LETTER OF APPOINTMENT

MEMORANDUM FOR TJ CHEN, FEDSIM PM

Subject: Appointment as Contracting Officer's Representative

You are hereby appointed as the Contracting Officer's Representative (COR). This appointment is from the award date through the life of the Contract, to include close out, unless rescinded or transferred. As the COR, your primary duty is to monitor the Contractor's performance to ensure that all of the technical requirements under the contract are met by the delivery date or within the period of performance, and at the price or within the ceiling stipulated in the contract.

In the performance of the duties delegated to you in this letter, you are cautioned that you could be held personally liable for actions taken or directions given by you to the Contractor that are beyond the authorities given to you in this letter. The duties or authorities in this letter are not re-delegable; therefore, you must advise the Contracting Officer or the Contract Specialist immediately when you are unable to perform these duties.

Your duties and limitations, as applicable to the contract you will be monitoring, are as follows:

MONITORING AND EVALUATING PERFORMANCE

Ensure that the Contractor complies with all of the requirements of the statement of work, specifications, or performance work statement. When requested by the Contractor, provide technical assistance within the scope of the contract (e.g., interpreting specifications, statement of work, performance work statement, etc.). When a difference of opinion between you and the Contractor occurs, notify the Contracting Officer and/or the Contract Specialist immediately for resolution.

If the contract requires Key Personnel, the COR shall ensure that the personnel being used by the Contractor meet the requirements of the position. Review and approve travel and other direct cost (ODC) prior to the Contractor incurring those expenses. Any decrease in or lack of performance shall be brought to the attention of the Contracting Officer and/or Contract Specialist.

If applicable and in accordance with FAR 42.302, the COR shall monitor contractor compliance with specifications or other contractual requirements requiring the delivery or use of environmentally preferable products, energy-efficient products, products containing recovered materials, and bio-based products.

In accordance in Federal Acquisition Circular (FAC) 2005-34 and OMB Memorandum "Improving the Use of Contractor Performance Information" on July 29, 2009, CORs are responsible for entering past performance into the Past Performance Information Retrieval System (PPIRS) annually.

MONITORING COSTS

Review and evaluate the Contractor's progress in relation to the expenditures. When the costs expended by the Contractor are not commensurate with the Contractor's progress, request a meeting with the Contractor and client in an attempt to resolve. If a resolution cannot be found, bring this to the attention of the Contracting Officer and/or Contract Specialist for immediate action.

Review and approve invoices using the rates and other fees established in the contract. Review the Contractor's invoices/vouchers for reasonableness and applicability to the contract and recommend approval or rejection for payment.

CHANGES TO THE CONTRACT

You cannot authorize the Contractor to stop work, and you are not authorized to delete, change, waive, or negotiate any of the technical requirements or other terms and conditions of the contract. Should a change (monetary or otherwise) to the contract become necessary, it must be made by a contract modification issued by the Contracting Officer. When in doubt, contact the Contracting Officer and/or Contract Specialist.

Any contract change requested by the Contractor must be put in writing by the Contractor to the Contracting Officer for action. If, however, you become aware of an impending change, you should immediately advise the Contracting Officer or Contract Specialist. When the proposed change is received by the Contracting Officer, you will be required to provide the Contracting Officer with a written analysis and rationale for the change and to evaluate any costs associated with the change.

You must also recognize and report to the Contracting Officer any Government-required changes to the contract (e.g., items or work no longer required, changes in the specifications, etc.).

INSPECTION OF CONTRACT ITEMS

Perform, in accordance with the terms of the contract, inspection, acceptance, or rejection of the services or deliverables under the contract. The COR must prepare, in writing, a written acceptance or rejection, provide it to the Contractor, and store a copy on the FEDSIM common drive. Immediately notify the Contracting Officer of all rejections and the reason for the action.

Review progress reports from the Contractor and advise the Contracting Officer of any Contractor problems or action required to be taken by the Government.

STANDARDS OF CONDUCT AND CONFLICT OF INTEREST

To avoid improper business practices and personal conflicts of interest and to deal with their apparent or actual occurrences, the COR shall sign any applicable non-disclosure forms. The COR shall also immediately report any potential conflict of interest to their supervisor.

CONTRACT FILE CONTENT AND MAINTENANCE

Establish and maintain an organized contract administration file to record all Contractor and Government actions pertaining to the contract. The file must also include a copy of the COR Letter of Appointment and other documents describing the COR duties; a copy of the contract administration functions delegated to the contract administration office, which may not be delegated to the COR; and documentation of COR actions taken in accordance with the delegation of authority. The files should be organized and saved on the FEDSIM common drive.

CONTRACT CLOSEOUT

Within 30 days after the Contractor has met all terms and conditions of the contract, you must evaluate the Contractor's performance using the information contained in General Services Administration Regulation (GSAR) 542.1503-71 (sample format attached).

Please acknowledge receipt and acceptance of this appointment by signing below. Please direct any questions you may have on this delegation to the Contracting Officer or Contract Specialist.

I understand and accept my assignment as the Contracting Officer's Representative (COR)

X _____

TJ Chen
COR

_____

GSAR 542.15 – Contractor Performance Information

542.1503-71 – Information to collect.

Note: This checklist follows the standard format of GSAM 542.1542.15 and content requirements of GSAM 542.15. The checklist may be tailored for the specific contract type. Any "NO" responses noted below shall be accompanied with a statement explaining the observation(s). For each observation(s) provide a recommendation to correct the non-compliance. Observations identify areas of non-compliance and do require response (and action plans, if applicable). Positive observations may be general or specific and may be suitable for replication across the agency as good practices.

Contractor Performance Information

Timeliness of delivery or performance	Yes	No	NA
(1) Adherence to contract delivery schedules.			
(2) Resolution of delays.			
(3) Number of "show cause" letters and "cure notices" issued.			
(4) Number of delinquent deliveries.			
(5) Number of contract extensions resulting from contractor-caused delays.			
(6) Timely submission or performance or required tests.			
(7) Other.			
Observations (specify item #): ***Recommendations***:			

Conformance of product or service to contract requirements	Yes	No	NA
(1) Quality of workmanship.			
(2) Reliability.			
(3) Adequacy of correction of defects.			
(4) Number of safety defects.			
(5) Number of product rejections.			
(6) Results of laboratory tests.			
(7) Number and extent of warranty problems.			
(8) Other.			
Observations (specify item #): ***Recommendations***:			

GSAR 542.15 – Contractor Performance Information

542.1503-71 – Information to collect.

Customer comments	Num	Qty	NA
(1) Number and quality of positive comments.			
(2) Number and nature of complaints.			
(3) Adequacy of resolving customer complaints.			
(4) Other.			
Observations (specify item #): ***Recommendations***:			

Terminations for default	Yes	No	NA
Observations (specify item #): ***Recommendations***:			

On-the-job safety performance record, including the number of lost or restricted workdays due to occupational injuries in comparison to the national average	Yes	No	NA
Observations (specify item #): ***Recommendations***:			

Adequacy of contractor's quality assurance system	Yes	No	NA
Observations (specify item #): ***Recommendations***:			

Compliance with other key contract provisions	Yes	No	NA
(1) Subcontracting program			
(2) Labor standards			
(3) Safety standards.			
(4) Reporting requirements			
Observations (specify item #): ***Recommendations***:			

GSAR 542.15 – Contractor Performance Information

542.1503-71 – Information to collect.

Exhibiting customer-oriented behavior	Yes	No	NA
Observations (specify item #): ***Recommendations***:			

Other performance elements identified	Yes	No	NA
Observations (specify item #): ***Recommendations***:			

Acronyms

Acronym	Term
AC	Actual Cost
AFDO	Award Fee Determining Official
AFDP	Award Fee Determination Plan
AFEB	Award Fee Evaluation Board
ANSI	American National Standards Institute
ANSI/EIA	ANSI /Electronic Industries Alliance
AO	Authorizing Official
API	Application Programming Interface
APO	Accountable Property Officer
ASR	Asset Summary Reporting Format
ATO	Authority To Operate
BOM	Bill of Materials
C&A	Certification and Accreditation
CD	Compact Disk
CDM	Continuous Diagnostics and Mitigation
CEO	Chief Executive Officer
CFR	Code of Federal Regulations
CISSP	Certified Information System Security Professional
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CLIN	Contract Line Item Number
CMaaS	Continuous Monitoring as a Service

Acronym	Term
CO	Contracting Officer
CONOPS	Concept of Operations
CONUS	Continental United States
COR	Contracting Officer's Representative
COTS	Commercial Off-the-Shelf
CPAF	Cost-Plus-Award-Fee
CPARS	Contractor Performance Assessment Report System
CPE	Common Platform Enumerations
CS&C	Office of Cybersecurity and Communications
CM	Configuration Settings Management
CPI	Cost Performance Index
CSM	Configuration Settings Management
CSP	Cloud Service Provider
CVE	Common Vulnerability Enumerations
CWE	Common Weakness Enumerations
DAU	Defense Acquisition University
DB	Database
Dev/Test	Development and Testing
DHS	Department of Homeland Security
DHS HQ	DHS Headquarters
DLM	Data Lifecycle Management
DOA	Date of Award

Acronym	Term
DOE	Department of Energy
DOI	Department of Interior
DOT	Department of Transportation
DVD	Digital Video Disk
EA	Enterprise Architecture
EAC	Estimate to Completion
EDMO	Enterprise Data Management Office
EIT	Electronic and Information Technology
EOD	Entry on Duty
EOP	Executive Office of the President
EST	Eastern Standard Time
ET	Eastern Time
EULA	End User License Agreement
EV	Earned Value
EVM	Earned Value Management
FAI	Federal Acquisition Institute
FAR	Federal Acquisition Regulation
FAQ	Frequently Asked Questions
FEDSIM	Federal Systems Integration and Management Center
FEMA	Federal Emergency Management Agency
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FNR	Federal Network Resilience

Acronym	Term
FOIA	Freedom of Information Act
FOC	Final Operating Capability
FSC	Federal Service Code
FTE	Full Time Equivalents
FTR	Federal Travel Regulations
G&A	General and Administrative
GFE	Government Furnished Equipment
GFI	Government Furnished Information
GFP	Government Furnished Property
GFS	Government Furnished Services
GOTS	Government Off-the-Shelf
GSA	General Services Administration
GSAM	General Services Acquisition Manual
GSS	General Support System
GUI	Graphic User Interface
HHS	Health and Human Services
HLSEA	Homeland Security Enterprise Architecture
HSPD	Homeland Security Presidential Directive
HWAM	Hardware Asset Management
HQ	Headquarters
IA	Information Assurance
IaaS	Infrastructure as a Service
IAW	In Accordance With

Acronym	Term
ILM	Information Lifecycle Management
ILSP	Integrated Logistics Support Plan
IMS	Integrated Master Schedule
IOC	Initial Operating Capability
IPR	In Progress Review
IPT	Integrated Project Team
IPv6	Internet Protocol Version 6
IRM	Information Risk Management
ISCM	Information Security Continuous Monitoring
ISSO	Information System Security Officer
IT	Information Technology
ITAR	Information Technology Acquisition Review
IV&V	Independent Verification & Validation
KPQM	Key Personnel Qualification Matrix
LDAP	Lightweight Directory Access Protocol
LH	Labor Hour
MAS	Multiple Award Schedule
MDM	Mobile Device Management
MOA	Memorandum of Agreement
MS	MicroSoft
MSR	Monthly Status Report
MSSP	Managed Security Service Provider
MTV	Metrica Team Venture

Acronym	Term
NASA	National Aeronautical and Space Administration
NDA	Non-Disclosure Agreement
NIST	National Institute of Standards and Technology
NLT	No Later Than
NPPD	National Protection and Programs Directorate
NTE	Not to Exceed
NVD	National Vulnerability Database
OA	Office of Administration, or the White House
OAST	Office of Accessible Systems and Technology
O&M	Operations and Maintenance
OCI	Organizational Conflict of Interest
OCIL	Open Checklist Interactive Language
ODC	Other Direct Cost
OEM	Original Equipment Manufacturer
OIG	Office of Inspector General
OMB	Office of Management and Budget
OPM	Office of Personnel Management
ORR	Operational Readiness Review
OTA	Operational Test Authority
OTRR	Operational Test Readiness Review
PCC	Product Capability Code
PDDL	Product Delivery Data List
PDF	Portable Document Format

Acronym	Term
PgMP	Program Management Professional
PIA	Privacy Impact Assessment
PIHG	Privacy Incident Handling Guide
PIR	Post Implementation Review
PM	Program/Project Manager
PMI	Project Management Institute
PMO	Program Management Office
PMP	Project Management Professional
PMP	Project Management Plan
PNR	Problem Notification Report
POA&M	Plan of Action and Milestones
POC	Point of Contact
PoP	Period of Performance
POV	Privately Owned Vehicle
PRR	Production Readiness Review
PS	Project Start
PTA	Privacy Threshold Analysis
PV	Planned Value
PWS	Performance Work Statement
QA	Quality Assurance
Q&A	Question and Answer
QASP	Quality Assurance Surveillance Plan
QCP	Quality Control Plan

Acronym	Term
RFS	Request for Service
RIP	Request to Initiate Purchase
RMF	Risk Management Framework
RTM	Requirements Traceability Matrix
SA	Solutions Architect
SBU	Sensitive but unclassified
SCAP	Security Content Automation Protocol
SCRM	Supply Chain Risk Management
SDR	Service Design Review
SELC	Systems Engineering Life Cycle
SEMP	System Engineering Management Plan
SF	Standard Form
SIM	Systems Integration Manager
SIN	Special Item Number
SIP	Standard Install Process
SOA	Service Oriented Architecture
SOC	Security Operations Center
SORN	System of Records Notice
SOW	Statement of Work
SP	Special Publications
SPI	Schedule Performance Index
SPII	Sensitive Personally Identifiable Information
S&T	Science and Technology Directorate

Acronym	Term
SRR	Service Readiness Review
SSA	Social Security Administration
SWAM	Software Asset Management
T&E	Test and Evaluation
T&M	Time and Materials
TBD	To Be Determined
TBOM	Technical Bill of Materials
TEB	Technical Evaluation Board
TEMP	Testing and Evaluation Master Plan
TO	Task Order
TOA	Task Order Award
TOR	Task Order Request
TOS	Task Order System
TPOC	Technical Point of Contact
TRM	Technical Reference Model
U.S.	United States
U.S.C.	United States Code
USPS	United States Postal Service
UIC	Unit Identification Code
USDA	United States Department of Agriculture
USGv6	United States Government version 6
VA	United States Department of Veteran Affairs
VAC	Variance at Completion

Acronym	Term
VPAT	Voluntary Product Accessibility Template
VUL	Vulnerability Management
WBS	Work Breakdown Structure
XML	Extensible Markup Language

ATTACHMENT F
ORGANIZATIONAL CONFLICT OF INTEREST (OCI) STATEMENT

The offeror and each subcontractor, consultant, and/or teaming partner shall complete and sign an Organizational Conflict of Interest (OCI) Statement. All information pertaining to OCI is outlined in Section H.7.

The contractor shall represent either that:

1. It is not aware of any facts that create any actual or potential OCI relating to the award of this contract, or
2. It has included information in its proposal, providing all current information bearing on the existence of any actual or potential OCI.

If a contractor with an actual or potential OCI believes the conflict can be avoided, neutralized, or mitigated, the contractor shall submit a mitigation plan to the Government for review.

Definition: FAR 2.101 "Organizational conflict of interest" means that because of other activities or relationships with other persons, a person is unable or potentially unable to render impartial assistance or advice to the Government, or the person's objectivity in performing the contract work is or might be otherwise impaired, or a person has an unfair competitive advantage.

SAMPLE 1 – OFFEROR OCI STATEMENT

The following is an example of the OCI statement that each offeror shall complete and sign. All information pertaining to OCI is outlined in Section H.7.

Offeror Name is responding to Task Order Request (TOR) Task Order number GSC-QF0B-18-33119 for services supporting the Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) Dynamic and Evolving Federal Enterprise Network Defense - Group E (DEFEND E). In accordance with solicitation Section H.7, Offeror Name has reviewed the requirements of the TOR and the Federal Acquisition Regulation (FAR) Subpart 9.5.

Offeror Name is not aware of any facts which create any actual or potential OCI relating to the award of this contract. Offeror Name agrees to immediately disclose all information concerning any actual or potential OCI during the performance of the Task Order.

Offeror Name

_____ _____

Point of Contact (POC) Name* Date

_____

POC Title

*Person must have the authority to bind the company.

SAMPLE 2 – SUBCONTRACTOR, CONSULTANT, TEAMING PARTNER OCI STATEMENT

The following is an example of the OCI statement that each subcontractor, consultant, and teaming partner shall complete and sign. All information pertaining to OCI is outlined in Section H.7.

Company Name is participating as a subcontractor to Offeror Name in response to Task Order Request (TOR) Task Order number GSC-QF0B-18-33119 for services supporting the Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) Dynamic and Evolving Federal Enterprise Network Defense - Group E (DEFEND E). In accordance with solicitation Section H.7.1, Company Name has reviewed the requirements of the TOR and the Federal Acquisition Regulation (FAR) Subpart 9.5.

Company Name is not aware of any facts which create any actual or potential OCI relating to the award of this contract. Company Name agrees to immediately disclose all information concerning any actual or potential OCI during the performance of the Task Order.

Subcontractor, Consultant, Teaming Partner

_____ _____

Point of Contact (POC) Name* Date

_____

POC Title

*Person must have the authority to bind the company.

ATTACHMENT H
MONTHLY STATUS REPORT FOR (INSERT MONTH AND YEAR)

Contractor Name:	
Task Order Number:	GSC-QF0B-18-33118
Report Prepared by:	
Reporting Period:	From: [Month Day, Year] To: [Month Day, Year]

WORK PLANNED FOR THE MONTH:

WORK COMPLETED DURING THE MONTH:

WORK NOT COMPLETED DURING THE MONTH:

WORK PLANNED FOR NEXT MONTH:

CONTRACT MEETINGS:

[Include the meeting date, meeting subject, persons in attendance, and duration of the meeting.]

DELIVERABLE STATUS:

ISSUES/QUESTIONS/RECOMMENDATIONS:

RISKS:

[Indicate potential risks and their probability, impact, and proposed mitigation strategy.]

FUNDS/HOURS EXPENDED:

[Indicate total hours expended by the contractor during the week and total funds expended by the contractor during the week.]

Department of Homeland Security

Continuous Diagnostics and Mitigation (CDM) Program

Test & Evaluation Master Plan (TEMP)

Version 2.1

June 20, 2017

Test and Evaluation Master Plan (TEMP)

for

National Security Deployment

Continuous Diagnostics and Mitigation (CDM) Program

This document is under formal change control. Modifications to this document must be documented and reviewed by the appropriate change control board prior to usage or distribution.

