technical Writer (Senior)
308	Training and Development Specialist (Journeyman)
309	Training and Development Specialist (Senior)
310	Agile Coach (Senior)
311	Agile Coach (Master)
312	Information Systems Security Officer (Journeyman)
313	Information Systems Security Officer (Senior)
314	Information Systems Security Officer (Master)
315	Information Security Engineer (Senior)
316	Information Security Engineer (Master)
317	Applications Software Developer (Journeyman)
318	Applications Software Developer (Senior)
319	Applications Software Developer (Master)
320	Web Developer (Journeyman)
321	Web Developer (Senior)
322	Web Developer (Master)
323	UI/UX Designer (Journeyman)
324	UI/UX Designer (Senior)
325	UI/UX Designer (Master)

326	Business Systems Analyst (Journeyman)
327	Business Systems Analyst (Senior)
328	Business Systems Analyst (Master)
329	Solutions Architect (Senior)
330	Solutions Architect (Master)
331	Database Architect (Senior)
332	Database Architect (Master)
333	Database Administrator (Journeyman)
334	Database Administrator (Senior)
335	Database Administrator (Master)
336	Data Warehousing Specialist (Journeyman)
337	Data Warehousing Specialist (Senior)
338	Data Warehousing Specialist (Master)
339	Business Intelligence Analyst (Journeyman)
340	Business Intelligence Analyst (Senior)
341	Business Intelligence Analyst (Master)
342	Software Quality Assurance Engineer and Tester (Journeyman)
343	Software Quality Assurance Engineer and Tester (Senior)
344	Software Quality Assurance Engineer and Tester (Master)
345	Cloud Engineer (Senior)
346	Cloud Engineer (Master
347	DevOps Engineer (Journeyman)
348	DevOps Engineer (Senior)
349	DevOps Engineer (Master)
350	User Support Specialist (Journeyman)
351	User Support Specialist (Senior)
352	User Support Specialist (Master)
353	Financial Analyst (Journeyman)
354	Financial Analyst (Senior)
355	COTS Product Specialist (Senior)
356	COTS Product Specialist (Master)

OPTION PERIOD 2 TOTAL

COMET BPA PRICING - Optior	
CLIN #	**Labor Category (LCAT)**
401	Program Manager (Senior)
402	Program Manager (Master)
403	IT Project Manager (Senior)

404	IT Project Manager (Master)
405	Management Analyst (Senior)
406	Technical Writer (Journeyman)
407	Technical Writer (Senior)
408	Training and Development Specialist (Journeyman)
409	Training and Development Specialist (Senior)
410	Agile Coach (Senior)
411	Agile Coach (Master)
412	Information Systems Security Officer (Journeyman)
413	Information Systems Security Officer (Senior)
414	Information Systems Security Officer (Master)
415	Information Security Engineer (Senior)
416	Information Security Engineer (Master)
417	Applications Software Developer (Journeyman)
418	Applications Software Developer (Senior)
419	Applications Software Developer (Master)
420	Web Developer (Journeyman)
421	Web Developer (Senior)
422	Web Developer (Master)
423	UI/UX Designer (Journeyman)
424	UI/UX Designer (Senior)
425	UI/UX Designer (Master)
426	Business Systems Analyst (Journeyman)
427	Business Systems Analyst (Senior)
428	Business Systems Analyst (Master)
429	Solutions Architect (Senior)
430	Solutions Architect (Master)
431	Database Architect (Senior)
432	Database Architect (Master)
433	Database Administrator (Journeyman)
434	Database Administrator (Senior)
435	Database Administrator (Master)
436	Data Warehousing Specialist (Journeyman)
437	Data Warehousing Specialist (Senior)
438	Data Warehousing Specialist (Master)
439	Business Intelligence Analyst (Journeyman)
440	Business Intelligence Analyst (Senior)
441	Business Intelligence Analyst (Master)
442	Software Quality Assurance Engineer and Tester (Journeyman)
443	Software Quality Assurance Engineer and Tester (Senior)
444	Software Quality Assurance Engineer and Tester (Master)
445	Cloud Engineer (Senior)
446	Cloud Engineer (Master
447	DevOps Engineer (Journeyman)

448	DevOps Engineer (Senior)
449	DevOps Engineer (Master)
450	User Support Specialist (Journeyman)
451	User Support Specialist (Senior)
452	User Support Specialist (Master)
453	Financial Analyst (Journeyman)
454	Financial Analyst (Senior)
455	COTS Product Specialist (Senior)
456	COTS Product Specialist (Master)