Submitted by:

Program Manager	Date

Endorsed by:

NCCIC (User Representative)	Date

Endorsed by:

Operational Test Agent (OTA)	Date

Endorsed:

Component Acquisition Executive (CAE)	Date

Approved by:

DHS, Director, Office of Test and Evaluation	Date

Table of Contents

Table of Contents iii
List of Tables vi
List of Figures vii
Revision Summary viii
Executive Summary 1
Section 1: System Description 1
1.1 Purpose 1
1.2 Mission 1
1.2.1 System Users 3
1.2.2 System Threat Assessment 4
1.3 Capabilities 5
1.3.1 Acquisition Approach 6
1.3.2 Interfaces 7
1.3.3 Special Test or Certification Requirements 7
1.4 Integrated Master T&E Schedule 8
1.5 T&E Stakeholders 9
1.5.1 CDM PMO Organizational Construct 11
1.5.2 T&E Working-level Integrated Product Team (WIPT) 11
1.5.3 Operational User Representatives 15
1.5.4 Additional T&E Stakeholders 15
1.6 T&E Role in Systems Engineering 15
1.6.1 Requirements Analysis and Management 15
1.6.2 Systems Architecture Analysis 17
1.6.3 Deficiency and Risk Management 17
1.6.4 Technical Documentation Review 18
Section 2: Evaluation Framework 19
2.1 Decision Support Questions 19
2.2 Decision Support Matrix 23
2.3 Integrated Evaluation Framework (IEF) 24
2.3.1 IT&E Opportunities 25
Section 3: Integrated Test and Evaluation Activities 27
3.1 Integrated T&E Process 27
3.1.1 IT&E Preparation Process 29
3.1.2 IT&E Execution and Reporting Process 31
3.1.3 IT&E Process References 33
3.1.4 IT&E Assumptions, Limitations, and Constraints 33

3.2 Level-1 IT&E 34
3.2.1 Description 34
3.2.2 Objectives 37
3.2.3 Data Collection 38
3.2.4 Deficiency Report Generation 38
3.2.5 Test Limitations 38
3.2.6 Reliability Growth 38
3.2.7 Level-1 IT&E Reporting 40
3.3 Level-2 IT&E 40
3.3.1 Description 40
3.3.2 Objectives 41
3.3.3 Data Collection 42
3.3.4 Deficiency Report Generation 42
3.3.5 Test Limitations 42
3.3.6 Reliability Growth 42
3.3.7 Level-2 IT&E Reporting 42
3.4 Level-3 IT&E 43
3.4.1 Description 43
3.4.2 Objectives 43
3.4.3 Data Collection 45
3.4.4 Deficiency Report Generation 45
3.4.5 Test Limitations 45
3.4.6 Reliability Growth 45
3.4.7 Level-3 IT&E Reporting 45
3.5 OT&E Activities 46
3.5.1 Description 46
3.5.2 COIs 48
3.5.3 OT&E Strategy 49
3.5.4 Test Limitations 61
3.5.5 Reports 65
ANNEX 1: Operational View 1
ANNEX 2: Critical Technical Parameters 1
ANNEX 3: Key Performance Parameters 1
ANNEX 4: Critical Operational Issues 1
ANNEX 5: Interface Requirements 1
ANNEX 6: Failure Definition and Scoring Summary 1
ANNEX 7: Resource Summary 1
ANNEX 8: Decision Support Matrix and Integrated Evaluation Framework 1
ANNEX 9: Functional Requirements Documents 1

ANNEX 10: CDM RAM Rationale Document 1
ANNEX 11: Acronyms 1
ANNEX 12: References 1

List of Tables

Table 1-1: CDM User Community 4
Table 1-2: CDM Roll-Out by Phase 6
Table 1-3: CDM T&E Stakeholders 9
Table 2-1: CDM DSQs 19
Table A4-1: CDM List of COIs, MOEs, MOSs, and MOCs 1

List of Figures

Figure 1-1 - CDM Milestone Schedule 8
Figure 1-2 – CDM PMO Org Chart 11
Figure 1-3 - CDM T&E WIPT Org Chart 12
Figure 1-4 - CDM Requirement Source Diagram 16
Figure 1-5 – Common Deficiency Reporting Priority Scale 18
Figure 2-1 - CDM Decision Support Matrix 23
Figure 2-2 – CDM Integrated Evaluation Framework (IEF) Template 25
Figure 2-3 – Opportunities for CDM IT&E based on BPA Ordering Options, Segment(s) Tested, and DHS T&E Authority for the Different Levels of Risk Reduction Testing 26
Figure 3-1 - CDM IT&E Preparation Process (IT&E-PP) 31
Figure 3-2 - CDM IT&E Execution and Reporting Process 33
Figure 3-3 – Notional MTBOMF of COTS Product with Initial High Reliability 39
Figure 3-4 – Hypothetical MTBOMF of Selected CDM Element with Initial Low Reliability 40
Figure 3-5 – CDM COIs and Associated MOEs, MOSs, and MOCs 49

Revision Summary

The Table of Changes below describes specific changes, including references to changed sections/paragraphs.

Table 1: Configuration Management Tracker

Version	Document Date	Affected Pages	Revised By	Description of Change
1.0	Feb 24, 2014	All	N/A	Baseline
1.1	Mar 11, 2014	i, viii, ix, 1, 6-10, 14, 15, 17, 18, 20- 22, 25, 28, 29, 3, 34, 36, 45, A-3, A-4	CDM Test Team	Changes made based on review by DHS Director T&E and System Engineering
2.0 (Draft)	Feb 5, 2016	All	CDM Test Team and Operational Test Agent (OTA)	TEMP updated based on new SELC Appendix L guidance submitted for T&E WIPT Coordination
2.0	Feb 1, 2017	All	CDM Test Team	TEMP Updated based on all comments received
2.0	Mar 30, 2017	All	CDM Test Team	Final TEMP Updated based on all comments received
2.1	June 20, 2017		CDM Test Team	Revised per recommendations from Director, DOT&E to Table 1-3, 3-1, Figure 3-2, sections 1.2.1, 1.5, 3.2.2, 3.5.4.1, 3.5.3.5. Revised Table 1-1, Figure 1-1, Table 2-1, Page 47, Table A7-1,

Executive Summary

The Continuous Diagnostics and Mitigation (CDM) Program provides hardware, software, and services to enable continuous monitoring (CM) and diagnostics in support of mitigation activities designed to strengthen the security posture of government networks. CDM is available to all federal civilian executive Agencies in the .gov space.[1] Under this program, the Department of Homeland Security (DHS) centrally oversees the phased procurement, operations, and maintenance of monitoring equipment, diagnostic sensors and tools, and dashboards to provide situational awareness of Information Technology (IT) security at the federal and Agency levels. The Agencies will feed summary system security data to the DHS Federal Dashboard enabling it to support "government-wide and agency-specific efforts to provide adequate, risk-based and cost-effective cyber-security,"[2] consistent with its responsibilities as established by Congress and the Office of Management and Budget (OMB).

The purpose of this revision to the CDM Test and Evaluation Master Plan (TEMP) is to update the original CDM TEMP and to provide a framework for verifying the ability of the systems and services making up the CDM program to attain their required technical and operational capabilities. This TEMP is an update to the initial approved version (v1.1, March 2014), driven by changes to the CDM Operational Requirements Document (ORD) and a revision of the DHS Acquisition Instruction Guide 026-06-001-01: TEMP. The TEMP presents the overall structure and objectives of the planned Test and Evaluation (T&E) program, provides a framework within which to generate detailed T&E plans, documents the proposed test schedule, required test resources, identifies issues (systems, test, and requirements) to be resolved and those responsible for their resolution.

The CDM Program is an acquisition program that funded the establishment of Blanket Purchase Agreements (BPAs) by 17 identified vendors called Continuous Monitoring as a Service (CMaaS) integrators. This TEMP covers all three phases of the CDM Program: Phase 1, what is on the Network; Phase 2, Who is on the Network; and Phase 3, What is happening on the Network. The program identifies technical requirements for each identified Phase of the Program. CMaaS vendors are then invited to submit for consideration any commercial off the shelf (COTS) products (sensors and tools) that they believe meet those technical requirements. The Program completes a technical review to approve (or not) the products that enables the CMaaS vendor to include those products on their respective BPAs.

The program releases Requests For Quotes (RFQs) for groups of participating agencies; the RFQs are for tools and sensors, agency dashboards and integration services. The resulting awards bind the winning CMaaS integrator to proceed through DHS system engineering lifecycle

1 Per Public Law 113-6 in reference to CDM, "This section shall not apply to the legislative and judicial branches of the Federal Government and shall apply to all Federal agencies within the executive branch except the Department of Defense, the Central Intelligence Agency, and the Office of the Director of National Intelligence."

2 Office of Management and Budget Memorandum 10-28, Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security, July 6, 2010.

gates (tailored to reflect the COTS basis of the program); to produce its own TEMP to outline the testing strategy; to conduct appropriate testing within each agency, including user acceptance testing; and to share test plans, cases and results with the CDM Test Team.

The CDM testing strategy relies heavily on Integrated Test and Evaluation (IT&E) to be a more efficient and effective method of system testing. IT&E is designed to satisfy the needs of all Test and Evaluation (T&E) stakeholders collaboratively and efficiently by optimizing the use of available resources to test and evaluate a system. IT&E activities are developed collaboratively among all T&E stakeholders to collect data in support of unique T&E needs.[3] IT&E objectives primarily include program Developmental Test and Evaluation (DT&E) and Operational Test and Evaluation (OT&E) objectives while also supporting and leveraging customer Agency T&E objectives. DT&E is conducted to verify that CDM solutions conform to program specified functional requirements and specifications, mitigate program risk, assess cybersecurity, and ensure readiness for operational implementation. OT&E is conducted to evaluate effectiveness, suitability, interoperability, and cybersecurity of the overall system-of-systems when operated by typical users in an operational environment.

The CDM IT&E strategy encompasses CMaaS integration, the Agency CDM Dashboard, and the Federal Dashboard. Integrated evaluation of the systems includes any/all of the following: component testing of the Agency CDM Dashboard and Federal Dashboard, Independent Verification and Validation (IV&V) of the CMaaS provider's DT&E, systems testing of the CMaaS provider's solution, integration testing of the CMaaS provider's solution with the Agency CDM Dashboard, qualification of the CMaaS provider's solution and Agency CDM Dashboard to be deployed into the operational environment, Security Test and Evaluation (ST&E) of select CDM system components, Acceptance Testing (AT) of the CMaaS provider's solution and Agency CDM Dashboard in a controlled operational environment, integration testing of the Agency CDM Dashboard with the Federal Dashboard, and independent systems and services operational evaluation covering effectiveness, suitability, interoperability, and cybersecurity.

The CDM OT&E program is focused on identified assets and associated operating and support processes that reside within DHS, which coincides with where the DHS Director, Office of Test and Evaluation (DOT&E) have full T&E authority. Other than Operational Test Agent (OTA) observation at representative (to-be-specified) Agencies, as allowed by contract, no DHS funded OT&E will be conducted outside of DHS (i.e., in the Agency environment) unless requested by the Agency, approved by DHS Office of General Counsel (OGC), and with required documentation.[4] n[5] OT&E will be performed by the approved independent OTA through user participation in a operational environment. Operational Assessments (OAs) will be performed

3 DHS Acquisition Instruction Guidebook #026-06-001-01: Interim Appendix L TEMP v2.0, February, 2017

4 DHS Director of T&E only has authority within DHS. Legal concern have been identified that would have to be resolved through DHS OGC, referencing legislation contained in Title 31 U.S.C. and Title 44 U.S.C which confine Agency activities internally. See next footnote.

5 Part of the complication experienced here is acknowledged in Title 31 U.S.C. which states, "However, a single agency cannot fairly be expected to judge overall effectiveness in programs that cross agency lines—and the difference between agency and Presidential perspectives requires a capacity in the Executive Office to evaluate program performance whenever appropriate."

during the development of system-of-system to evaluate progress towards meeting specific operational requirements and Critical Operational Issue (COI) based measures. The OTA will conduct any remaining Operational Test (OT), in the operational environment or, if appropriate, an operationally representative environment, and will use actual data versus simulated data where possible.

This revised TEMP supports CDM Phases 1, 2 and 3 milestone decisions including program Initial Operational Capability (IOC), Acquisition Decision Event (ADE)-2B, ADE-3, and supporting project decision events. Program Final Operational Capability (FOC) is included for planning purposes at this time. It is expected that the TEMP will be updated prior to the execution of the test events associated with those decision events.

Section 1: System Description

1.1 Purpose

The purpose of this update to the Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) Test and Evaluation Master Plan (TEMP) is to provide a framework for verifying the ability of the systems and services making up the CDM program to attain their required technical and operational Phase1, 2, and 3 requirements and capabilities. The TEMP presents the overall structure and objectives of the planned Test and Evaluation (T&E) program, provides a framework within which to generate detailed T&E plans, documents the proposed schedule and required test resources, and identifies issues to be resolved and responsibilities for their resolution.

The CDM Program TEMP is the CDM program manager's (PM's) primary T&E planning document; the TEMP describes the capabilities the program must deliver, an evaluation framework that defines how the system will be evaluated in support of key acquisition decisions, and an efficient sequence of integrated test activities necessary to collect data across the performance envelope.

This TEMP is an update to the initial approved version (v1.1, March 2014), driven by changes to the CDM Operational Requirements Document (ORD)[6] and a revision of the DHS Acquisition Instruction Guidebook #026-06-001-01: TEMP, February, 2017 . This revised TEMP supports CDM Phases 1, 2 and 3 milestone decisions including program Initial Operational Capability (IOC), Acquisition Decision Event (ADE)-3, and supporting program decision events. If this TEMP is approved in time, it will also inform the CDM Phase 3 ADE-2B decision. Program Final Operational Capability (FOC) is included for planning purposes at this time

The following documents establish the CDM program:

- ORD 3.0 for CDM October 31, 2016
- DHS National Cyber Security Division Federal Network Security (FNS) Program Mission Needs Statement (MNS) for CDM, August 10, 2012
- DHS Concept of Operations (CONOPS) for CDM Version 1.0 March 11, 2013

1.2 Mission

CDM is designed to fill the following identified capability gaps:[6]

- In a dynamic threat space, the Federal Government continues to rely upon periodic security control assessments.
- The approach for implementing continuous monitoring within Federal Agencies is inconsistent, thus resulting in processes that cannot be replicated or reused.

6 ORD 3.0 for CDM October 31, 2016

- Agencies are challenged to manage their Information Technology (IT) assets to maintain an accurate inventory on hardware and software
- Agencies do not always have confidence that the assets are authorized, configured and patched appropriately.
- Without accurate information, information systems' managers cannot make risk-based decisions regarding information system security.
- Prioritization of system risks is difficult for managers because they are unable to clearly identify security issues and their relative importance across spaces within the organization.
- A solution is needed which will address the aforementioned gaps while streamlining current IT security institutions in order to gain efficiencies while increasing security.

In order to address these capability gaps, the Federal Government has identified multiple purposes for the CDM program to be one of the operational mechanisms to address the issues:[7]

- Improve the security posture of federal .gov networks;
- Improve the effectiveness and efficiency with which federal networks are secured;
- Improve the effectiveness and efficiency of Federal Information Security Management Act (FISMA) reporting;
- Build maturity into the continuous monitoring/diagnostics program across the federal enterprise;
- Develop a federal network infrastructure that is solidly based on secure engineering principles;
- Identify risks and establish a means to categorize them and a system to establish and maintain accountability; and
- Improve visibility allowing decision-makers to prioritize risks and ultimately fix the most security critical items first, allowing prioritization of remediation activities and resources.

Leveraging the past ten years of Federal civilian activities to strengthen continuous monitoring of their networks, DHS established the CDM program, based in part on authorities provided by Office of Management and Budget (OMB) to include OMB memos 10-28 and later the addition of OMB memo 14-03, and now OMB memo 16-03[7].

The Program releases Requests for Quotes (RFQs) for groups of participating agencies; the RFQs are for tools and sensors, CDM Agency Dashboards, and integration services. The resulting awards bind each winning Continuous Monitoring-as-a-service (CMaaS) integrator to proceed through DHS Systems Engineering Lifecycle (SELC) gates (tailored to reflect the Commercial off-the-shelf (COTS) basis of the program); to produce their own TEMP outlining their test strategy; to conduct appropriate testing in their lab environment and within each Agency, including User Acceptance Testing (UAT); with Independent Verification and Validation (IV&V) oversight from the CDM Test Team on behalf of the CDM Program Management Office (PMO).

7 Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements, Office of Management and Budget Memorandum M-16-03

Annex 1 provides a high-level view graph of the CDM system. As shown there are multiple levels within the CDM system structure. At the top level is the Federal Dashboard [level D]; which allows insight into Cybersecurity Risks from the entire Federal stakeholders. The Agency CDM system has two key elements. At the highest level, the Agency CDM Dashboard [level C] has a two part role: (1) the interaction of the Agency equities to the Federal Dashboard and (2) the central focus for the Agency by insight into Cybersecurity Risks via their Agency CDM Dashboard. At the lowest level [level A] are the tools and sensors that take the Agency assets and provides instrumentation to measure security management to them. The middle layer [level B] operates as the data integration mechanism between the tools & sensors and the Agency Dashboard to include functioning as the "collection" system. The general architecture for CDM provides for horizontal and vertical scaling at all levels as is appropriate for the Agency. For all levels except for the Dashboard [levels C&D], there is no constraint to singular technology implementations; in fact product diversity is allowed so that best fit and value can be provided to the participating Agencies.

1.2.1 System Users

Table 1-1 lists the constituent members of the CDM user community and outlines their respective responsibilities.[8]

8 Operational Test Agent's System Evaluation Plan for the CDM Program, IDA, February 2015 this document was not authorized to be provided by OTA and has not been reviewed or approved by the PMO.

Table 1-1: CDM User Community

User Community	Description of Responsibilities
User 1: Operational Users: Agencies, including Chief Information Officer (CIO) and Chief Information Security Officer (CISO) staff; operational administrators as appropriate	• May also function as the Agency Risk Executive, Authorizing Official (AO), Senior Information Security Officer (SISO), Information Security Owner (ISO)/Information Owner/Steward, Information System Security Officer (ISSO) • Operational User of CDM Agency Dashboard • Participate/Consult in IT&E activities
User 2: DHS National Protection and Programs Directorate (NPPD) Office of CyberSecurity and Communications (CS&C) Federal Network Resilience (FNR) staff; operational administrators as appropriate	• Uses the Federal Dashboard as an enterprise-level user group with appropriate access to view federal civilian agency data to develop Cross Agency Performance (CAP) and Federal Information Security Management Act (FISMA) reports for National Security Council (NSC), OMB and other federal stakeholders. • Query the Federal Dashboard database to generate federal IT enterprise cybersecurity performance management reports.
User 3: National Cybersecurity and Communications Integration Center (NCCIC)	• US Computer Emergency Readiness Team (US-CERT) has direct access to CDM federal data via the backend repository • Provides reporting and analysis of the Federal Executive Civilian Branch's security posture and provides mitigation recommendations • Provides threat and risk based policy to inform CDM scoring • Influence Agency cyber behavior by modifying federal risk scores
User 4: OMB staff	• Oversight of Agency Federal Information Systems Modernization Act (FISMA) Reporting Requirements – OMB gets reporting data from NPPD CS&C FNR
User 5: Agency Offices of the Inspector General (OIGs)	• Used for potential Agency assessments

1.2.2 System Threat Assessment

This section addresses the representation of potential threats to the systems, components and tools of the CDM program during integrated and independent operational testing. Broad threat categories include attacks on the confidentiality, integrity, and availability of the CDM system of systems and services. Another threat category included as part of the threat assessment is pivot-exploits in which attackers exploit possible new vulnerabilities introduced by CDM's integration of systems and services.

The CDM program has completed the following for considerations in this space:

- Assure that any of the parts provided by the CDM program within the solution set are all meeting the CDM monitoring and reporting activities

- US-CERT conducted a preliminary assessment in June 2016 of some of the COTS products associated with the CDM program and found three vulnerabilities which were noted for later action. A more robust assessment will be conducted at a later time.
- Provide support for the application of Risk Management (via scoring methodologies) to best remove known critical weaknesses and provide the information to formulate risk posture for new or previously unknown threats
- However, it is important to note that the CDM solution is hosted within the Agency's ecosystem and it is the risk assessment of that Agency that must address all cyber threats to the Agency.

The CDM cybersecurity (OT&E) framework requires credible representations of realistic cybersecurity threats that the CDM family of systems is expected to face in the real operational environment. The threat assessment should characterize both the capability and intent of current and future threats, including nation-state adversaries, in order to design OT&E to assess operational effectiveness and suitability to contest all threats. As part of the threat assessment all tools and services should be researched for potential threats posed by known adversaries. Furthermore, the threat representation should include descriptions of potential adversaries' behaviors and actions at a level of detail sufficient for defining kill-chains in support of IT&E. At present, NSD leadership is discussing with S&T regarding the need for a Department-wide cyber threat assessment to address the CDM system threat assessment.

1.3 Capabilities

The CDM program provides hardware, software, and services to enable fifteen capability areas for continuous monitoring (CM) and diagnostics plus the Agency Dashboards and the Federal Dashboard in support of mitigation activities to enhance situational awareness and ultimately strengthen the security posture of government networks (Table 1-2). Under this program, DHS centrally oversees the phased procurement, and installation of diagnostic sensors (tools) and dashboards deployed to each agency to accomplish these capabilities. Using input from the sensors and Agency Dashboards, officials at each Agency seek to be able to quickly identify which problems to fix first, and empower technical managers to prioritize and mitigate risks. In addition, DHS will maintain a Federal Dashboard taking input from the Agency Dashboards, to provide situational awareness on a federal level.

Table 1-2[9] shows the planned phased rollout of CDM capabilities.

9 Data in this table originates from the CDM ORD version 3.0 signed May, 2017

Table 1-2: CDM Roll-Out by Phase

Phase	Capability Area	Capabilities
Phase 1	Manage Assets	1) Hardware Inventory, 2) Software Inventory / Anti-virus, 3) Configuration Settings, 4) Vulnerabilities (Federal Dashboard)
Phase 2	Manage Accounts for People and Services	6) Trust in People Granted Access, 7) Security Related Behavior, 8) Credentials & Authentication, 9) Account Access, now termed Privileged Access
Phase 3	Manage Events	5) Network/Physical Access Control[10], (deferred from Phase 2) 10) Prepare for Incidents and Contingencies, 11) Respond to Incidents and Contingencies Ongoing assessment
	Security Lifecycle Management/ Design and Build in Security	12) Requirements, Policy and Planning, 13) Quality Management Supply Chain Risk Management
	Security Lifecycle Management/ Operate, Monitor and Improve	14) Operational Security, 15) Generic Audit/ Monitoring Ongoing Risk Management

1.3.1 Acquisition Approach

CDM Program is an acquisition program that funded the establishment of Blanket Purchase Agreements (BPAs) by 17 identified vendors called CMaaS integrators. The Program includes three phases (Phase 1, What is on the Network; Phase 2, Who is on the Network; and Phase 3, What is happening on the Network). The program identifies technical requirements for each identified Phase of the Program. CMaaS vendors are then invited to submit for consideration any COTS products (sensors and tools) that they believe meet those technical requirements. The Program completes a technical review to approve (or not) the products that enables the CMaaS vendor to include those products on their respective BPAs.

The program RFQs for groups of participating agencies; the RFQs are for tools and sensors and integration products and services. The resulting awards bind the winning CMaaS integrator to proceed through DHS system engineering lifecycle gates (tailored to reflect the COTS basis of the program); to produce its own TEMP to outline the testing strategy; to conduct appropriate testing within each agency, including user acceptance testing; and to share test plans, cases and results with the CDM Test Team.

10 Operational realities have led the program to conclude that while Manage Network/Physical Access Control is key, it can only be fully deployed after Manage Assets and Manage Accounts for People and Services have been completed. Accordingly, Capability 5, Manage Network/Physical Access, was deferred to the third phase.

1.3.2 Interfaces

The CDM program is comprised of various sensors/tools that have to interoperate with each other as well as with systems outside the CDM boundary. For the most part, the program is filling gaps in continuous network monitoring tools already operating in Agency networks. The CDM Program has released a CDM Data Model Document[11], and the CD Architecture Principles Document[12]. The sensors/tools will be connected to the Agency CDM Dashboard and an Interface Control Document (ICD) will be required for those interconnections. In addition, an ICD will be necessary for Agencies to connect to the Federal Dashboard. In order for the program to be successful, information exchanges across separate CDM solutions need to be evaluated from an interoperability perspective along with the external interfaces. See ANNEX 5: for additional details.

The following types of critical interfaces exist within the CDM program across CDM solution boundaries:

- CDM Agency Dashboard interfaces with the primary Federal Dashboard

CDM has the following types of critical external interfaces:

- CDM solution integration with Agency enterprise networks (multiple unique interfaces for each Agency) as appropriate
- CMaaS solution integration with CDM provided and legacy Agency tools / sensors (multiple unique interfaces for each Agency) as appropriate
- CDM solution integration with Cyber Scope or other surrogate Federal Dashboard, if required

1.3.3 Special Test or Certification Requirements

The IT&E strategy for CDM includes the option for the CDM PMO to request the CDM Test Team to conduct T&E in a PMO-designated test environment should the PMO decide that additional risk reduction is necessary (referred to as Level-2 IT&E, described in detail in Section 3) beyond that achieved or expected from Level-1 and Level-3 IT&E alone. Such activity may include the use of a Type-2 Technology Demonstrator[13]. Level-2 IT&E may include the use of a cyber range (live, virtual, and/or constructive test environment with deployed CDM solution) to evaluate technical, functional, operational, suitability, interoperability, and/or security characteristics of CDM.

---

11 CDM Data Model Document Version 1.0 DRAFT September 13, 2016

12 CDM Architecture Principles Document Version 0.5 DRAFT August 31, 2016

13 Type-2 Technology Demonstrators are used as part of a Program to develop, refine or verify requirements, explore technologies, and develop and/or verify designs throughout the Obtain phase. Type-2 demonstrations are typically conducted in simulated or laboratory (non-operational) environments, but may be conducted in controlled operationally relevant environments to obtain operational/user feedback. Type-2 demonstrations may be part of a program's contractor or DT effort. The scope of a Type-2 Demonstrator must be within the scope of the MNS/ORD, with objectives included in the APB. If part of a Developmental Test effort, the Type-2 Demonstrator objectives must be documented in the TEMP and DT Plans before evaluation. For CDM, the scope and plan for Type-2 technology demonstrators was part of the APB approval at ADE-2A.

At the present time, the CDM PMO is not planning any Level-2 IT&E for the CDM program. However, Level-2 IT&E remains an option for the CDM PMO should the need for additional risk reduction arise.

1.4 Integrated Master T&E Schedule

Figure 1-1 depicts the latest CDM program-level notional milestone schedule. At the present time, there is not a T&E-specific schedule. Test activity, described in detail in Section 3, occurs starting in the obtain phase for each Task Order (TO) stream. T&E events are scheduled in order to inform TO Operational Readiness Review (ORR) decision events (which occur at the end of each obtain phase), program Acquisition Decision Event (ADE) 2B (Phase 3 only) and IOC decisions, ADE 3, and the program FOC decision. The CDM program schedule and each of the supporting TO schedules are very dynamic. The T&E strategy for CDM is flexible and can accommodate frequent shifts in the program schedule by heavily leveraging T&E capabilities of the Solution Providers and receiving Agencies.

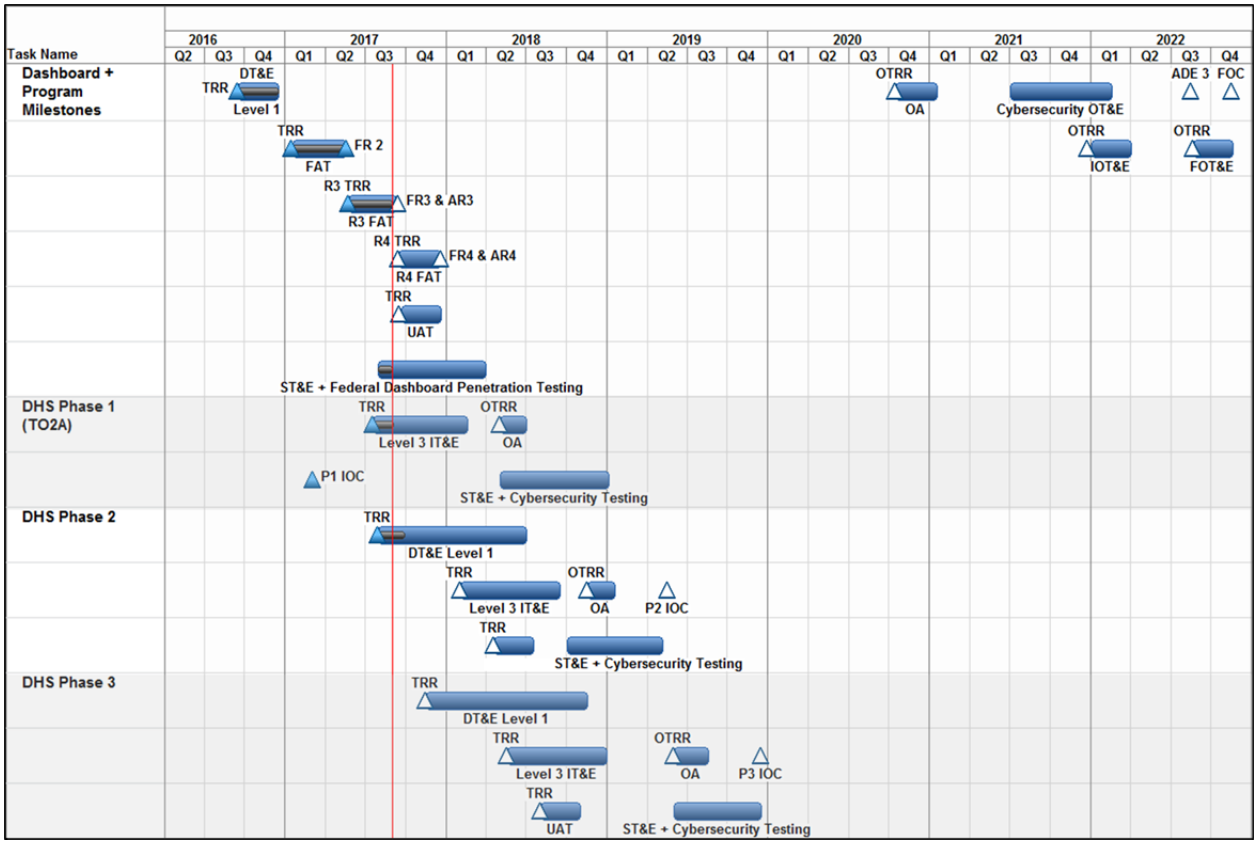


Figure 1-1 - CDM Milestone Schedule

1.5 T&E Stakeholders

Table 1-3 describes the stakeholders associated with the CDM program.

Table 1-3: CDM T&E Stakeholders

Stakeholder Group / Organization	Description of Responsibilities
Federal Agencies	• Manage Agency Risk (including authorize system operation) • Performs Operations and Maintenance (O&M) of CDM Agency Dashboard and Agency sensors and tools • Defines and conducts Level-3 IT&E with Solution Provider support • Provides the necessary insight to the CDM PMO, CDM Test Team, and (operational Test Agent (OTA) allowing for IV&V and assessment of readiness for operational implementation
CDM PMO	• Functional, operational, and program management group for CDM program • Program Implementation including development and management of acquisition strategy, related systems engineering, and risk management activities • Engineering support for architecture responsibilities • Working with the CMaaS vendors and Agencies to evaluate respective network environments and provide engineering expertise to review CMaaS proposed approaches for each Agency • Engineering support for the dashboards • Overall supervision of engineering control gates as successive releases become available • Work on future capabilities architecture
PM	• Program management lead for the CDM Program and head of the CDM PMO • Key CDM decision maker • Reference DHS MD 026-06[14] • Ensure the articulation of well-defined threats to the CDM system
DHS Director, Office of Test and Evaluation (DOT&E)	• Provides T&E oversight per MD 026-06 and DN 10003 • Issues DHS T&E policy and procedures • Approves OTA, TEMP, Operational Assessment Plan (OAP), Operational Test Plan (OTP) • Member of DHS Acquisition Review Board (ARB) • Reviews and analyzes results of IT&E for DHS acquisition programs
OTA - IDA	• Reference DHS MD 026-06
Operational Tester - APL	• JHU/APL will support the PMO by performing operational testing by following the Operational Test Plan provided by the OTA JHU/APL will support the PMO by performing operational testing by following the Operational Test Plan provided by the OTA
CDM Lead Systems Engineer (SE)	• Coordinate systems engineering activities for the CDM program • Review requirements, systems design and architecture, develop / update systems engineering management plan, and provide acquisition support including TO and statement of work (SOW) development • Technical Point of Contact (TPOC) between the Federal Systems Integrated Management Center (FedSIM) and the CDM PMO

14 Ibid., DHS Management Directive, Test and Evaluation, 22 May 2009

Stakeholder Group / Organization	Description of Responsibilities
CDM T&E Manager	• CDM point of contact for testing authority; leads the T&E working-level integrated product team (WIPT) • Generates the CDM Program TEMP and other test-related acquisition documents • Monitors system testing activities during program execution
CDM Test Team - APL	• Tasked with providing T&E and IV&V support as prescribed by CDM PMO
CMaaS Integrators	• Responsible for conducting development, integration and T&E as directed by their TO • Responsible for participating in the T&E WIPT and interacting with the CDM Test Team in support of IV&V activities
Security Test and Evaluation (ST&E) Teams (Multiple)	• Conduct ST&E on behalf of DHS Chief Information Systems Officer (CISO) supporting the Security Authorization to include the Authority to Operate (ATO) process for all CDM solutions • Provide Security Assessment Report to inform the DHS and Agency CIO or otherwise designated Authorizing Official (AO) • Leverage CDM host Agency self-assessment results prior to official Security Assessment (Agency self-assessment could be part of IT&E)
System Sustainment - National Security Deployment (NSD)	• Host Federal Dashboard
National Protection and Programs Directorate (NPPD) Component Acquisition Executive (CAE)	• Reference DHS MD 026-06
Federal Network Resilience (FNR)	• Develop and manage CDM maturity model for continuous monitoring and ongoing authorization • Lead business requirement efforts for the Federal Dashboard • Work with National Institute for Standards and Technology (NIST) in providing input to the risk scoring methodology/algorithms
National Cybersecurity & Communications Integration Center (NCCIC)	• Participate in all elements of Operational Test for Federal Dashboard components and support relevant Agency Dashboard tests that may impact data quality of the Federal Dashboard • Support CDM PMO in Risk Assessment activities on and against the CDM Infrastructure • Contribute to Business Requirements for Enterprise components of CDM including Federal Dashboard and Agency data interoperability based on operational partnerships.
General Service Administration (GSA) FEDSIM	• Communicate with vendors • Provides Contracting Officer (CO) • Provides Contracting Officer's Representative (COR) • Provides contractual legal oversight for all TO efforts

1.5.1 CDM PMO Organizational Construct

The CDM PMO is organized as follows:

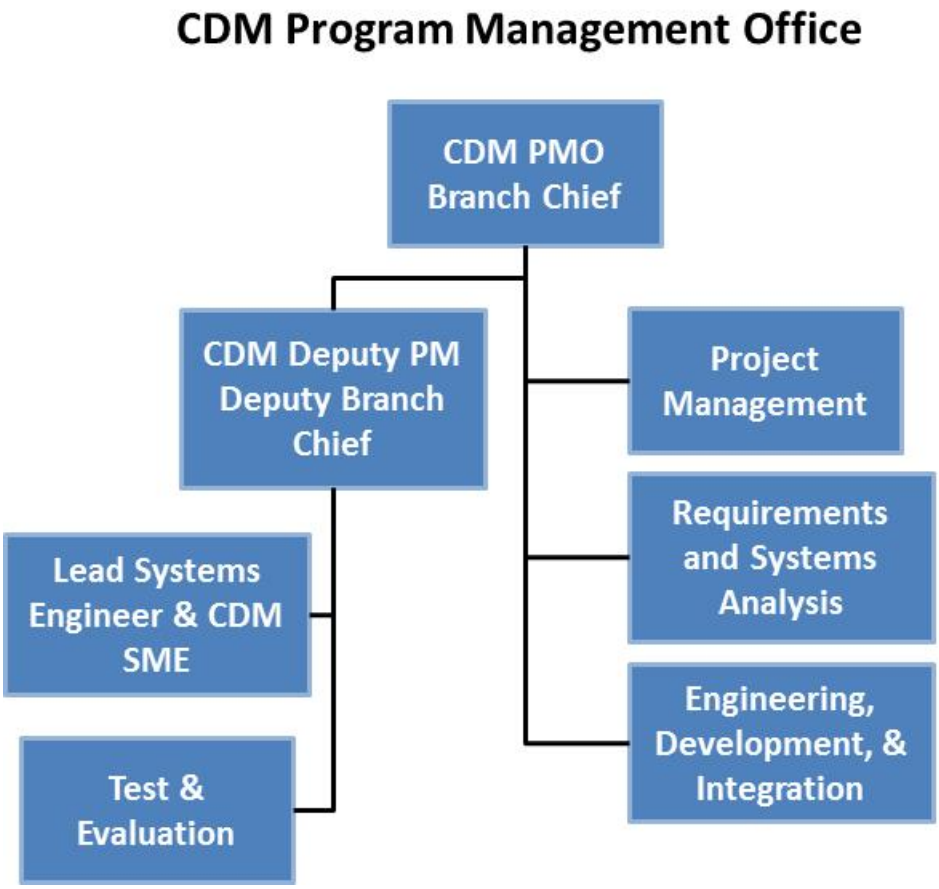


Figure 1-2 – CDM PMO Org Chart

1.5.2 T&E Working-level Integrated Product Team (WIPT)

The CDM T&E WIPT is the collaborative and integrated body of T&E professionals supporting the CDM program. The T&E WIPT is the forum for all T&E stakeholders to exchange information in order to ensure that all aspects of T&E are accomplished successfully. The CDM T&E WIPT is governed by the CDM Test Manager. T&E WIPT members include the CDM Test Team, OTA, Solution Provider T&E representatives, PMO representatives, Operational Testers, Agency T&E representatives, top-level CDM users, and other T&E stakeholders. Specific roles and responsibilities for each member group are included below. See Figure 1-3 for the T&E WIPT organizational structure.

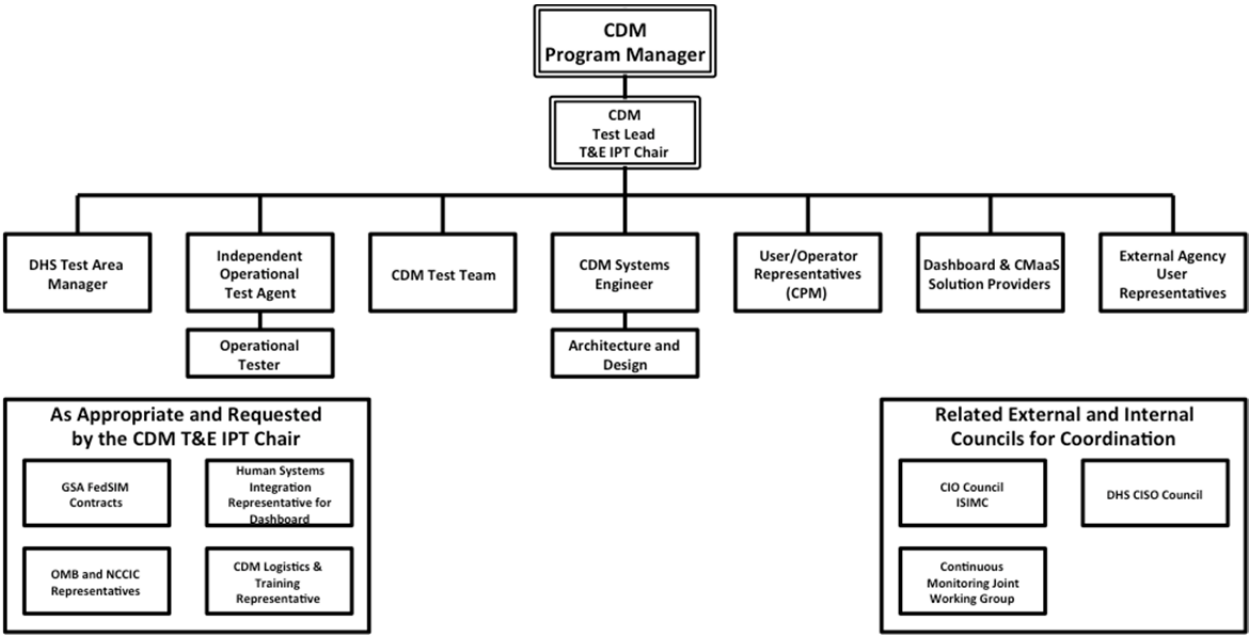


Figure 1-3 - CDM T&E WIPT Org Chart

1.5.2.1 CDM Test Team

The CDM Test Team, which is comprised of the DHS T&E Manager and Johns Hopkins University Applied Physics Lab (JHU/APL) team members, will serve on the CDM T&E WIPT and actively contribute to the planning for, conduct of, and evaluation of CDM T&E activities. Additionally, the CDM Test Team will participate in working level meetings in support of CDM. The CDM PMO will facilitate these interactions as necessary.