OPTION PERIOD 3 TOTAL

COMET BPA PRICING -Option P	
CLIN #	**Labor Category (LCAT)**
501	Program Manager (Senior)
502	Program Manager (Master)
503	IT Project Manager (Senior)
504	IT Project Manager (Master)
505	Management Analyst (Senior)
506	Technical Writer (Journeyman)
507	Technical Writer (Senior)
508	Training and Development Specialist (Journeyman)
509	Training and Development Specialist (Senior)
510	Agile Coach (Senior)
511	Agile Coach (Master)
512	Information Systems Security Officer (Journeyman)
513	Information Systems Security Officer (Senior)
514	Information Systems Security Officer (Master)
515	Information Security Engineer (Senior)
516	Information Security Engineer (Master)
517	Applications Software Developer (Journeyman)
518	Applications Software Developer (Senior)
519	Applications Software Developer (Master)
520	Web Developer (Journeyman)
521	Web Developer (Senior)
522	Web Developer (Master)
523	UI/UX Designer (Journeyman)
524	UI/UX Designer (Senior)
525	UI/UX Designer (Master)

526	Business Systems Analyst (Journeyman)
527	Business Systems Analyst (Senior)
528	Business Systems Analyst (Master)
529	Solutions Architect (Senior)
530	Solutions Architect (Master)
531	Database Architect (Senior)
532	Database Architect (Master)
533	Database Administrator (Journeyman)
534	Database Administrator (Senior)
535	Database Administrator (Master)
536	Data Warehousing Specialist (Journeyman)
537	Data Warehousing Specialist (Senior)
538	Data Warehousing Specialist (Master)
539	Business Intelligence Analyst (Journeyman)
540	Business Intelligence Analyst (Senior)
541	Business Intelligence Analyst (Master)
542	Software Quality Assurance Engineer and Tester (Journeyman)
543	Software Quality Assurance Engineer and Tester (Senior)
544	Software Quality Assurance Engineer and Tester (Master)
545	Cloud Engineer (Senior)
546	Cloud Engineer (Master
547	DevOps Engineer (Journeyman)
548	DevOps Engineer (Senior)
549	DevOps Engineer (Master)
550	User Support Specialist (Journeyman)
551	User Support Specialist (Senior)
552	User Support Specialist (Master)
553	Financial Analyst (Journeyman)
554	Financial Analyst (Senior)
555	COTS Product Specialist (Senior)
556	COTS Product Specialist (Master)

OPTION PERIOD 4 TOTAL

47QDCB21K0007, ID16210006
Ops and Maint FPDS SAM

Enter quoted rates & discount (if any) on this page.

EMS AND PRICES

CING - Base Year

Corresponding COMET BPA LCAT Cross Reference(if applicable)	COMET BPA Rate	Discount Rate	Amount of Discount	COMET Task Order Rate
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00

	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00

Option Period 1 - Year 2

Corresponding COMET BPA LCAT Cross Reference(if applicable)	COMET BPA Rate	Discount Rate	Amount of Discount	COMET Task Order Rate
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00

	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00

	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00

Option Period 2 - Year 3

Corresponding COMET BPA LCAT Cross Reference(if applicable)	COMET BPA Rate	Discount Rate	Amount of Discount	COMET Task Order Rate
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00

	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00

n Period 3 - Year 4 (First Half)

Corresponding COMET BPA LCAT Cross Reference(if applicable)	COMET BPA Rate	Discount Rate	Amount of Discount	COMET Task Order Rate
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00

	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00

	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00

Period 4 - Year 4 (Second Half)

Corresponding COMET BPA LCAT Cross Reference(if applicable)	COMET BPA Rate	Discount Rate	Amount of Discount	COMET Task Order Rate
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00

	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00
	$0.00	0.00%	$0.00	$0.00

Base Year

ENTER LABOR CATEGORY, NUMBER OF HOURS AND DISCOUNTED RATES FROM LH TAB. Enter prices only for proposed labor.

Tasks/Labor Category	Number of Hours/MONTH	Labor Rate (Enter Rates from LR Rate tab)	Fixed Price Buildup/MONTH
CLIN 1001: Phase-In (FFP)			
Enter Labor Category	0	$0.00	$0.00
Enter Labor Category	0	$0.00	$0.00
Enter Labor Category	0	$0.00	$0.00
Enter Labor Category	0	$0.00	$0.00
Enter Labor Category	0	$0.00	$0.00
Enter Labor Category	0	$0.00	$0.00
Enter Labor Category	0	$0.00	$0.00
Enter Labor Category	0	$0.00	$0.00
CLIN 1002: PMO (FFP)			
Enter Labor Category	0	$0.00	$0.00
Enter Labor Category	0	$0.00	$0.00
Enter Labor Category	0	$0.00	$0.00
Enter Labor Category	0	$0.00	$0.00
CLIN 1003: FPDS Operations and Maintenance (O&M) (FFP)			
Enter Labor Category	0	$0.00	$0.00
Enter Labor Category	0	$0.00	$0.00
Enter Labor Category	0	$0.00	$0.00
Enter Labor Category	0	$0.00	$0.00
Enter Labor Category	0	$0.00	$0.00
Enter Labor Category	0	$0.00	$0.00
Enter Labor Category	0	$0.00	$0.00
Enter Labor Category	0	$0.00	$0.00
Enter Labor Category	0	$0.00	$0.00
Enter Labor Category	0	$0.00	$0.00
Enter Labor Category	0	$0.00	$0.00
Enter Labor Category	0	$0.00	$0.00
Enter Labor Category	0	$0.00	$0.00
Enter Labor Category	0	$0.00	$0.00

Enter Labor Category	0	$0.00	$0.00
Enter Labor Category	0	$0.00	$0.00
Enter Labor Category	0	$0.00	$0.00
CLIN 1004: FPDS Security (FFP)			
Enter Labor Category	0	$0.00	$0.00
Enter Labor Category	0	$0.00	$0.00
Enter Labor Category	0	$0.00	$0.00
Enter Labor Category	0	$0.00	$0.00
CLIN 1005: FPDS Tier 2 Ticket Help Desk Support (FFP)			
Enter Labor Category	0	$0.00	$0.00
CLIN 1006: SAM Operations and Maintenance (O&M) (FFP)			
Enter Labor Category	0	$0.00	$0.00
Enter Labor Category	0	$0.00	$0.00
Enter Labor Category	0	$0.00	$0.00
CLIN 1007: SAM Security (FFP)			
Enter Labor Category	0	$0.00	$0.00
Enter Labor Category	0	$0.00	$0.00
CLIN 1008: SAM Tier 2 Ticket Help Desk Support (FFP)			
Enter Labor Category	0	$0.00	$0.00
CLIN 1009: Minor Enhancements (Reimburseable) NTE			
1009a Enter Labor Category (list Labor CLIN number also)	0	$0.00	
1009b Enter Labor Category (list Labor CLIN number also)	0	$0.00	
1009c Enter Labor Category (list Labor CLIN number also)	0	$0.00	
1009d Enter Labor Category (list Labor CLIN number also)	0	$0.00	
1009e Enter Labor Category (list Labor CLIN number also)	0	$0.00	
1009f Enter Labor Category (list Labor CLIN number also)	0	$0.00	
CLIN 1010: SAM/FPDS COOP (AWS) (FFP)			
CLIN 1011: SAM/FPDS Software/Tools (Reimburseable)			
CLIN 1012: ODC (Reimburseable)			
CLIN 1013: Training (Reimburseable)			

TOTALS	**0**

Ops and Maint FPDS SAM

Total CLIN Amount/MONTH	Total Amount/Year	Notes
$0.00	$0.00	
$0.00	$0.00	
$0.00	$0.00	

$0.00	$0.00	
$0.00	$0.00	
$0.00	$0.00	
$0.00	$0.00	
$0.00	$0.00	
	$0.00	
$0.00		
$0.00		
$0.00		Reimburseable Note: list the CLIN associated with the Labor Category, e.g. CLIN 1009a Business Systems Analyst (Journeyman) CLIN 126
$0.00		
$0.00		
$0.00		
	$0.00	
	$1,500,000.00	See Attachment to be provided. NTE
	$50,000.00	NTE
	$0.00	

	$1,550,000.00

Option Year 1

ENTER LABOR CATEGORY, NUMBER OF HOURS AND DISCOUNTED RATES FROM LH TAB. Enter prices only for proposed labor.