The CDM Test Team will perform CDM testing roles prescribed by CDM PMO. This will include close coordination and cooperation with the OTA on CDM Operational Test and Evaluation (OT&E) matters, development and execution of detailed test plans, and issuance of required reports to DHS. The CDM Test Team will be responsible for:

- Working with the CDM T&E WIPT, including CDM PM, systems engineering personnel, and requirements personnel, to conduct CDM Program Technical Analysis to support all levels of IT&E, starting with review of CDM Program systems engineering and acquisition documentation
- Conducting IV&V executed as part of CDM PMO oversight, including a thorough review of technical documentation (solution design documentation, test plans, requirements traceability matrices, etc.), test data and analysis, and other relevant information
- Conducting optional DT&E (at the CDM PMO's direction) conducted by the CDM Test Team on behalf of the CDM PMO as necessary to verify technical/functional specifications, confirm issue resolution, reduce program risks, gather additional data, and

ensure readiness to proceed to Level-3 IT&E testing in the Agency environment or solution
- Documenting deficiencies/limitations in conducting/executing testing

1.5.2.2 CDM Operational Test Agent (OTA)

The Institute for Defense Analyses (IDA) is the designated OTA for CDM and has overall responsibility for leadership on CDM OT&E and will serve as the Operational Evaluator. The OTA serves on the CDM T&E WIPT and actively contributes to the planning for, conduct of, and evaluation of CDM T&E activities, with a focus on the evaluation of Operational Effectiveness (OE), Operational Suitability (OS), interoperability, and cybersecurity. Additionally, the OTA participates in working level meetings in support of CDM.

As noted earlier, the OTA's authority to observe testing activity and collect data is limited to DHS HQ (Federal Dashboard) and DHS Component activities (T02A) and to testing activity conducted within CMaaS Integrator Provider facilities. The OTA may be permitted to observe and collect data at non-DHS Agencies with permission from those Agencies.

The OTA will determine OT&E issues, methods of evaluation, test resources, and test methodologies. The OTA will issue reports to DHS. Those reports will either explicitly acknowledge contributing operational tester personnel or, as appropriate, list the operational testers as co-authors. The OTA will be responsible for:

- Evaluation of CDM OE, OS, interoperability and cybersecurity
- Preparation of OA and OT Reports
- Monitoring, observation, and evaluation of OT&E events
- Determine Red/Blue Team activities supporting the resolution of OT&E objectives
- Determine characteristics of any scenario injects to live CDM operations
- Participation in the Data Authentication Group (DAG) for OT&E events
- Preparation of the OTA System Evaluation Plan (SEP) and updates
- Prescription of data definitions and scoring criteria that will be used to assess CDM operational performance (e.g., system reliability failures)
- Preparation of Letters Of Observations (LOOs) documenting findings from CDM IT&E and pre-OT&E CDM operations
- Monitoring, observation, and assessment of IT&E events (especially system integration) and pre-OT&E CDM operations
- Observation of and/or review of operational performance summaries for systems that potentially could serve as evaluation baselines for CDM

1.5.2.3 Operational Tester

The designated operational tester supports CDM and will coordinate with and assist the OTA for CDM. The operational tester is responsible for:

- Executing OT&E events (including dry runs) – ensuring compliance with test set-up and execution rules, recording and collecting prescribed quantitative and qualitative descriptive data, and distributing and collecting operator/user survey questionnaires.

- Providing inputs to the OTA for OT reports, OAs, LOOs, SEPs, and any other documentation related to OT&E
- Providing data in prescribed reduced forms and formats to support OTA analyses
- Preparation of Event Design Plans (EDPs) and Detailed Test Plans (DTPs) for the execution of OT&E events and data collection for the federal dashboard
- Assisting the OTA in determining Red/Blue Team requirements for activities supporting the resolution of OT&E objectives
- Leading the DAG effort for OT&E events, including chairing of the DAG

Both the OTA and the operational tester will be responsible for:

- Participation in the CDM T&E WIPT, with a focus on the planning for DT&E and OT&E
- Updating the overarching OT&E strategy of the TEMP as required
- Reviewing all portions of the TEMP and all other CDM T&E documentation and support of IT&E
- Development of operational scenarios and OT&E event concept plans
- Development of OT&E resource plans – including test hardware/software, operators, users, maintainers, trainers, and T&E-specific personnel, data collection, and instrumentation requirements
- Participation in Test Readiness Reviews (TRRs) and Operational Test Readiness Reviews (OTRRs)
- Reviewing all IT&E reports documenting demonstrated CDM performance and deficiencies

1.5.2.4 Solution Provider T&E Activity

The CMaaS Solution Provider and dashboard Solution Provider is contractually responsible for:

- Performing Level-1 DT&E, included but not limited to component testing, Modeling and Simulation (M&S), integration testing, systems testing, cybersecurity testing, and Acceptance Testing (AT)
- Defining their own testing strategy and presenting their test plan and design documentation to the CDM PMO for review and acceptance at the Solution Design Review (SDR) and Solution Readiness Review (SRR), and to the CDM Test Team to support their solution technical analysis and DT&E Plan development
- Providing test plans, procedures, test reports, and access to testing activities to the OTA and the CDM Test Team
- (CMaaS Solution Provider only) Verifying that the tools/sensors comprising their solution collectively satisfy program requirements
- (CMaaS Solution Provider and Agency based on Agency policy) Ensuring interoperability with the Agency and Federal Dashboard

1.5.2.5 PMO Representative(s)

The PMO will attend in person or designate representatives to participate in the T&E WIPT in order to facilitate communication between the test community and the CDM PMO.

Representatives can include but are not limited to program / project management staff, systems engineering / architecture staff, and the TPOC. PMO representatives are responsible for:

- Providing a program update to the T&E WIPT
- Addressing questions or providing information requested by T&E WIPT personnel
- Reviewing and providing guidance on T&E WIPT activities
- Providing formal direction to all Solution Providers based on T&E WIPT discussion, where necessary

1.5.3 Operational User Representatives

Representatives from the CDM user community are welcome and invited to participate in the CDM T&E WIPT. The role of user representatives includes participating in user acceptance T&E, independent OT&E, and providing feedback on CDM solution T&E planning, execution, and assessment activities which contributes to system validation activities.

1.5.4 Additional T&E Stakeholders

Additional T&E stakeholders include but are not limited to representatives from the DHS DOT&E's office, contract support to the CDM program, or other organizations involved or concerned with CDM T&E. Additional CDM T&E WIPT stakeholders may participate only as directed by the CDM Test Manager.

1.5.4.1 Department / Agency T&E Activity

Federal Agencies receiving CDM solutions have the authority to conduct acceptance testing of solutions entering their network. Therefore, Agencies may send representatives to the T&E WIPT in order to determine how best to integrate their T&E activities with those of the CDM program. Agency T&E representatives are encouraged to participate in the T&E WIPT; however they should coordinate attendance with the CDM Test Manager.

1.6 T&E Role in Systems Engineering

The DHS CDM Test Team, supported by other T&E stakeholders as necessary, provide support to the CDM program systems engineering activities, and also receive information from system engineering activities in order to accomplish their mission. For more information on CDM Systems Engineering activities see the CDM Systems Engineering Management Plan (SEMP).

1.6.1 Requirements Analysis and Management

In order to accomplish IV&V of Solution Provider activities, the CDM Test Team must completely understand CDM program requirements from the operational level down to the decomposed technical and functional level. Requirement sources include:

- Operational Requirements or Metrics/Measures
    - Mission Needs Statement
    - CONOPS
    - ORD
- Functional / Technical Requirements

  - Dashboard TO Attachment I
  - Phase 1 CMaaS TO Attachment N
  - Phase 2 CMaaS TO Attachment N2
  - Phase 3 CMaaS TO Attachment N3
  - Solution Provider Derived Requirements as delivered in their Requirements Traceability Matrix (RTM)
  - CDM Test Team Decomposed Requirements
- Cybersecurity Requirements
  - Requirements derived from DHS and Agency Information Assurance (IA) policy
  - Requirements derived from Cybersecurity Threat Assessment

In addition the OTA has developed its own SEP to guide its own OT&E planning and assessment. This SEP includes measures related to OE, OS, and cybersecurity. Requirement sources for the CDM program follow the diagram in Figure 1-4.

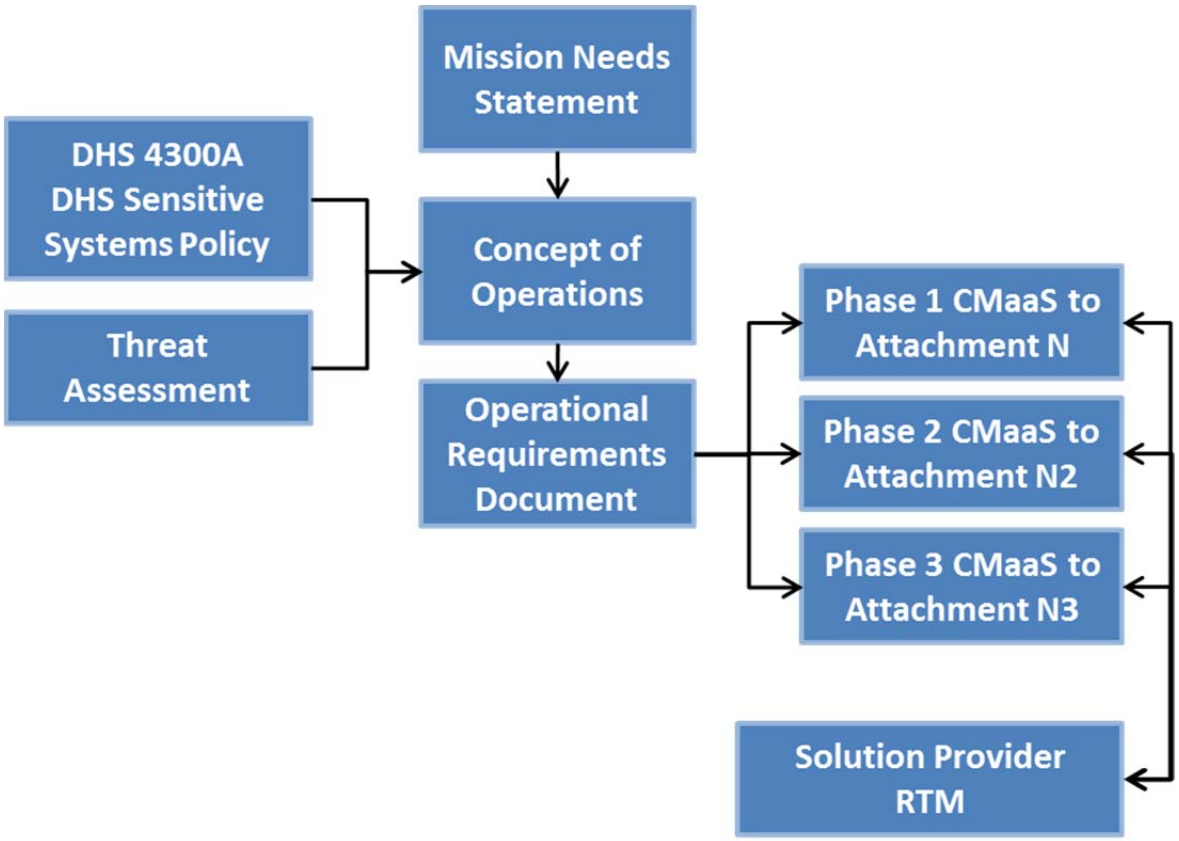


Figure 1-4 - CDM Requirement Source Diagram

In order to do perform the requirements analysis, the CDM Test Team works with CDM systems engineering staff to review and evaluate requirements for clarity, completeness, testability, and traceability. The CDM Test Team traces program requirements through the use of IBM Rational DOORS® Next Generation. This requirements repository supports effective requirements review through analysis of requirements linking (e.g. identify requirements gaps or orphan

technical requirements) and allows for the generation of Functional Requirements Documents (FRDs) for the Dashboard and CMaaS portions of the program.

1.6.2 Systems Architecture Analysis

The CDM Test Team uses and provides review of CDM systems architecture products as necessary in the review, creation, and execution of test plans and test cases. Where available, architecture products are used by the CDM Test Team to define system boundaries, interfaces, and use cases.

1.6.3 Deficiency and Risk Management

Test Deficiencies and risks are tracked at the CDM Program level by the CDM Test Team. All Solution Providers, the PMO, FEDSIM and Agency T&E representatives will have mechanisms for tracking problems discovered during test activities. The CDM TPOC, PMO, FEDSIM, and the CDM Test Team are responsible for tracking those issues as well as issues discovered by the CDM Test Team and the OTA on behalf of the CDM program. The CDM Test Team will support the PMO in deficiency tracking and resolution, and will maintain a T&E risk registry that is routinely provided to the PMO.

1.6.3.1 System Deficiencies

The CDM Test Team and OTA will use a common rating system for tracking deficiencies with CDM solutions discovered during T&E activities as defined in the Institute of Electrical and Electronics Engineers (IEEE) Standard 12207.2, p. 94. Deficiencies reported by Solution Providers may be documented according to different processes, depending on Solution Provider practices. As part of the IV&V process, the CDM Test Team will evaluate each Solution Providers' process. This rating system will be applied to system deficiencies identified during T&E by the CDM Test Team. It will not be applied to issues related to requirements and/or test execution. However, in order to assign the appropriate priority level, feedback from T&E stakeholders such as the CDM PMO user community and OTA are critical for understanding mission impact. If the CDM Test Team does not have the resources available to assign the priority level, the deficiencies will be reported to the PMO without prioritization.

Priority	Applies if a problem could
1	a) Prevent the accomplishment of an essential capability b) Jeopardize safety, security, or other requirement designated "critical"
2	a) Adversely affect the accomplishment of an essential capability and no work-around solution is known b) Adversely affect technical, cost, or schedule risks to the project or to life cycle support of the system, and no work-around solution is known
3	a) Adversely affect the accomplishment of an essential capability but a work-around solution is known b) Adversely affect technical, cost, or schedule risks to the project or to life cycle support of the system, but a work-around solution is known
4	a) Result in user/operator inconvenience or annoyance but does not affect a required operational or mission-essential capability b) Result in inconvenience or annoyance for development or maintenance personnel but does not prevent the accomplishment of the responsibilities of those personnel
5	Any other effect

Figure 1-5 – Common Deficiency Reporting Priority Scale[15]

1.6.3.2 Program Risk

The CDM PMO established a Risk Integrated Product Team (IPT) in 2013 and it meets twice a month for a full discussion of each risk, its status, and its mitigation. New risks and issues are added as identified. The Risk manager maintains a risk registry that includes risk items at a higher level than system deficiencies and other test-related risks. The CDM Test Team will provide input to the program risk registry based on findings and assessments from all T&E activities when appropriate.

1.6.4 Technical Documentation Review

The CDM Test Team and OTA, as members of the T&E WIPT, participate in program and Solution Provider technical documentation review. Such program documentation can include systems engineering, acquisition, architecture products, and contract documentation (e.g. SEMP, SELC tailoring guide, TOs). Example Solution Provider documentation includes the Solution Provider's TEMP, test plans and test cases, quality management documentation, test reports, defect tracking data, and test schedules. For more information see Section 3.1.1 and the CDM Test Team's IV&V strategy for a listing of documents that fall under CDM Test Team technical review.

[15] As defined in the IEEE Std. 12207.2, p. 94

Section 2: Evaluation Framework

2.1 Decision Support Questions

The test strategy for CDM is designed to inform the following acquisition milestone decisions by providing information needed to answer the associated Decision Support Questions (DSQs):

Table 2-1: CDM DSQs

Decision Event	Date	Associated DSQs
Phase 1 ADE 2A/B (Program)	3QFY14 (completed)	N/A – No DSQs drafted for this decision event
Agency Dashboard Release 1 Functional Acceptance	4QFY15 (completed)	1. Is the Agency Dashboard Release 1 solution ready for CMaaS integration? 2. Are the remaining program requirements (functional) user-validated, traceable, measurable, testable and achievable?
Phase 2 ADE 2B (Program)	4QFY15 (completed)	1. Is the program documentation current (ORD, TEMP…)? 2. Are the program requirements (functional / Critical Technical Parameters (CTP) / Measure of Effectiveness (MOE) / Measure of Suitability (MOS) / Measures of Cybersecurity (MOCs) / Key Performance Parameter (KPP)) user-validated, traceable, measurable, testable and achievable? 3. Is the PMO adequately resourced to conduct testing for each phase of system deployment the program is entering? OT and OTA? 4. Have all the users of the system been identified, and has the PMO reached out to all of them? 5. Are the security responsibilities between the CDM PMO and the Agencies (to include DHS) clearly defined?
Agency Dashboard Release 2 Functional Acceptance	4QFY16 (completed)	1. Is the Agency Dashboard Release 2 solution ready for CMaaS integration? 2. Are the remaining program requirements (functional) user-validated, traceable, measurable, testable and achievable?
Federal Dashboard Release 1 Functional Acceptance	2QFY16 (completed)	1. Is the Federal Dashboard Release 1 solution ready for Agency Dashboard integration? 2. Are the remaining program requirements (functional) traceable, measurable, testable, and achievable
Phase 3 ADE 2B (Program)	3QFY22 (TBD)	3. Is the program documentation current (ORD, TEMP…)? 4. Are the program requirements (functional / CTP / MOE / MOS / MOCs / KPP) user-validated, traceable, measurable, testable and achievable? 5. Is the PMO adequately resourced to conduct testing for Phase 2? OT and OTA?

Decision Event	Date	Associated DSQs
		6. Have all the users of the system been identified, and has the PMO reached out to all of them? 7. Are the security responsibilities between the CDM PMO and the Agencies (to include DHS) clearly defined?
CMaaS TO 2A ORR	Q1FY19	1. Are the CMaaS solution integration activities complete? 2. Has the CMaaS solution successfully undergone adequate test and evaluation (e.g. Level-1 and Level-3 IT&E)? 3. Have all functional and operational requirements been satisfied? 4. Are there any open high-level operational risks with the solution? 5. Have operational users been identified and trained on the CMaaS solution? 6. Is the CMaaS solution ready for operational use?
CMaaS TO 2B ORR	TBD	1. Are the CMaaS solution integration activities complete? 2. Has the CMaaS solution successfully undergone adequate test and evaluation (e.g. Level-1 and Level-3 IT&E)? 3. Have all functional and operational requirements been satisfied? 4. Are there any open high-level operational risks with the solution? 5. Have operational users been identified and trained on the CMaaS solution? 6. Is the CMaaS solution ready for operational use?
IOC (Program)	Q1FY17	1. Are CDM Phase 1 capabilities operationally deployed in at least 5 Agencies? 2. Are there any open high-level operational risks with the deployed solutions?
Federal Dashboard Release 2 Functional Acceptance	Q3FY17	1. Is the Federal Dashboard Release 2 solution ready for Agency Dashboard integration? 2. Are the remaining program requirements (functional) user-validated, traceable, measurable, testable, and achievable
Agency Dashboard Release 3 Functional Acceptance	Q4FY17	1. Is the Agency Dashboard Release 3 solution ready for CMaaS integration? 2. Are the program requirements (functional) tested and user-validated, traceable, measurable, testable and achievable?
Integrated Readiness Review (IRR) / OTRR (Program)	Q4FY21	1. Are all program solutions ready for integration? 2. Are all program solutions ready to enter operational testing?
CMaaS TO 2C ORR	TBD	1. Are the CMaaS solution integration activities complete? 2. Has the CMaaS solution successfully undergone adequate test and evaluation (e.g. Level-1 and Level-3 IT&E)?