Ops and Maint FPDS SAM

Tasks/Labor Category	Number of Hours/MONTH	Labor Rate (Enter Rates from LR Rate tab)	Fixed Price Buildup/MONTH
CLIN 2001: PMO (FFP)			
Enter Labor Category	0	$0.00	$0.00
Enter Labor Category	0	$0.00	$0.00
Enter Labor Category	0	$0.00	$0.00
Enter Labor Category	0	$0.00	$0.00
CLIN 2002: FPDS Operations and Maintenance (O&M)			
Enter Labor Category	0	$0.00	$0.00
Enter Labor Category	0	$0.00	$0.00
Enter Labor Category	0	$0.00	$0.00
Enter Labor Category	0	$0.00	$0.00
Enter Labor Category	0	$0.00	$0.00
Enter Labor Category	0	$0.00	$0.00
Enter Labor Category	0	$0.00	$0.00
Enter Labor Category	0	$0.00	$0.00
Enter Labor Category	0	$0.00	$0.00
Enter Labor Category	0	$0.00	$0.00
Enter Labor Category	0	$0.00	$0.00
Enter Labor Category	0	$0.00	$0.00
Enter Labor Category	0	$0.00	$0.00
Enter Labor Category	0	$0.00	$0.00
Enter Labor Category	0	$0.00	$0.00
Enter Labor Category	0	$0.00	$0.00
Enter Labor Category	0	$0.00	$0.00
CLIN 2003: FPDS Security (FFP)			
Enter Labor Category	0	$0.00	$0.00
Enter Labor Category	0	$0.00	$0.00
Enter Labor Category	0	$0.00	$0.00

Enter Labor Category	0	$0.00	$0.00
CLIN 2004: FPDS Tier 2 Ticket Help Desk Support (FFP)			
Enter Labor Category	0	$0.00	$0.00
CLIN 2005: SAM Operations and Maintenance (O&M) (FFP)			
Enter Labor Category	0	$0.00	$0.00
Enter Labor Category	0	$0.00	$0.00
Enter Labor Category	0	$0.00	$0.00
CLIN 2006: SAM Security (FFP)			
Enter Labor Category	0	$0.00	$0.00
Enter Labor Category	0	$0.00	$0.00
CLIN 2007: SAM Tier 2 Ticket Help Desk Support (FFP)			
Enter Labor Category	0	$0.00	$0.00
CLIN 2008: Minor Enhancements (Reimburseable) NTE			
2009a Enter Labor Category (list Labor CLIN number also)	0	$0.00	
2009b Enter Labor Category (list Labor CLIN number also)	0	$0.00	
2009c Enter Labor Category (list Labor CLIN number also)	0	$0.00	
2009d Enter Labor Category (list Labor CLIN number also)	0	$0.00	
200ea Enter Labor Category (list Labor CLIN number also)	0	$0.00	
2009f Enter Labor Category (list Labor CLIN number also)	0	$0.00	
CLIN 2009: SAM/FPDS COOP (AWS) (FFP)			
CLIN 2010: SAM/FPDS Software/Tools (Reimburseable)			
CLIN 2011: ODC (Reimburseable)			
CLIN 2012: Training (Reimburseable)			
TOTALS	**0**		

Total CLIN Amount/MONTH	Total Amount/Year
$0.00	$0.00
$0.00	$0.00
$0.00	$0.00

$0.00	$0.00
$0.00	$0.00
$0.00	$0.00
$0.00	$0.00
	$0.00
$0.00	
$0.00	
$0.00	
$0.00	
$0.00	
$0.00	
	$0.00
	$1,500,000.00
	$50,000.00
	$0.00
	$1,550,000.00

Notes: Firm Fixed

Reimburseable Note: list the CLIN associated with the Labor Category, e.g. CLIN 1009a Business Systems Analyst (Journeyman) CLIN 126

See Attachment to be provided. NTE

NTE

Option Year 2

ENTER LABOR CATEGORY, NUMBER OF HOURS AND DISCOUNTED RATES FROM LH TAB. Enter prices only for proposed labor.

Ops and Maint FPDS SAM

Tasks/Labor Category	Number of Hours/MONTH	Labor Rate (Enter Rates from LR Rate tab)	Fixed Price Buildup/MONTH
CLIN 3001: PMO (FFP)			
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
CLIN 3002: FPDS Operations and Maintenance (O&M) (FFP)			
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
CLIN 3003: FPDS Security (FFP)			
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00

Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
CLIN 3004: FPDS Tier 2 Ticket Help Desk Support (FFP)			
Labor Category (Choose personnel)	0	$0.00	$0.00
CLIN 3005: SAM Operations and Maintenance (O&M) (FFP)			
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
CLIN 3006: SAM Security (FFP)			
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
CLIN 3007: SAM Tier 2 Ticket Help Desk Support (FFP)			
Labor Category (Choose personnel)	0	$0.00	$0.00
CLIN 3008: Minor Enhancements (Reimburseable) NTE			
3008a Enter Labor Category (list Labor CLIN number also)	0	$0.00	
3008b Enter Labor Category (list Labor CLIN number also)	0	$0.00	
3008c Enter Labor Category (list Labor CLIN number also)	0	$0.00	
3008d Enter Labor Category (list Labor CLIN number also)	0	$0.00	
3008e Enter Labor Category (list Labor CLIN number also)	0	$0.00	
3008f Enter Labor Category (list Labor CLIN number also)	0	$0.00	
CLIN 3009: SAM/FPDS COOP (AWS) (FFP)			
CLIN 3010: SAM/FPDS Software/Tools (Reimburseable)			
CLIN 3011: ODC (Reimburseable)			
CLIN 3012: Training (Reimburseable)			

TOTALS	**0**

Total CLIN Amount/MONTH	Total Amount/Year
$0.00	$0.00
$0.00	$0.00
$0.00	$0.00

$0.00	$0.00
$0.00	$0.00
$0.00	$0.00
$0.00	$0.00
	$0.00
$0.00	
$0.00	
$0.00	
$0.00	
$0.00	
$0.00	
$0.00	$0.00
	$1,500,000.00
	$50,000.00
	$0.00
	$1,550,000.00

Notes

Reimburseable Note: list the CLIN associated with the Labor Category, e.g. CLIN 1009a Business Systems Analyst (Journeyman) CLIN 126

See Attachment to be provided. NTE

NTE

Option Period 3

ENTER LABOR CATEGORY, NUMBER OF HOURS AND DISCOUNTED RATES FROM LH TAB, Enter prices only for proposed labor.

Ops and Maint FPDS SAM

Tasks/Labor Category	Number of Hours/MONTH	Labor Rate (Enter Rates from LR Rate tab)	Fixed Price Buildup/MONTH
CLIN 4001: PMO (FFP)			
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
CLIN 4002: FPDS Operations and Maintenance (O&M) (FFP)			
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
CLIN 4003: FPDS Security (FFP)			
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00

Labor Category (Choose personnel)	0	$0.00	$0.00
CLIN 4004: FPDS Tier 2 Ticket Help Desk Support (FFP)			
Labor Category (Choose personnel)	0	$0.00	$0.00
CLIN 4005: SAM Operations and Maintenance (O&M) (FFP)			
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
CLIN 4006: SAM Security (FFP)			
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
CLIN X007: SAM Tier 2 Ticket Help Desk Support (FFP)			
Labor Category (Choose personnel)	0	$0.00	$0.00
CLIN 4008: Minor Enhancements (Reimburseable) NTE			
4008a Enter Labor Category (list Labor CLIN number also)	0	$0.00	
4008b Enter Labor Category (list Labor CLIN number also)	0	$0.00	
4008c Enter Labor Category (list Labor CLIN number also)	0	$0.00	
4008d Enter Labor Category (list Labor CLIN number also)	0	$0.00	
4008e Enter Labor Category (list Labor CLIN number also)	0	$0.00	
4008f Enter Labor Category (list Labor CLIN number also)	0	$0.00	
CLIN 4009: SAM/FPDS COOP (AWS) (FFP)			
CLIN 4010: SAM/FPDS Software/Tools (Reimburseable)			
CLIN 4011: ODC (Reimburseable)			
CLIN 4012: Training (Reimburseable)			
CLIN 4013: Transition Out - Optional for OP3 (FFP)			
4013a Enter Labor Category (list Labor CLIN number also)	0	$0.00	
4013b Enter Labor Category (list Labor CLIN number also)	0	$0.00	
4013c Enter Labor Category (list Labor CLIN number also)	0	$0.00	
4013d Enter Labor Category (list Labor CLIN number also)	0	$0.00	
4013e Enter Labor Category (list Labor CLIN number also)	0	$0.00	
4013f Enter Labor Category (list Labor CLIN number also)	0	$0.00	
4013g Enter Labor Category (list Labor CLIN number also)	0	$0.00	
4013h Enter Labor Category (list Labor CLIN number also)	0	$0.00	