Decision Event	Date	Associated DSQs
		3. Have all functional and operational requirements been satisfied? 4. Are there any open high-level operational risks with the solution? 5. Have operational users been identified and trained on the CMaaS solution? 6. Is the CMaaS solution ready for operational use?
CMaaS TO 2D ORR	TBD	1. Are the CMaaS solution integration activities complete? 2. Has the CMaaS solution successfully undergone adequate test and evaluation (e.g. Level-1 and Level-3 IT&E)? 3. Have all functional and operational requirements been satisfied? 4. Are there any open high-level operational risks with the solution? 5. Have operational users been identified and trained on the CMaaS solution? 6. Is the CMaaS solution ready for operational use?
CMaaS TO 2E ORR	TBD	1. Are the CMaaS solution integration activities complete? 2. Has the CMaaS solution successfully undergone adequate test and evaluation (e.g. Level-1 and Level-3 IT&E)? 3. Have all functional and operational requirements been satisfied? 4. Are there any open high-level operational risks with the solution? 5. Have operational users been identified and trained on the CMaaS solution? 6. Is the CMaaS solution ready for operational use?
CMaaS TO 2F ORR	TBD	1. Are the CMaaS solution integration activities complete? 2. Has the CMaaS solution successfully undergone adequate test and evaluation (e.g. Level-1 and Level-3 IT&E)? 3. Have all functional and operational requirements been satisfied? 4. Are there any open high-level operational risks with the solution? 5. Have operational users been identified and trained on the CMaaS solution? 6. Is the CMaaS solution ready for operational use?
ADE 3 (Program)	Q3FY22	1. Have all CDM solutions successfully completed their respective operational readiness reviews? 2. Has adequate OT&E of all deployed CDM solutions been completed and are there any identified limitations to effectiveness, suitability, interoperability, or cybersecurity?
Federal Dashboard Release 3 Functional	TBD	1. Is the Federal Dashboard Release 3 solution ready for CMaaS integration?

Decision Event	Date	Associated DSQs
Acceptance		2. Are the program requirements (functional) user-validated, traceable, measurable, testable and achievable?
Agency Dashboard Release 4 Functional Acceptance	Q4FY17	1. Is the Agency Dashboard Release 4 solution ready for CMaaS integration? 2. Are the program requirements (functional) user-validated, traceable, measurable, testable and achievable?
Federal Dashboard Release 4 Functional Acceptance	Q1FY18	1. Is the Federal Dashboard Release 4 solution ready for CMaaS integration? 2. Are the program requirements (functional) user-validated, traceable, measurable, testable and achievable?
FOC (Program)	4QFY22	1. Are all CDM operational capabilities deployed? 2. Has end-to-end IT&E been completed where possible? 3. Has OT&E identified any limitations on solution operational capabilities?

2.2 Decision Support Matrix

The full CDM Decision Support Matrix (DSM) is included in ANNEX 8: along with the CDM Integrated Evaluation Framework (IEF). Figure 2-1 provides an illustration of the DSM for reference purposes.

	A	B	C	S	T	U	V	W	X	Y	Z
1											
2	**Evaluation Objective**	**Systems Requirements and T&E Measures**		**CMaaS TO 2A ORR (1QFY16)**						**CMaaS TO 2B ORR (1QFY16)**	
3	**Evaluation Area / System Capability Categories**	**Requirements Document Reference**	**Description**	**1. Are the CMaaS solution integration activities complete?**	**2. Has the CMaaS solution successfully undergone adequate test and evaluation (e.g. Level 1 and Level 3 IT&E)?**	**3. Have all functional and operational requirements been satisfied?**	**4. Are there any open high-level operational risks with the solution?**	**5. Have operational users been identified and trained on the CMaaS solution?**	**6. Is the CMaaS solution ready for operational use?**	**1. Are the CMaaS solution integration activities complete?**	**2. Has the CMaaS solution successfully undergone adequate test and evaluation (e.g. Level 1 and Level 3 IT&E)?**
4	**Requirements Statements**										
5	1. The Continuous Diagnostics and Mitigation (CDM) program shall provide capabilities to enable situational awareness of asset management (Phase 1) in Federal Information System Management Act (FISMA) reportable systems in the following Tool Functional Areas, as noted in the CDM/CMAAS BPA.	CDM ORD v2.0 Section 3.4 (Requirements Statements)	TOOL FUNCTIONAL AREA 1 - HARDWARE ASSET MANAGEMENT The Hardware Asset Management (HWAM) Function is to discover unauthorized or unmanaged hardware on a network. Requirements for Operational Effectiveness Discover the actual state of all D/A Hardware Assets on the network, collecting attributes to allow determination of compliance to the desired state and report actual state, desired stated, and defect checks via Dashboard capability to appropriate parties.	KCG / Mantech Level 1 IT&E; Level 3 IT&E (to include Pilot) (Possible)	KCG / Mantech Level 1 IT&E; Level 3 IT&E (to include Pilot) (Possible)	KCG / Mantech Level 1 IT&E; Level 3 IT&E (to include Pilot) (Possible)	KCG / Mantech Level 1 IT&E; Level 3 IT&E (to include Pilot) (Possible)	KCG / Mantech Level 1 IT&E; Level 3 IT&E (to include Pilot) (Possible)	KCG / Mantech Level 1 IT&E; Level 3 IT&E (to include Pilot) (Possible)	BAH Level 1 IT&E; BAH Level 3 IT&E (to include Pilot) (Possible)	BAH Level 1 IT&E; BAH Level 3 IT&E (to include Pilot) (Possible)
6		CDM ORD v2.0 Section 3.4 (Requirements Statements)	TOOL FUNCTIONAL AREA 2 - SOFTWARE ASSET MANAGEMENT The Software Asset Management (SWAM) Function is to discover unauthorized or unmanaged software configuration items (SWCI) in IT assets on a network. Requirements for Operational Effectiveness Discover the actual state of all D/A Software Assets on the network, collecting attributes to allow determination of compliance to the desired state and report actual state, desired stated, and defect checks via Dashboard capability to appropriate parties.	KCG / Mantech Level 1 IT&E; Level 3 IT&E (to include Pilot) (Possible)	KCG / Mantech Level 1 IT&E; Level 3 IT&E (to include Pilot) (Possible)	KCG / Mantech Level 1 IT&E; Level 3 IT&E (to include Pilot) (Possible)	KCG / Mantech Level 1 IT&E; Level 3 IT&E (to include Pilot) (Possible)	KCG / Mantech Level 1 IT&E; Level 3 IT&E (to include Pilot) (Possible)	KCG / Mantech Level 1 IT&E; Level 3 IT&E (to include Pilot) (Possible)	BAH Level 1 IT&E; BAH Level 3 IT&E (to include Pilot) (Possible)	BAH Level 1 IT&E; BAH Level 3 IT&E (to include Pilot) (Possible)
		CDM ORD v2.0 Section 3.4	TOOL FUNCTIONAL AREA 3 - CONFIGURATION MANAGEMENT	KCG / Mantech Level 1 IT&E;	KCG / Mantech Level 1 IT&E; Level 3 IT&E (to	KCG / Mantech Level 1 IT&E;	KCG / Mantech Level 1 IT&E;	KCG / Mantech Level 1 IT&E;	KCG / Mantech Level 1 IT&E;	BAH Level 1 IT&E; BAH Level	BAH Level 1 IT&E; BAH Level 3 IT&E (to

Figure 2-1 - CDM Decision Support Matrix

2.3 Integrated Evaluation Framework (IEF)

"Meaningful metrics are required to answer the DSQs. The IEF is a structured approach to define measures necessary to thoroughly evaluate system performance, understand limitations, and determine if trained operators can employ the system to accomplish their mission.

An IEF takes technical and operational measures and matches them with capability releases. An IEF provides an overarching theme by linking the DSQs to the data needed to answer them and the test activities and scenarios needed to produce the data. An IEF also provides a link between requirements, measures, and associated test events. Finally, a good IEF will measure the system and identify the capabilities and limitations of a system throughout the acquisition life cycle."[16]

The CDM Test Team and the OTA are working together with support from the CDM PMO and Solution Providers to develop a comprehensive IEF. It is a work-in-progress, with the starting point being the initial SEP that the OTA will develop and update. The current version of the OTA's SEP addressing OE, OS, interoperability, and cybersecurity is presented here in ANNEX 8.[17] Since Level 1 and Level 3 IT&E are aimed at using test cases to demonstrate compliance with hundreds of Dashboard and CMaaS functionality requirements (derived from Attachment I of the Dashboard RFQ and Attachment N of the BPA, respectively), the focus of the IEF coincides with that of the OTA SEP – CDM system operational performance requirements and identification of test and information sources supporting their resolution. The structure of the IEF adheres to the template presented in Figure 2-2.

The CDM IEF is a living document that will be maintained by the CDM Test Team and the OTA. Challenges to developing a focused and precise IEF include fluid TO and program milestone schedules and uncertainties associated with planned testing events (e.g., objectives, environment, and data availability). Conceptually, the content of the IEF necessarily would expand when Phase 2 and Phase 3 capabilities are incorporated into the framework. Some reductions, dropping secondary MOPs and/or data elements, could be anticipated, however, as the CDM mission and supporting processes become more clearly defined and as the OTA, Operational Tester, and CDM Test Team become more cognizant of data collection realities.

At this time, a complete and comprehensive IEF is not available for the following reasons:

- Mission threads, vignettes, scenarios, and use cases have not been fully developed by the CDM PMO or Solution Providers
- Beyond what has been integrated into this TEMP's depiction of the OTA SEP, performance criteria identified in the CDM ORD and referenced in this TEMP and DSM have not yet been associated definitively with operational objectives, desired effects, or specific measures. An effort to complete this activity is ongoing.
- Associated target milestones for CDM TO streams and the CDM schedule are in the process of being updated. The current DSM contains the information presently available; however, that information is expected to change.

---

[16] DHS Acquisition Instruction Guidebook #026-06-001-01: Interim Appendix L TEMP v2.0, February, 2017

[17] Augmented with the incorporation of CTPs listed in ANNEX 4 and other revisions noted in ANNEX 8

The CDM Test Team and OTA are working with the Dashboard and CMaaS Solution Providers and CDM PMO to identify test events and associated technical and operational measures.

COI	MOE/S/C	MOP	Data Element/Type	Test Event	Notes
The statement of the Critical Operational Issue (COI) is derived from the ORD.	Associated with each COI are a number of supporting MOEs, MOSs, or MOCs. These are linked to source ORD requirements and CTPs.	Subordinate to each MOE, MOS, or MOC are a number of Measures of Performance (MOPs). If there are any related (KPP) or other quantitative requirements from the CDM ORD, they follow the MOP statement. Each MOP also has at least one associated data element.	This column provides the specific data item(s) supporting each MOP (typically "Number of" or "Time of/for"), and/or characterizes the non-testing means for obtaining such data (e.g., documentation reviews, interview summaries, or survey results).	Indicates whether a data element will be based on OT (OA, IOT&E, or FOT&E), Developmental Test (DT) (Level-1, Level-2, or Level-3 IT&E), Early Deployment (ED), Special Test Event, or some combination thereof. Special test events include events like Maintenance Demonstrations and Disaster Recovery Demonstrations.	Provides additional information to clarify the associated COI, MOE/S/C, MOP, Data Element/ Type, or Test Event.

Figure 2-2 – CDM Integrated Evaluation Framework (IEF) Template

2.3.1 IT&E Opportunities

As a complement to the integrated evaluation framework, the CDM Test Team and OTA have identified the following opportunities (Figure 2-3) for IT&E based on BPA ordering options, components tested and DHS T&E authority for the different levels of risk reduction testing. IT&E of CMaaS activity is focused on evaluation of the integrated CMaaS solution and should[18] not include IT&E of tools and sensors incorporated into the CMaaS provider's solution, since all CMaaS tools/sensors are COTS products available on the GSA Schedule.

[18] IT&E of tools/sensors is not planned. Verification of CDM requirements satisfied by individual COTS components will be accomplished through inspection, analysis, and/or demonstration of Solution Provider capabilities. This language was chosen to allow flexibility to evaluate tools and/or sensors in specific cases if needed. This language was suggested at the request of DHS Director T&E.

BPA Ordering Options (Funding Source)	CDM Segment(s) Tested		IT&E Opportunities		
			Level-1 IT&E	Level-2 IT&E	Level-3 IT&E
DHS Process (DHS-Funded)	Segments	(A) Tools and Sensors only	No	No	No
		(B) CMaaS Integration only	Yes	No	No
		(C) Agency CDM Dashboard only	Yes	No	No
		(D) Federal Dashboard only	Yes	TBD*	Yes*
	Segment Integration	A+B	Yes	TBD*	No
		A+B+C	Yes	TBD*	Yes*
		A+B+C+D	Yes	TBD*	Yes*
		C+D	Yes	No	No
DHS IT&E	**Agency Only**		*** See footnote [19]**		
* The PMO has the authority to order additional government testing per the BPA and may choose to do so if needed and resources are available (see footnote 19)					

Figure 2-3 – Opportunities for CDM IT&E based on BPA Ordering Options, Segment(s) Tested, and DHS T&E Authority for the Different Levels of Risk Reduction Testing

19 Other than CDM Test Team V&V, OTA and operational tester observation at to-be-specified Agencies, as allowed by contract, no DHS funded OT&E will be conducted outside of DHS (i.e., in the Agency environment) unless requested by the Agency, approved by DHS OGC, and with required documentation. DHS DOT&E only has authority within DHS. Legal concern that would have to be resolved through DHS OGC includes legislation contained in Title 31 U.S.C. and Title 44 U.S.C.

Section 3: Integrated Test and Evaluation Activities

3.1 Integrated T&E Process

The IT&E process for CDM consists of leveraging the T&E capabilities of the CMaaS and Dashboard Solution Providers, CDM Test Team, OTA, and Agency activities in a cohesive and collaborative manner to accomplish effective and efficient T&E from multiple perspectives. This process leverages an IT&E preparation process leading up to the testing activity followed by up to three levels of IT&E followed by additional OT&E if necessary. This process is executed independently for each CDM TO. There will be multiple instances of this process executing concurrently. The processes are designed to integrate with the program's Integrated Master Schedule (IMS). The preparation process consists of CDM Test Team and OTA technical documentation review, which serves to aid the PMO in their management of the TOs, as well as enabling the effective planning of IT&E by the CDM Test Team and OTA for each TO. The following Task Orders are have been awarded and are currently going through this IT&E process:

- Federal and Agency CDM Dashboard – Metrica Team Venture (MTV)
- CDM Phase 1 (Hardware Asset Management (HWAM), Software Asset Management (SWAM), Configuration Settings Management (CSM), and Vulnerability Management (VUL)) CMaaS Integration
    - TO 2A – Knowledge Consulting Group (KCG) ManTech
        - DHS
    - TO 2B – Booz Allen Hamilton (BAH)
        - Department of Energy (DOE)
        - Department of the Interior (DOI)
        - United States Department of Agriculture (USDA)
        - United States Department of Transportation (USDOT)
        - Office of Personnel Management (OPM)
        - Veterans Affairs (VA)
        - Executive Office of the President (EOP)
    - TO 2C – Northrup Grumman Corporation (NGC)
        - Department of Commerce (DOC)
        - Department of Justice (DOJ)
        - Department of Labor (DOL)
        - Department of State (DOS)
        - U.S. Agency for International Development (USAID)
    - TO 2D – BAH
        - Health and Human Services (HHS)
        - Treasury Department
        - National Aeronautics and Space Administration (NASA)
        - GSA
        - Social Security Administration (SSA)
        - United States Postal Service (USPS)
    - TO 2E – Hewlett Packard Enterprise Services (HPE)
        - Department of Education (ED)

- Environmental Protection Agency (EPA)
- Housing and Urban Development (HUD)
- Nuclear Regulatory Commission (NRC)
- National Science Foundation (NSF)
- Small Business Administration (SBA)

- TO 2F – KCG Mantech
  - Services:
    - American Battle Monuments Commission (ABMC)
    - Broadcasting Board of Governors (BBG)
    - Council of the Inspectors General on Integrity and Efficiency (CIGIE)
    - Corporation for National and Community Service (CNCS)
    - Court Services and Offender Supervision Agency (CSOSA)
    - Millennium Challenge Corporation (MCC)
    - National Endowment for the Arts (NEA)
    - National Endowment for the Humanities (NEH)
    - Peace Corps
    - Selective Service System (SSS)
    - Tennessee Valley Authority (TVA)
    - U.S. Africa Development Foundation (USADF)
  - Financial:
    - Consumer Financial Protection Bureau (CFPB)
    - Commodity Futures Trading Commission (CFTC)
    - Farm Credit Administration (FCA)
    - Federal Housing Finance Agency (FHFA)
    - Federal Trade Commission (FTC)
    - Overseas Private Investment Corporation (OPIC)
    - Pension Benefit Guaranty Corporation (PBGC)
    - U.S. Railroad Retirement Board (RRB)
    - U.S. Securities and Exchange Commission (SEC)
    - U.S. International Trade Commission (USITC)
  - Regulatory:
    - Consumer Product Safety Commission (CPSC)
    - Defense Nuclear Facilities Safety Board (DNFSB)
    - U.S. Department of State Office of Inspector General (DOSOIG)
    - Equal Employment Opportunity Commission (EEOC)
    - Federal Election Commission (FEC)
    - Federal Energy Regulatory Commission (FERC)
    - Federal Maritime Commission (FMC)
    - International Boundary and Water Commission (IBWC)
    - U.S. Merit Systems Protection Board (MSPB)
    - National Archives and Records Administration (NARA)
    - National Capital Planning Commission (NCPC)
    - National Labor Relations Board (NLRB)

- National Transportation Safety Board (NTSB)
- Office of Government Ethics (OGE)
- U.S. Office of Special Council (OSC)
- Occupational Safety & Health Review Commission (OSHRC)
- Privacy and Civil Liberties Oversight Board (PCLOB)
- Postal Regulatory Commission (PRC)
- United States Postal Service Office of the Inspector General (USPSOIG)

The testing model for future phases will follow previous task orders, as appropriate, with modified DHS SELC gate reviews included across agencies.

TO 2A includes only DHS components and as such is the primary focus of IT&E activities for the CDM Test Team and OTA.

3.1.1 IT&E Preparation Process

After a TO is awarded, the CDM IT&E Preparation Process (IT&E-PP) begins, which includes design/document evaluation cycles and DHS PMO decision points that determine whether the proposed testing is adequate or whether the proposed testing methodology and schedule are appropriate.

The CDM PMO has numerous milestones at which a decisive path to testing will be chosen for each solution. These decisions can be based on the CDM PMO's risk criteria, including any/all, but not limited to the following:

- Solution provider's previous CMaaS implementation(s)
- Similarity to previously implemented solution(s) by the same Solution Provider
- Similarity to previous environment(s) by the Solution Provider
- Implementation of new technologies
- Data and results of Solution Provider testing conducted to date
- Solution provider's TEMP, requirements traceability matrix (RTM), design documents, solution specific test plans, progress reports
- Analyses and recommendations from the CDM Test Team
- CDM Test Team IV&V findings
- OTA LOOs
- Agency T&E infrastructure and formal T&E policy
- Threat and vulnerability assessments
- Other risk factors

For solutions that reduce risk to a level the CDM PMO is willing to accept, further steps to optimize the available resources may include financial considerations and random or representative sampling of solutions/environments.