TOTALS	**0**

Total CLIN Amount/MONTH	Total Amount/Year
$0.00	$0.00
$0.00	$0.00
$0.00	$0.00

$0.00	$0.00
$0.00	$0.00
$0.00	$0.00
$0.00	$0.00
	$0.00
$0.00	
$0.00	
$0.00	
$0.00	
$0.00	
$0.00	
	$0.00
	$1,500,000.00
	$25,000.00
	$0.00
	$0.00
$0.00	
$0.00	
$0.00	
$0.00	
$0.00	
$0.00	
$0.00	
$0.00	
	$1,525,000.00

Notes

Enter prices only for proposed labor. Reimburseable Note: list the CLIN associated with the Labor Category, e.g. CLIN 1009a Business Systems Analyst (Journeyman) CLIN 126

See Attachment to be provided. NTE / Full Year to be provided

NTE

Reimburseable Note: list the CLIN associated with the Labor Category, e.g. CLIN 1009a Business Systems Analyst (Journeyman) CLIN 126

Option Period 4

ENTER LABOR CATEGORY, NUMBER OF HOURS AND DISCOUNTED RATES FROM LH TAB, Enter prices only for proposed labor.

Ops and Maint FPDS SAM

Tasks/Labor Category	Number of Hours/MONTH	Labor Rate (Enter Rates from LR Rate tab)	Fixed Price Buildup/MONTH
CLIN 5001: PMO (FFP)			
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
CLIN 5002: FPDS Operations and Maintenance (O&M) (FFP)			
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
CLIN 5003: FPDS Security (FFP)			
Labor Category (Choose personnel)	0	$0.00	$0.00

Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
CLIN 5004: FPDS Tier 2 Ticket Help Desk Support (FFP)			
Labor Category (Choose personnel)	0	$0.00	$0.00
CLIN 5005: SAM Operations and Maintenance (O&M) (FFP)			
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
CLIN 5006: SAM Security (FFP)			
Labor Category (Choose personnel)	0	$0.00	$0.00
Labor Category (Choose personnel)	0	$0.00	$0.00
CLIN 5007: SAM Tier 2 Ticket Help Desk Support (FFP)			
Labor Category (Choose personnel)	0	$0.00	$0.00
CLIN 5008: Minor Enhancements (Reimburseable)			
5008a Enter Labor Category (list Labor CLIN number also)	0	$0.00	
5008b Enter Labor Category (list Labor CLIN number also)	0	$0.00	
5008c Enter Labor Category (list Labor CLIN number also)	0	$0.00	
5008d Enter Labor Category (list Labor CLIN number also)	0	$0.00	
5008e Enter Labor Category (list Labor CLIN number also)	0	$0.00	
5008f Enter Labor Category (list Labor CLIN number also)	0	$0.00	
CLIN 5009: FPDS/SAM COOP (AWS) (FFP)			
CLIN 5010: ODC (Reimburseable)			
CLIN 5011: Training (Reimburseable)			
CLIN 5012: Transition Out (FFP)			
5012a Enter Labor Category (list Labor CLIN number also)	0	$0.00	
5012b Enter Labor Category (list Labor CLIN number also)	0	$0.00	
5012c Enter Labor Category (list Labor CLIN number also)	0	$0.00	
5012d Enter Labor Category (list Labor CLIN number also)	0	$0.00	
5012e Enter Labor Category (list Labor CLIN number also)	0	$0.00	
5012f Enter Labor Category (list Labor CLIN number also)	0	$0.00	
5012g Enter Labor Category (list Labor CLIN number also)	0	$0.00	
5012h Enter Labor Category (list Labor CLIN number also)	0	$0.00	

TOTALS	**0**

Total CLIN Amount/MONTH	Total Amount/Year
$0.00	$0.00
$0.00	$0.00
$0.00	$0.00

$0.00	$0.00
$0.00	$0.00
$0.00	$0.00
$0.00	$0.00
$0.00	$0.00
$0.00	
$0.00	
$0.00	
$0.00	
$0.00	
$0.00	
	$0.00
	$25,000.00
	$0.00
	$0.00
$0.00	
$0.00	
$0.00	
$0.00	
$0.00	
$0.00	
$0.00	
$0.00	
	$25,000.00

Notes

Enter prices only for proposed labor. Reimburseable Note: list the CLIN associated with the Labor Category, e.g. CLIN 1009a Business Systems Analyst (Journeyman) CLIN 126

NTE

Enter prices only for proposed labor. Reimburseable Note: list the CLIN associated with the Labor Category, e.g. CLIN 1009a Business Systems Analyst (Journeyman) CLIN 126