NOTE: The Solution Provider is contractually required to conduct testing and support government directed testing as per the TO award, to share test plans, cases, and results with the

CDM Test Team and PMO and to incorporate PMO requests for modification, consistent with the TO. The PMO expects that each Agency will participate in the necessary reviews, V&V, and acceptance testing (AT) according to the guidelines of their organization.

Within TO award +30 days[20], the Solution Provider will deliver their TEMP (which must comply with the DHS 026-06-001-01 Guidance), hereafter referred to as the "Solution Provider's TEMP," covering the portion[21] of the TO for which they will be deploying a solution. The CDM Test Team will then review the Solution Provider's TEMP and make recommendations to the CDM PMO (within 14 days[22]). If the CDM PMO rejects the Solution Provider's TEMP, it is returned to the Solution Provider with comments to be addressed. This cycle is then repeated until the CDM PMO accepts the Solution Provider's TEMP. Once the TEMP has been accepted, the CDM PMO decides to either continue with the IT&E-PP or proceed directly to the TRR.

If directed to continue with the IT&E-PP, at TO Award +60 days[23] the Solution Provider delivers their TEMP, design documents, and test-related documentation including solution-specific RTM, and draft test plan(s) for planned test events. This milestone aligns to the tailored SELC SDR. The CDM Test Team will review the documentation, interact with the Solution Provider as necessary, and deliver a design Deficiency Report Document (DRD) along with recommendations to CDM PMO in support of the solution's SDR. At the SDR, the CDM PMO assesses solution design completeness towards meeting requirements and the provider's readiness to develop the solution. If the solution passes the SDR, the Solution Provider continues with the roll out of proposed CDM tools/sensors preceding through the next SELC gates, including SRR and Production Readiness Review (PRR), and the CDM PMO then decides to either continue with the IT&E-PP or proceed directly to the TRR.

The IT&E-PP continues as the Solution Provider makes any design adjustments contained in the DRD and continues integration development efforts. As the Solution Provider nears design completion, they will begin to prepare solution specific test plans for review. These solution specific test plans may not be ready for review for the TRR. When they are ready, the CDM Test Team will evaluate the test plan(s) and submit a Test Plan Recommendation Report to the CDM PMO. If the CDM PMO rejects the test plan, it is returned to the Solution Provider for modifications. Once the CDM PMO accepts the Solution Provider's test plan, the CDM Test Team provides a solution technical analysis report, which includes recommendations to the PMO.

If the solution specific test plans are submitted, reviewed, and accepted before the TRR, then the TRR also acts as the Level-1 ITRR[24] for Solution Provider-executed testing; otherwise, a separate Level-1 IT&E TRR will be required. This milestone corresponds to the SELC's SRR. At the TRR, based on input from the Solution Provider, the Agency, and the CDM Test Team (if

---

20 Or as specified within the task order award
21 This terminology is used because multiple Solution Providers may be awarded for each TO issued
22 Or as specified within the task order award
23 Or as specified within the task order award
24 Integrated (TRR) is identified as the review held prior to IT&E execution. For the CDM Program, the Developmental Test Readiness Review (DTRR) is used to assess readiness for a specific IT&E event, and can be combined with the TRR for Level-1 IT&E.

applicable based on the CDM PMO's previous decisions for testing) the CDM PMO, in collaboration with the Agency, decides whether to proceed into CDM Level 3 IT&E Integration Testing, proceed with Solution Provider Integration and Testing with the Agency conducting V&V (no DHS IT&E) and AT, or that the solution is not ready for integration and testing (and how to proceed). Figure 3-1 depicts the CDM IT&E-PP.

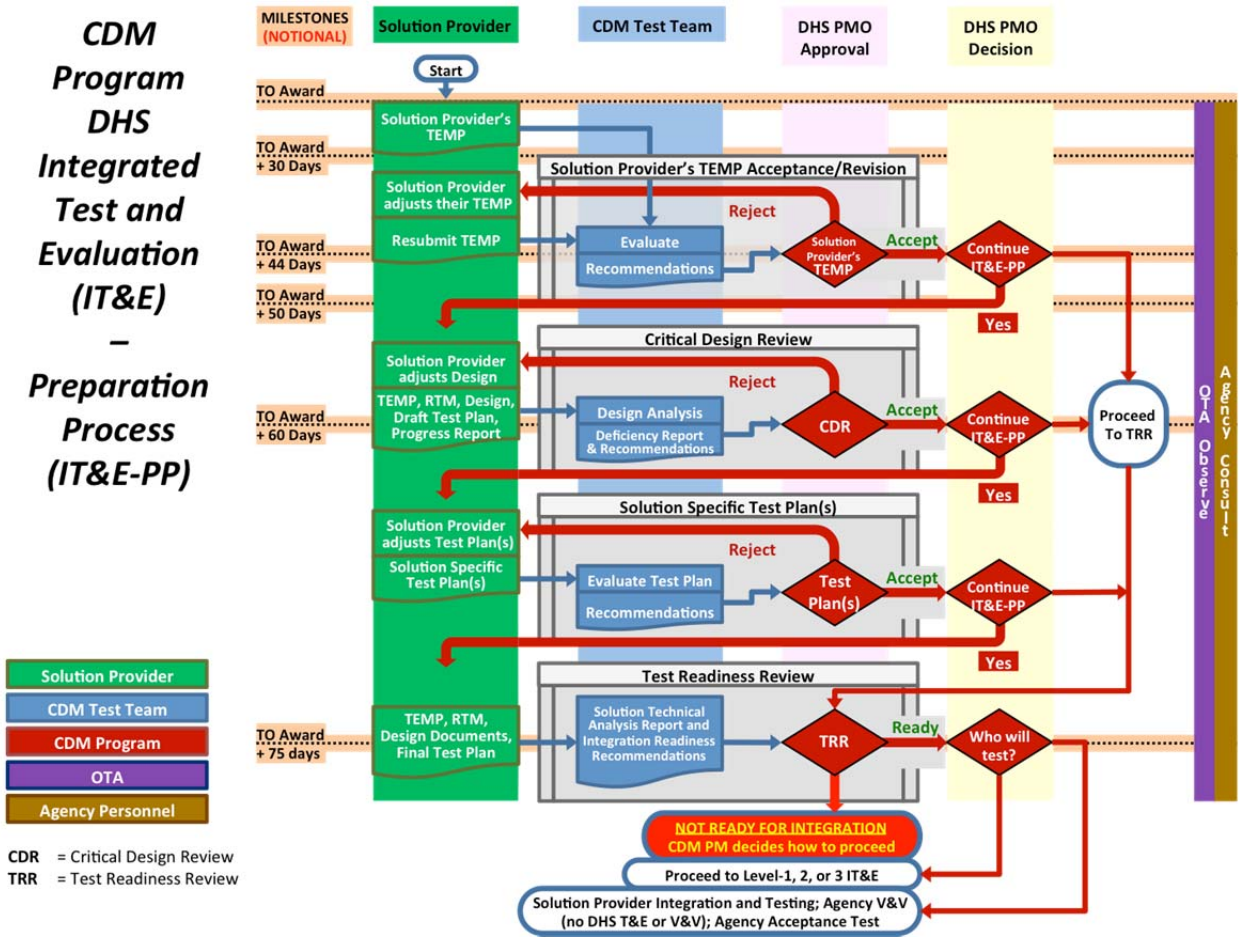


Figure 3-1 - CDM IT&E Preparation Process (IT&E-PP)

3.1.2 IT&E Execution and Reporting Process

Following the IT&E-PP, each CDM solution TO will go through the CDM IT&E Execution and Reporting Process depicted in

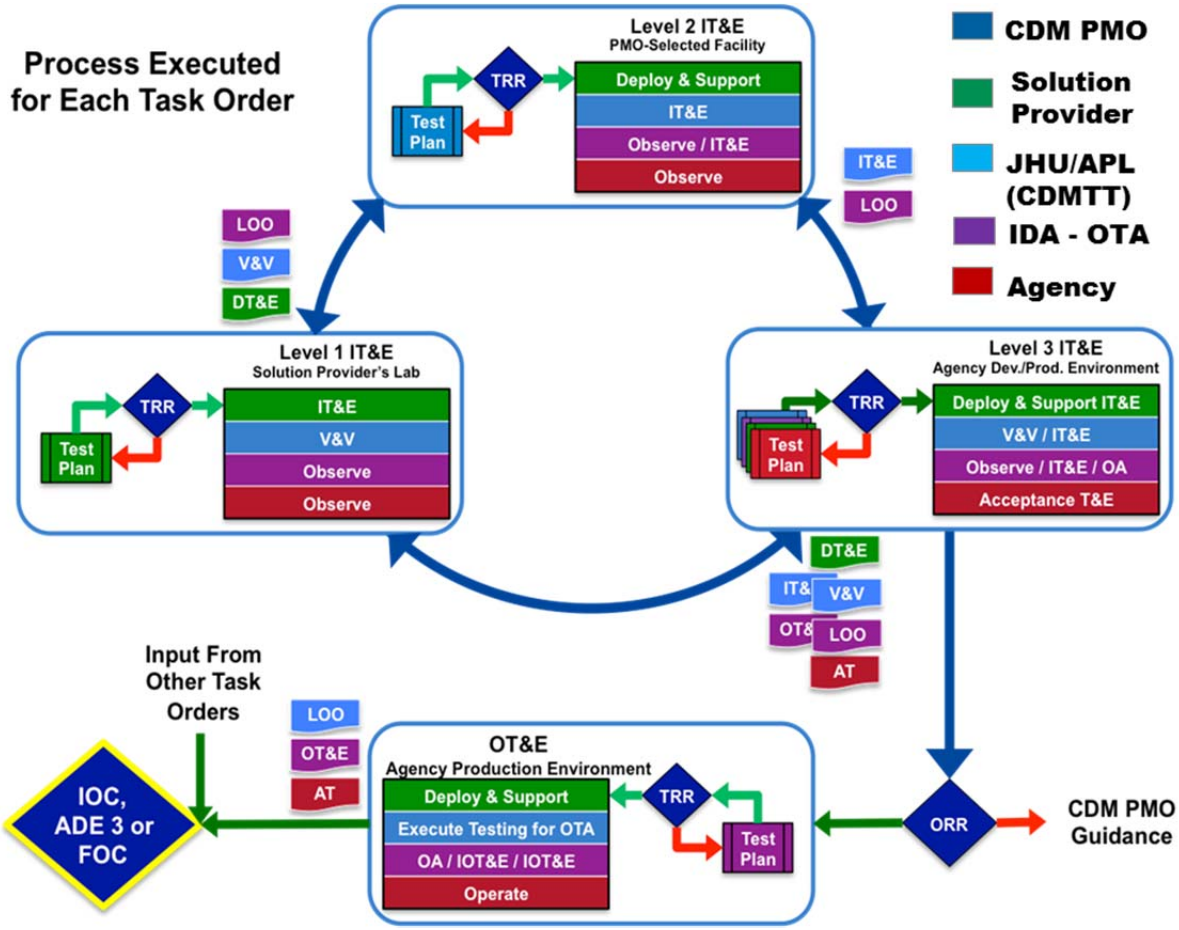


Figure 3-2. This process, hereafter referred to as the CDM IT&E process, illustrates that CDM T&E activities go through a cycle of IT&E as determined by the CDM PMO with CDM Test Team and OTA feedback.

Following the IT&E-PP for each TO, the Solution Provider is responsible for executing Level-1 IT&E activities. During this activity, other T&E stakeholders perform their V&V or observation functions and all information is provided to the PMO for evaluation. If additional risk reduction is necessary, the CDM PMO may request that the CDM Test Team conduct Level-2 IT&E. If additional testing is not necessary, the PMO may decide that the Solution Provider may proceed, with Agency concurrence and cooperation, to conduct testing in the Agency environment (Level-3 IT&E). The cycle of Level-1, 2, and 3 activities may continue as long as the PMO determines is necessary in order to ensure adequate risk reduction leading into operational deployment of the system. Following operational deployment marked by the ORR milestone, the OTA may conduct additional OT&E.

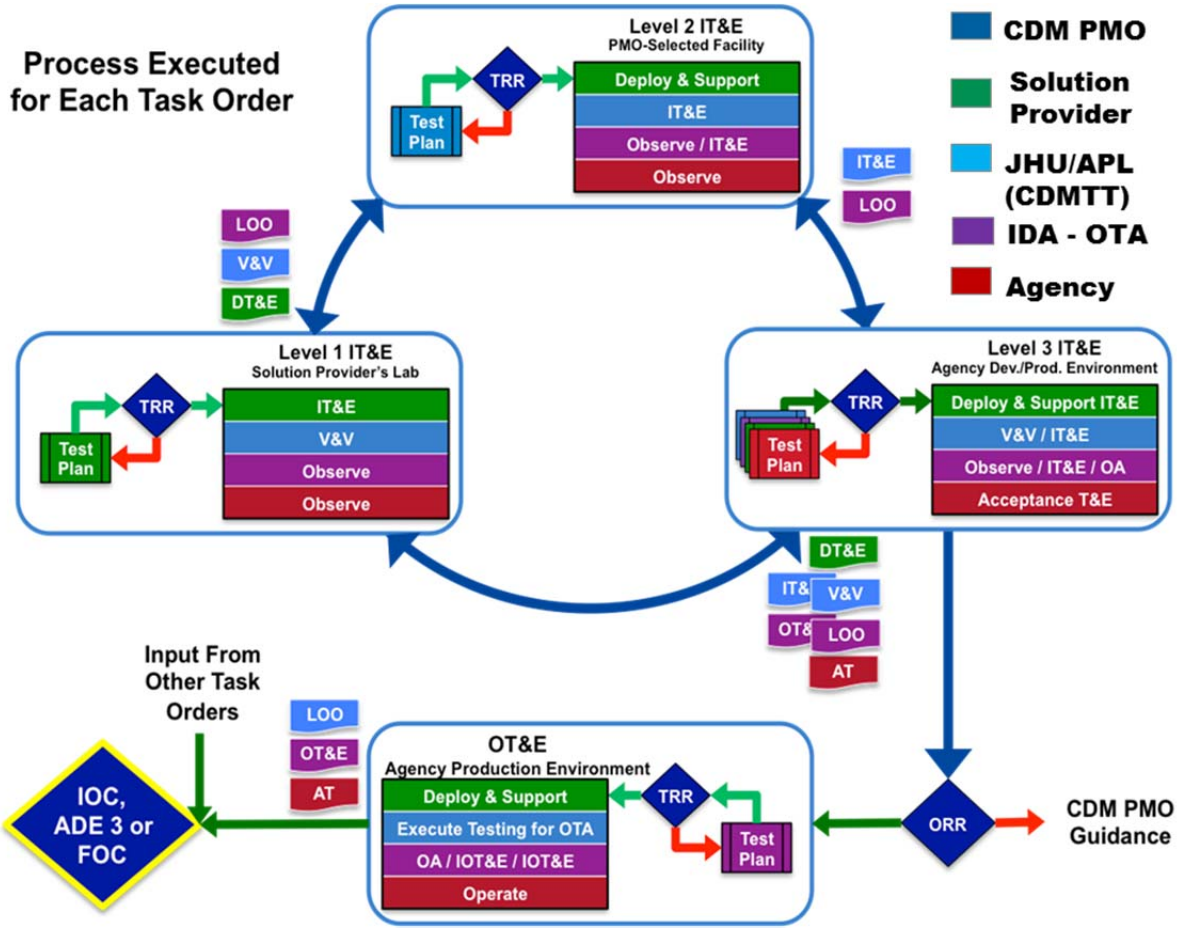


Figure 3-2 - CDM IT&E Execution and Reporting Process

3.1.3 IT&E Process References

Additional information on the CDM Test Team's IV&V activities can be found in the CDM Test Team IV&V Strategy. This living document accompanies the TEMP and is made available to all CDM T&E WIPT stakeholders in order to ensure that they understand how their T&E activities will be the subject of IV&V on behalf of the CDM PMO.

Additional information describing how the OTA will conduct an independent evaluation of the CDM system can be found in the OTA's SEP.

3.1.4 IT&E Assumptions, Limitations, and Constraints

In order for this IT&E process to function effectively, the following assumptions are made (below). If these assumptions are incorrect, the CDM Test Team may have to conduct additional mitigation activities.

- The CDM Test Team and the OTA assume that the Solution Providers will conduct testing activities as directed in their respective TOs
- The CDM Test Team and OTA assume that the CDM PMO will provide systems engineering support as required to understand program requirements

- The Solution Provider(s) and/or integrator(s) will support any applicable Level-2 and Level-3 IT&E as directed by the CDM PM
- CMaaS provider's proposal adequately clarified all requirements addressed in the CMaaS BPA, CMaaS TO Attachment N, demonstrated by their award on the BPA, thereby eliminating the need to further refine any requirements
- The dashboard integrator's proposal adequately clarified all requirements addressed in the Dashboard RFQ (December 2013) Attachment I, demonstrated by their award on the BPA, thereby eliminating the need to further refine any requirements.

The following limitations and constraints have been identified with respect to this IT&E process:

- The CDM Test Team and OTA only have insight into testing activity within DHS and its Components or at Solution Providers' facilities. The CDM Test Team and OTA do not have authority to conduct IV&V or T&E in non-DHS Agency environments
- Use of CDM in the operational environment is not well defined. Operational use cases and other program-level architecture products have not been developed
- CDM operational requirements (from the ORD) were not included in the CMaaS TO SOW contractual language; However, due to their traceability from Attachment N to the ORD the CMaaS Providers are required to operationally test their solutions.
- This TEMP section provides a framework for IT&E activities that encompass many Agencies and cannot address specific Agency operational processes. According to Title 31 U.S.C., a single agency cannot fairly be expected to judge overall effectiveness in programs that cross agency lines. The intent is to make best effort in reducing risk to the PMO who, per OMB memo 10-28 is responsible for "overseeing the government-wide and agency-specific implementation" of this system-of-systems
- The current delivery framework allows for Agencies to purchase against the CDM BPA using Agency internal funding. In this case, DHS-directed CDM IT&E is not authorized and not within the scope of the CDM appropriation to perform; therefore, there is no case in which DHS will either offer or accept a request to help an Agency that directly purchased CMaaS tools from the BPA
- Objectives for Level-1 IT&E are not clearly articulated in Solution Provider TOs which will likely result in differences in expectation of Level-1 IT&E between Solution Providers and the T&E community.

3.2 Level-1 IT&E

3.2.1 Description

Level-1 IT&E is any test activity conducted by the Solution Provider in their lab environment. The approach used in Level-1 IT&E will vary and be defined by each Solution Provider. Level-1 IT&E applies to both CMaaS and Dashboard elements. All Level-1 IT&E activity will be within scope of CDM Test Team IV&V and OTA observation.

The CDM Test Team will review the Solution Provider's processes, methodologies, plans, technical documentation, observe testing, analyze their data and results, and review their reports. These activities collectively support a comprehensive IV&V of the each CDM solution, which

will include technical and functional requirements verification, issue/risk analysis, and an assessment of operational readiness to the greatest extent possible.

Level-1 IT&E activities will be conducted for each Phase of CDM.

3.2.1.1 Dashboard Level-1 DT&E

Dashboard integrator-executed Level-1 DT&E includes several activities such as dashboard unit-level testing, M&S and acceptance testing. In addition to these test activities, design review and test support activities are within scope of Level-1 DT&E.[25] It is expected that there will be multiple releases of the CDM Dashboards (Federal and Agency) and therefore multiple Level-1 Dashboard IT&E events.

During Level-1 DT&E, the Dashboard integrator plans and executes their testing activities and delivers results to the CDM PMO and CDM Test Team. During this level, the CDM Test Team will also track the status of program-wide requirements, identify and assess solution-specific technical/functional requirements, track risks/issues and identify gaps in dashboard Level-1 DT&E (if applicable). The OTA is also authorized to participate in these reviews and observe testing activities along with the CDM Test Team. Upon completion of dashboard integrator-directed IT&E, additional Level-1 DT&E involving dashboard components becomes the responsibility of the CMaaS providers. The CMaaS provider(s), with the support of the dashboard integrator, continues on with Level-1 DT&E integration and systems-level IT&E activities (which include dashboard components).

Upon completion of the dashboard Level-1 DT&E, the CDM Test Team will present IV&V results and recommendations to the CDM PMO in a IV&V report. Recommendations will be based on the satisfaction of the acceptance criteria[26] and DSQs developed by the CDM Test Team and approved by the CDM PMO. The acceptance process consists of a formal review of IV&V results, review of dashboard integrator's test design and rigor, prior solution testing and deployment history (if applicable), and a comprehensive solution-based risk assessment. Recommended actions can include correction of issues and/or retesting by the providers (more Level-1 DT&E), additional testing executed by the CDM Test Team for the CDM PMO (execution of Level-2 IT&E), or direct transition to Level-3 IT&E in a Agency environment determined by the CDM PMO. Evaluation of the dashboard integrator's activities will be coordinated with dashboard-related IT&E conducted by the CMaaS provider so that a complete dashboard assessment can be presented to the CDM PMO.

Federal Dashboard Level-1 DT&E component and initial integration testing for the Federal Dashboard and CDM Agency dashboard will take place at the Federal dashboard integrator's facility. Follow-on dashboard Level-1 DT&E will occur at the CMaaS providers' labs.

---

25 Additional IT&E utilizing Dashboard components (such as CMaaS integration or systems testing) is the responsibility of the CMaaS Solution Provider per the CMaaS TO and SOW.

26 To be generated as part of the iterative pre-testing activities with the dashboard integrator

3.2.1.2 CMaaS Level-1 DT&E

All CMaaS solution Level-1 DT&E will occur at the CMaaS Solution Providers' facilities. Level-1 DT&E for CMaaS integration and systems testing involving CDM Agency dashboard components will occur at the CMaaS Solution Providers' facilities as they are responsible for dashboard integration per the TO and SOW.

Level-1 DT&E covers all CDM segments that the CMaaS Solution Provider incorporates into their solution. The CMaaS Solution Provider is responsible for verifying that the tools and sensors selected for their solution collectively satisfy program requirements, taking into consideration the limitations and interactions with any pre-existing tools on Agency networks as part of the CMaaS solution. The CMaaS provider is responsible for ensuring interoperability between their solution and the CDM Agency dashboard(s), as well as ensuring interoperability of the CDM Agency dashboard(s) with the Federal Dashboard.[27] In addition to these test activities, design review and test support activities are within scope of CDM Level-1 DT&E.

Solution provider-executed DT&E will include a broad range of testing activities such as unit-level testing, segment testing, M&S, integration testing, systems testing, cybersecurity testing, and concludes with acceptance testing. The details of this activity will be defined in the Solution Provider's TEMP and test plans once accepted by the CDM PMO. If the solution specific test plans are presented for the first time at the Level-1 TRR, a review/acceptance procedure will take place before proceeding to the TRR.

During Level-1 DT&E, the Solution Provider(s) executes testing activities, verifies requirement satisfaction, and delivers the results to the CDM PMO and CDM Test Team. The CDM Test Team will review the Solution Providers' processes, methodologies, plans, technical documentation, witness Solution Provider testing, analyze their data and results, and review their reports. These activities collectively support a comprehensive IV&V of each CDM solution, which will include technical and functional requirements verification, issue/risk analysis, and an assessment of readiness for operational implementation.

CDM PMO recommended actions as a result of Level-1 DT&E can include (1) correction of issues and/or retesting by the providers (more Level-1 DIT&E), (2) additional testing executed by the CDM Test Team for the CDM PMO (execution of Level-2 IT&E), (3) Level-3 IT&E in a Agency environment, or (4) proceeding directly to the PRR. If the CDM PMO recommends option (4), then Level-1 DT&E aligns with the SELC OTRR and the IT&E PRR aligns with the SELC ORR. If the CDM PMO recommends option (3) and the SELC OTRR requires a Limited Production Review (LPR), then Level-3 testing aligns with the SELC OTRR and the IT&E PRR aligns with the SELC ORR. The SELC OTRR will include technical testing evaluation results from prior milestone reviews and the completed elements of the Level-1 testing designated for the targeted Solution Provider.

27 CMaaS TO, Section 2.5.1.4, 2.5.3, 2.5.9, and 2.5.11.1; Component testing the Agency Dashboard and the Federal Dashboard are the responsibility of the dashboard integrator.

During Level-1 DT&E, the CDM Test Team will also track the status of program-wide technical/functional requirements, identify and assess solution-specific technical/functional requirements, risks/issues and identify gaps in Level-1 DT&E (if applicable). The OTA is also authorized to participate in these reviews and observe testing activities prior to any additional OT&E. The applicable Agency(s) for each solution is/are strongly encouraged to engage at this stage to ensure smooth transition to later IT&E stages and/or solution deployment.

3.2.2 Objectives

The primary objective of Level-1 DT&E is to reduce risk prior to deployment of CDM capabilities in the operational environment. This includes verification of applicable functional requirements, demonstration of tool / sensor capabilities and thorough T&E of the integration of system components. Level-1 DT&E should also include, to the greatest extent possible, early evaluation of operational capabilities, interoperability testing, ST&E, and OS (reliability, maintainability, availability, usability, etc.) assessment.

A secondary objective of Level-1 DT&E is to assess the T&E capabilities of the Solution Provider. Given that the CDM program encompasses many concurrent activities, the CDM Test Team does not have the resources available to witness and IV&V all Solution Providers' activities. Analysis of Solution Providers' technical capability will be one factor in the CDM Test Team's IV&V sampling plan.

3.2.2.1 Cyber T&E Objectives

Cyber T&E objectives for Level-1 DT&E largely focus on compliance-based cybersecurity and the associated T&E required to achieve the ATO or similar requirement for deployment, integration, and T&E in Agency environments (pre-deployment or full-production). The CDM Test Team would like to see additional risk-based cybersecurity T&E such as penetration testing, however Solution Provider TOs do not specify this activity. Additional cyber T&E objectives may be added for Level-1 DT&E (or follow-on testing) based on the results of the cybersecurity threat assessment, which is currently in progress. The CDM Test Team expects to IV&V cybersecurity T&E activities conducted by the Solution Providers during Level-1 to the greatest extent possible. The Program plans to use the NCCIC NCATS (National Cybersecurity Assessment and Technical Services) team to conduct penetration testing of the Federal CDM dashboard. In addition, the team is planning table top exercises.

3.2.2.2 Interoperability T&E Objectives

Interoperability T&E objectives in Level-1 DT&E include demonstrating interoperability between CMaaS and the CDM Agency Dashboard, between CMaaS and a notional Agency environment (simulated in the Solution Provider's Lab), and if possible, interoperability between the object level CDM Agency Dashboard and the summary level Federal Dashboard.

3.2.2.3 Modeling and Simulation Objectives

There are no specific M&S objectives for Level-1 DT&E other than in the implementation of the Solution Provider's test environment. The lab environment should model and/or simulate characteristics of the actual operational environment(s) that the Solution Provider is expected to deploy their solution into. The Solution Providers may conduct additional M&S, however

specific objectives are not directed per their TO, at least for Phase 1. For Level-1 DT&E, verification, validation, and accreditation (VV&A) are the responsibility of the Solution Provider, however their VV&A activities will be evaluated by the CDM Test Team's IV&V.

3.2.2.4 Operational Test Objectives

Since the Solution Providers are not given the CDM ORD-level operational requirements and since the functional requirements, which they do have, were not derived from the ORD, the amount of operational evaluation that can be completed in their environment may be limited. All Level-1 IT&E activities are available for OTA observation. The CDM Test Team will also consider operational implications when conducting IV&V in their effort to produce an assessment of readiness for operational implementation.

3.2.3 Data Collection

Data collection and validation will be planned and executed according to the Solution provider executing the Level-1 DT&E activity. All data collection will be made available to the CDM Test Team and OTA for IV&V and Operational Assessment (OA) purposes if applicable.

3.2.4 Deficiency Report Generation

The Solution Provider executing the Level-1 DT&E activity is responsible for collecting and tracking deficiencies (e.g. issues, deficiencies, or defects) discovered during their Level-1 DT&E activity. Methods for report generation and tracking will vary based on each Solution Provider. The CDM Test Team and the OTA may also track additional deficiencies for IV&V or operational assessment purposes, respectively.

3.2.5 Test Limitations

General limitations of Level-1 DT&E include using one synthetic test environment to assess readiness for deployment of a solution in multiple different operational environments. The impact of this limitation (level of risk) will depend on the Solution Provider's process and facilities. The level of risk (if any) will be included in the CDM Test Team's IV&V report delivered to the PMO following Level-1 DT&E activity.

3.2.6 Reliability Growth

CDM technologies rely extensively on established COTS products with known high reliabilities. The expectation, as articulated in the CDM ORD, is that the CDM system readily will satisfy its reliability requirements (measured in terms of Mean Time Between Operational Mission Failures (MTBOMF)) upon deployment into Agency environments. Figure 3-3 notionally portrays this situation, with the 200 hours MTBOMF reliability objective applying to each of the constituent CDM system elements, i.e., Federal Dashboard, Agency CDM Dashboard, CMaaS Integration Element, and Sensor/Tool. There is no anticipation that out-of-the-box reliability levels will be deficient and thus there are no plans to "grow" reliability from their initial values up to ORD-prescribed requirements. Accordingly, no reliability growth curves have been developed for the CDM system or constituent elements, a reliability, availability and maintainability rational for CDM was[28].

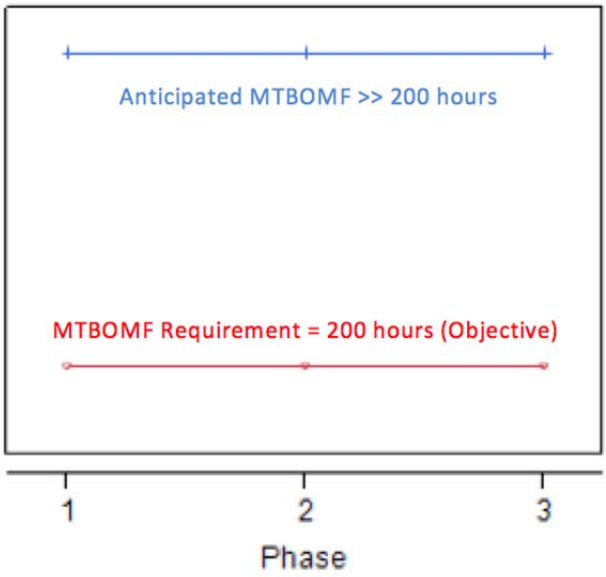


Figure 3-3 – Notional MTBOMF of COTS Product with Initial High Reliability

CDM reliability performance will be monitored, recorded, and tracked throughout DT&E and OT&E events. If early tests and deployments indicate that there are unanticipated reliability shortfalls, a formal reliability growth developmental program will be constituted and a system reliability growth curve will be constructed. Methods guiding these activities will follow the principles and practices described in standard reliability growth documentation.[29,30,31] Figure 3-4

[28] *Reliability Availability Maintainability Rationale – Performance Plan, DHS Office of Cybersecurity & Communications, NSD, January 2016*

[29] *DoD Guide for Achieving Reliability, Availability, and Maintainability*, U.S. Department of Defense, Washington DC, 2005.

[30] *Department of Defense Handbook: Reliability Growth Management*, MIL-HDBK-189C, U.S. Department of Defense, Washington DC, 2011.

illustrates a hypothetical reliability growth that could be imposed for a particular CDM system element if needed.

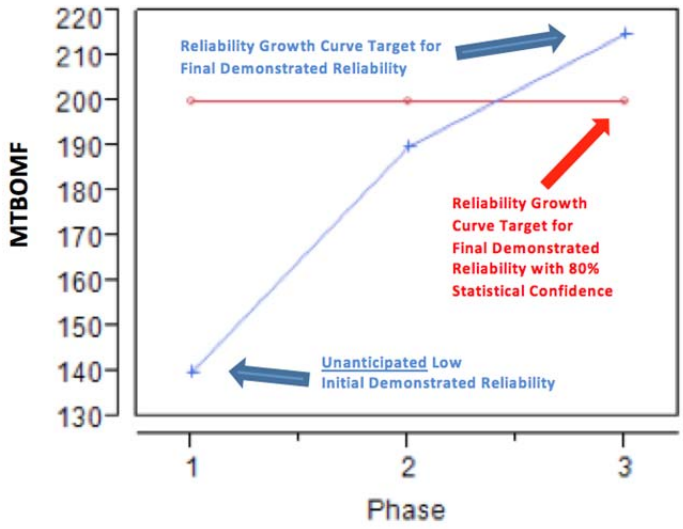


Figure 3-4 – Hypothetical MTBOMF of Selected CDM Element with Initial Low Reliability

3.2.7 Level-1 DT&E Reporting

Level-1 DT&E activities will include the following reporting:

- Solution Provider test report
- CDM Test Team IV&V report (if selected based on IV&V sampling plan)
- OTA LOO and/or OA Report (if applicable)

3.3 Level-2 IT&E

3.3.1 Description

OPTIONAL—Execution of Level-2 IT&E is one of the most powerful risk reduction options at the CDM PMO's disposal but may require a contract modification for the Solution Provider and additional financial resources.

In Level-2 IT&E, the CDM Test Team conducts testing on behalf of the CDM PMO to satisfy gaps identified in Level-1 IT&E and/or Level-3 IT&E. Typically, Level-2 is expected to follow Level-1 IT&E, but it is possible that a Level-3 IT&E event, such as a Pilot in the Agency

[31] *Reliability Growth: Enhancing Defense System Reliability*, National Research Council, Panel on Reliability Growth Methods for Defense Systems, Committee on National Statistics, Division of Behavioral and Social Sciences and Education, The National Academies Press, Washington DC, 2015.

environment, will follow Level-1 IT&E. In this case, Level-2 IT&E may follow if the PMO decides it is necessary.

Level-2 IT&E will focus on verifying technical/functional specifications, confirming issue resolution, reducing program risks, gathering additional data, and ensuring readiness to proceed to either Level-3 testing or to the PRR as directed by the PMO. Level-2 IT&E takes place in a location determined by the CDM PMO. Possible locations can include but are not limited to DHS, the Solution Provider's test environment, or other cyber range environment.

Follow-on options after Level-2 IT&E include Level-3 IT&E testing in the Agency environment (e.g. Pilot) or proceeding to the PRR. Level-2 IT&E may include a Type-2 Technology Demonstrator[32] exercised in a systems-level test, which will include test objectives of demonstrating applicable KPPs and/or CTPs assessing solution risk.

The CDM Test Team is responsible for developing the Level-2 IT&E Test Plan, which is presented at a Level-2 TRR. The CDM Test Team will coordinate this plan with the DOT&E, the OTA, Agency representatives, Solution Providers, and other stakeholders as necessary. The CDM test team is responsible for coordinating, configuration and setup, verifying, base-lining the environment, writing and executing test procedures, and collecting and analyzing data. The CMaaS Solution Provider is responsible for deploying/configuring their solution to the test environment. It is highly encouraged that the CDM OT&E community including DOT&E, the OTA, and Agency representatives witness and/or contribute to Level-2 IT&E activities enabling all T&E stakeholders to gather data and produce assessments. Upon completion of Level-2 IT&E, the CDM Test Team will deliver a solution-specific Level-2 IT&E report containing the test results regarding requirements verification, issues/risks, results of AT, and readiness for Level-3 IT&E and/or solution deployment.

3.3.2 Objectives

The overarching objective of Level-2 IT&E fill gaps identified in Level-1 DT&E and/or Level-3 IT&E activities and to serve as a risk identification and reduction activity. Level-2 IT&E events will be tailored for specific objectives and could include broad systems end-to-end testing or be very targeted on a specific capability or characteristic of a CDM solution.

3.3.2.1 Cyber T&E Objectives

Specific objectives for Level-2 IT&E will be defined based on the gaps and risk identified by the CDM Test Team and OTA from other testing activity. Level-2 IT&E can employ the use of cyber ranges to support a broad range of cyber T&E objectives if necessary.

---

32 Type-2 Technology Demonstrators are used as part of a Program to develop, refine or verify requirements, explore technologies, and develop and/or verify designs throughout the Obtain phase. Type-2 demonstrations are typically conducted in simulated or laboratory (non-operational) environments, but may be conducted in controlled operationally relevant environments to obtain operational/user feedback. Type-2 demonstrations may be part of a program's contractor or DT effort. The scope of a Type-2 Demonstrator must be within the scope of the MNS/ORD, with objectives included in the Acquisition Program Baseline (APB). If part of a DT effort, the Type-2 Demonstrator objectives must be documented in the TEMP and DT Plans before evaluation. The scope and plan for Type-2 technology demonstrators is part of the APB approval at ADE-2A.

3.3.2.2 Interoperability T&E Objectives

Specific objectives for Level-2 IT&E will be defined based on the gaps and risk identified by the CDM Test Team and OTA from other testing activity. Level-2 IT&E can employ the use of virtualized computing technology and cloud computing enabling the creation of a multi-Agency test environment permitting interoperability assessment.

3.3.2.3 Modeling and Simulation Objectives

Specific objectives for Level-2 IT&E will be defined based on the gaps and risk identified by the CDM Test Team and OTA from other testing activity. Level-2 IT&E can employ the use of virtualized computing technology and cloud computing enabling modeling and simulation of CDM and/or external Agency systems or capabilities if required.

3.3.2.4 Operational Test Objectives

In the spirit of IT&E, planning and execution of Level-2 IT&E will be a collaborative effort between all interested T&E stakeholders. The CDM Test Team will lead the planning effort, however the OTA, Solution Provider, and Agency representatives are encouraged to assist in planning and execution so as to enable data collection and assessment from all perspectives. This includes the possibility of a Level-2 IT&E event to be used for operational evaluation if the OTA so chooses.

3.3.3 Data Collection

Specific data collection requirements for Level-2 IT&E will depend on event objectives and will be coordinated by the CDM Test Team with all T&E stakeholders via the CDM Program T&E WIPT.

3.3.4 Deficiency Report Generation

The CDM Test Team will track any deficiencies identified during Level-2 IT&E according to the process defined in Section 1.6.3.1. Feedback from all participating stakeholders will be leveraged in the prioritization of deficiency reports.

3.3.5 Test Limitations

There are no program-wide limitations with Level-2 IT&E. Specific limitations for each Level-2 IT&E event will be identified in the Level-2 IT&E Test Plan authored by the CDM Test Team. This plan will include feedback from all stakeholders collaborating in the planning and execution of this specific event.

3.3.6 Reliability Growth

The content in Section 3.2.6 applies to Level-2 IT&E.

3.3.7 Level-2 IT&E Reporting

Level-2 IT&E Reports will include the following:

- Level-2 IT&E Test Report authored by the CDM Test Team
- OTA LOO and/or OA Report (if applicable)
- Solution Provider Level-2 observations and/or test report (if applicable)
- Agency observations and/or test report (if applicable)

3.4 Level-3 IT&E

3.4.1 Description

Level-3 IT&E will test the solution capabilities as they are deployed in the Agency environments. The nature of the testing environment may vary from Agency to Agency and may include testing in Agency test networks and/or Agency operational networks. Solution Provider Pilot events are considered a Level-3 IT&E activity. Participants and observers in this stage may include the Agency personnel, CDM PMO personnel, the CDM Test Team, the CDM OT&E community, the Solution Providers, and other stakeholders as necessary.

The test lead and the testing process used during this stage will be defined by the Agency but in many cases this role may be deferred to the Solution Provider by the Agency with CDM PMO oversight. With the Agency as the test lead, it is expected that they will conduct the testing necessary to accept (or reject) the solution (e.g. a user acceptance test). The CDM PMO may accept the IT&E and/or OT&E test role for testing conducted in the Agency environment if the CMaaS solution being implemented is DHS funded, upon request by the Agency, approved by the DHS OGC, and with required documentation. Factors influencing participating stakeholders and scope of Level-3 IT&E include the TO delivery framework, Agency network environment technical considerations, and prior IT&E results. In parallel to Agency conducted testing, the CDM Test Team will conduct IV&V similar to that in Level-1 IT&E. **There is no case in which DHS will either offer or accept a request to help an Agency that directly purchased CMaaS tools from the BPA.**

After the Agency completes their acceptance testing, the CDM Test Team will use all available data to assess the solution's readiness for operational implementation. This assessment will be delivered to the CDM PMO in an IV&V report along with the Agency's AT results. In the DHS implementation, the CDM Test Team will have complete access to all Level-3 IT&E activity and data. In deployments to other Agencies, the CDM Test Team may have minimal insight of Level-3 IT&E depending on specific Memorandums of Agreement (MOAs). Under these circumstances, data from prior IT&E will be used to support the readiness assessment with an applicable risk assessment included for specified Agencies.

3.4.2 Objectives

The overarching objective for Level-3 IT&E is to assess operational readiness of a specific CDM solution implementation in an operationally representative environment. Those collecting data, analysis and assessing readiness can include the receiving Agency, the Solution Provider, the CDM PMO, CDM Test Team, OTA, and/or potentially others.

3.4.2.1 Cyber T&E Objectives

Level-3 IT&E cyberspace T&E objectives include the verification of agency defined policy critical cybersecurity requirements defined by the receiving Agency as necessary for the CDM solution to receive their ATO or equivalent (e.g. compliance with the Risk Management Framework (RMF), verification of security controls, cybersecurity risk assessment etc.). Additional cybersecurity T&E objectives include verification of any additional cybersecurity requirements as defined by the CDM PMO, CDM Test Team, and the OTA. These additional cybersecurity requirements may be derived from DHS cybersecurity policy, the CDM cybersecurity threat assessment, and/or results from cybersecurity risk assessment activity. Cybersecurity objectives for specific Level-3 IT&E activities will be defined in the Level-3 IT&E test and/or assessment plans developed by each stakeholder participating in the event.

3.4.2.2 Interoperability T&E Objectives

The primary interoperability T&E objective of Level-3 IT&E is to assess interoperability of CDM solutions with Agency legacy software and hardware systems in operational or operationally representative environments. A secondary objective is to assess the interoperability between interconnected CDM systems developed by different Solution Providers (as applicable) (e.g. interoperability between an Agency CDM Dashboard and the Federal Dashboard). Specific interoperability T&E objectives will be defined in the Level-3 IT&E test and/or assessment plans developed by each stakeholder participating in the event.

Note: Since there are no program-wide architecture products that completely define system boundaries and interfaces, the CDM Test Team is heavily reliant each of the CMaaS Integrators to define their respective interoperability objectives and requirements through Agency interaction.

3.4.2.3 Modeling and Simulation Objectives

Modeling and simulation, in general, will be minimized in Level-3 IT&E as the primary goal is to test in an operationally realistic environment. However, if Level-3 IT&E is taking place in an Agency test environment or other isolated environment, M&S may be used to replicate scale and/or interfacing systems to the CDM solutions being tested (e.g. simulation of a Federal Dashboard during a CMaaS Pilot T&E activity in an Agency test enclave). Specific M&S T&E objectives will be defined in the Level-3 IT&E test and/or assessment plans developed by each stakeholder participating in the event.

3.4.2.4 Operational Test Objectives

Level-3 IT&E will begin to address operational test objectives. All stakeholders participating in a Level-3 IT&E event have the ability to define operational test objectives and bring them to the table during Level-3 event planning. The receiving Agency has primary authority as to what events are conducted and what data is collected in Level-3 IT&E as the test is being conducted in their environment. If permitted to participate (or observe) and collect data, the CDM Test Team will attempt to verify as many of the CDM operational requirements defined in the ORD as possible on behalf of the CDM PMO and share this analysis with the OTA and other members of the CDM T&E WIPT. If permitted to participate and collect data, the OTA may chose to

produce an OA associated with the Level-3 IT&E event against measures defined in the OTA SEP.

Specific operational T&E objectives will be defined in the Level-3 IT&E test and/or assessment plans developed by each stakeholder participating in the event.

3.4.3 Data Collection

Specific data collection requirements for Level-3 IT&E will depend on event objectives and will be coordinated by the receiving Agency with all T&E stakeholders via the CDM Program and Solution Provider-specific T&E WIPT.

3.4.4 Deficiency Report Generation

The Solution Provider will track any deficiencies identified during Level-3 IT&E according to the process defined in their Quality Management Plan and the CDM Test Team will track deficiencies in accordance with the process defined in Section 1.6.3.1. Feedback from all participating stakeholders will be leveraged in the prioritization of deficiency reports.

3.4.5 Test Limitations

The primary limitation associated with Level-3 IT&E is the lack of legal authority granted to the CDM Test Team and OTA in non-DHS Agency environments to witness testing activity and collect data without Agency approval. It is expected that Agencies receiving CDM solutions will permit the DHS CDM Test Team and OTA to participate in test events and collect data, however if such permission is not granted, an opportunity for data collection and assessment will be lost. The CDM Test Team and OTA will work with each Solution Provider and Agency through the T&E WIPT forum to discuss involvement in non-DHS Agency Level-3 IT&E activities.

Limitations associated with specific Level-3 IT&E events will be defined in the associated IT&E test plans developed by participating stakeholders. All limitations should be discussed and reviewed at the TRR preceding the Level-3 IT&E event.

3.4.6 Reliability Growth

The content in Section 3.2.6 applies to Level-3 IT&E.

3.4.7 Level-3 IT&E Reporting

Level-3 IT&E Reports will include the following:

- Agency acceptance, observations and/or test report
- Solution Provider Level-3 observations and/or test report
- Level-3 IT&E Test Report or IV&V report authored by the CDM Test Team (if applicable)
- OTA LOO and/or OA Report (if applicable)

3.5 OT&E Activities

There are three distinct types of OT&E activities addressed in this TEMP. The primary focus of this present section is on the OTA's directed program-level OT&E that follows DHS Instruction Guide 026-06-001-01.[33] This section also discusses potential roles for the OTA with Agency-directed test and assessment activities that may be undertaken after ORRs at individual Agencies (including DHS and non-DHS[34]) have been completed (e.g., to support Post Implementation Reviews (PIRs)). Pre-ORR testing events designated as "OT&E" by individual Agencies and solution providers, e.g., User Acceptance Tests, are addressed in this TEMP in the Level-3 testing sections.

3.5.1 Description

3.5.1.1 Scope

The OTA's dedicated OT will be conducted by the OTA independently from system developers and the PMO to evaluate system effectiveness, suitability, and cybersecurity in operationally realistic environments. OT&E will focus on demonstrating sustained mission performance and interoperability over extended periods of continuous employment conforming to CDM operating profiles.

The primary dedicated program-level CDM OT events, especially the comprehensive Initial Operational Test and Evaluation (IOT&E) and Follow-on Operational test and Evaluation (FOT&E), are anticipated to be conducted predominantly within components of DHS. Supporting precursor OT events, more limited scope Agency-level OAs, also will be conducted within DHS as well as possibly in non-DHS Agencies. The OTA will work with the PMO to identify test opportunities for providing pre-IOT&E insights on CDM operational performance (addressing limited portions of overall mission performance), subject to any constraints that may require Agency invitation, approval by DHS OGC, and requisite documentation.[35] To inform OT&E planning, the OTA will monitor Level-1, Level-2, and Level-3 testing, and any relevant exercises, demonstrations, M&S, and analyses. Section 3.5.3 describes the OTA's overall OT&E strategy.

All OTs will involve CDM operators and users executing CDM functions and missions within realistic operational environments. CDM system components that will participate in OT events include Agency sensors and tools,[36] CMaaS elements, Agency dashboards (across deployed

---

33 DHS Acquisition Instruction Guidebook #026-06-001-01: Interim Appendix L TEMP v2.0, February, 2017.

34 This broader use of the term "Agency" to encompass both DHS and non-DHS agencies adheres to the convention recently adopted by the CDM Program and followed in ORD 3.0.

35 DHS DOT&E only has authority within DHS. Legal concern that would have to be resolved through DHS OGC includes legislation contained in Title 31 U.S.C. and Title 44 U.S.C.

36 The individual sensors/tools comprising CMaaS solutions already have undergone evaluation as part of the process for being included in the CDM BPA and CDM required technical functionalities have been verified in DT&E. Their intrinsic technical capabilities are not the focus of OTs, but their contributions to and impacts on CDM system operational performance are within scope.

hierarchies), and the Federal dashboard. CDM interfaces to external user organizations (as identified in Table 1-1, e.g., DHS NCCIC) will be tested. Limited scope OT events will not necessarily examine the operational performance of the complete spectrum of CDM system components.

The OTA will evaluate CDM OE, OS, and cybersecurity.[37] OTA evaluations will build on the structure of the COIs and associated performance metrics identified in Section 3.5.2, and will address CDM Phase 1, Phase 2, and Phase 3 capabilities. The CDM IEF (Section 2.3) will be refined and expanded as additional details on CDM capabilities and operational processes emerge.

3.5.1.2 Operational Performance Aspects

Operational Effectiveness (OE) is the overall degree of a system's ability to provide desired capability when used by representative personnel in the environment planned or expected for operational employment of the system. CDM OE requirements encompass situational awareness of asset management (Phase 1), risk scoring of Agency IT assets and their individual defects via the Federal-level CDM dashboard (Phase 1), situational awareness of account management (Phase 2), capabilities to monitor Agency planning and response to incidents and contingencies (Phase 3), and capabilities to monitor the status of security and life cycle management (Phase 3). Associated KPPs appear in ANNEX 3.

A general definition of interoperability is the ability of systems, personnel, and equipment to provide and receive functionality, data, information, and/or services to and from other systems, personnel, and equipment, between both public and private agencies, departments, and other organizations, in a manner enabling them to operate effectively together.[38] From an IT perspective, interoperability is the ability of different operating and software systems, applications, and services to communicate and exchange data in an accurate, effective, and consistent manner.[39] The focus of both versions is on "different systems." Within the context of CDM, there are data transfers between individual elements constituent to the CDM system – between sensors/tools and Agency base dashboards, between Agency dashboards, and between Agency dashboards and the Federal dashboard. The requisite functionalities will be tested in DT&E and their contributions to CDM system operational mission performance will be measured in OTs. The effectiveness of interactions of CDM user groups external to the CDM system with the CDM system constitutes an interoperability issue and is portrayed under the OE heading in the current IEF. No interoperability KPP is defined in the CDM ORD.

Operational Suitability (OS) is the degree to which a system can be placed satisfactorily in use with consideration given to various relevant factors. The attributes explicitly addressed within the CDM ORD are system design, availability, reliability, maintainability, safety, staffing, human factors, environmental considerations, integrated logistics support, survivability, and

---

[37] Section 3.5.1.2 gives basic definitions of OE, OS, and cybersecurity applicable to the CDM system. Interoperability also is defined and, within the context of CDM, is related to OE.

[38] Memorandum of Agreement on Operational Suitability Terminology and Definitions to be used in Operational Test and Evaluation, Service Operational Test Agencies, October 2005

[39] E-Government Act of 2002

training requirements. Reliability and availability KPPs are prescribed in the updated ORD and recorded in ANNEX 3 of this TEMP. The ORD provides same basic definitions of reliability, availability, and maintainability (RAM) terminologies, but formal Failure Definition and Scoring Criteria (FDSC) and definitive interpretations of RAM data items await development. Precise FDSC definitions will be formulated by the OTA and the T&E WIPT prior to any OTA OT event.

Cybersecurity is the body of technologies, processes, and practices designed to protect networks, computers, programs, and data from attack, damage, or unauthorized access. To support the acquisition decision authorities understanding of operational cybersecurity risks, OT&E must include relevant tests of cybersecurity.[40] One cybersecurity KPP appears in the updated CDM ORD and is listed in ANNEX 3 of this TEMP.[41]

3.5.2 COIs

Beginning with the broad OE, OS, and cybersecurity categories, the OTA developed seven subordinate COIs to guide its examination of CDM operational performance capabilities through OT&E (see ANNEX 4, the OTA's System Evaluation Plan (SEP),[42] or the CDM ORD[43]). The purpose of the COIs is to facilitate assessments and evaluations of CDM's ability to provide desired capabilities to CDM operators and users. The OTA, subject to CDM user approval, may refine their particular COIs for testability purposes and as necessary. Procedures defining modification to COIs will be identified through CDM program change management guidelines, to be developed as needed. Modified and approved COIs will be documented in future versions of the ORD, TEMP, and OTA SEP.

Error! Reference source not found. shows how at the overview level the seven COIs relate to specific CDM operational performance metrics – MOEs, MOSs, and MOCs originally prescribed by the OTA and subsequently adopted in the CDM IEF (presented in Section 2.3). The full text versions of the COIs, MOEs, MOSs, and MOCs appear in the OTA SEP, with COIs listed as questions and measures presented as statements. These are linked to specific enumerations of ORD-specified requirements and KPPs. Translations to subordinate issues and MOPs appear in the IEF and will be further refined and detailed in individual OTA test planning documents. Neither the metrics nor the subsidiary MOP counterparts detailed in the IEF should be interpreted as rigid prescriptions of definitive "pass-fail" requirements. Rather they should be considered as starting points for analytical discussions relating demonstrated OT&E performance to operational impacts for fielded systems.

---

40 Procedures for Operational Test and Evaluation of Cybersecurity, Memorandum, Director, Operational Test and Evaluation (now Director, Office of Test and Evaluation), 15 October 2015.

41 The OTA will interpret the cybersecurity KPP (listed in ANNEX 3 as subordinate to the 'respond' function) to be associated with the cybersecurity COI (listed in ANNEX 3 as part of the 'Protect' function).

42 Operational Test Agent's System Evaluation Plan for the Continuous Diagnostics and Mitigation (CDM) Program, Institute for Defense Analyses, Document D-5199, February 2015.

43 CDM ORD 2.0 and 3.0 officially accepted and endorsed the COI statements initially developed by the OTA (which were refinements to those appearing in ORD 1.0 and associated discussions in the accompanying text).

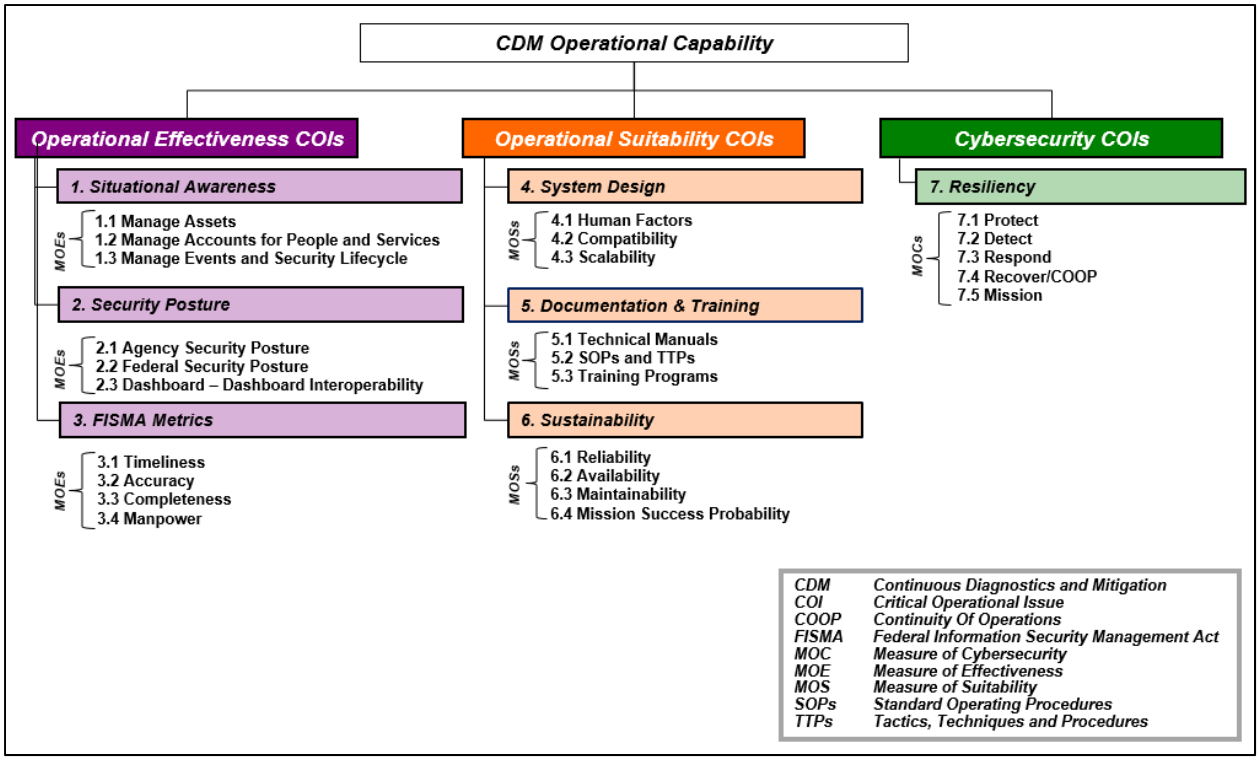


Figure 3-5 – CDM COIs and Associated MOEs, MOSs, and MOCs

3.5.3 OT&E Strategy

3.5.3.1 Planned OT&E

The specific locations for OT&E testing and data collection will coincide with the physical sites where the CDM systems and interfaces are operationally situated. OT&E testing and data collection will be conducted in accordance with detailed test plans and governing MOAs.

The OTA will plan, conduct, and report on two types of program-level DHS-centric OT&E events: major OTs, i.e., IOT&E (planned to comprehensively address all of the COIs per the OTA SEP) and FOT&E (if needed to address any unresolved COIs), that directly support CDM milestones and/or decision events, and limited scope (in the extent of represented CDM systems and/or their functionality) OAs conducted to reduce program risk. The OTA also will participate, when invited and in various test planning and test monitoring roles, in Agency-level designated OT events supporting Agency risk reduction, Agency PIRs, and informing broader CDM performance issues. OTA participation (planning and data collection) will be structured around ongoing Agency activities and OTA intrusion will be minimal. OTA objectives will be to obtain early indications of CDM system operational performance capabilities and to assist in the development of data collection and analysis methods supporting future OT&E. The OTA will build upon its participation in non-DHS OT activities to foster prospects for expanding the representation of non-DHS Agencies in formal program-level OT&E.

In addition to access limitations, OTA involvement in Agency controlled testing will be constrained by the extent of OTA resources. Important factors will include the degree to which

data collection supporting direct KPP assessments can be automated (e.g., via CDM dashboards) and the willingness of Agencies and their personnel to respond to survey instruments and participate in interview sessions. Conclusions drawn from an individual Agency's data will be specific to that Agency. In some circumstances, broader inference may be supportable at a qualitative level, e.g., when all tested Agencies demonstrate the attainment of a subject KPP with high confidence.

To the extent permissible and feasible, the OTA also will observe Level-1, Level-2, and Level-3 test events and activities as a means of gleaning operational performance insights and developing insights for OT&E planning. This may include interactions with the CDM Test Team, DHS Components, and Agencies – encompassing IV&V, pre-deployment activities, and acceptance testing. OTA attendance of CDM program reviews and regular engagement with the CDM Test Team will facilitate the identification of specific events amenable to OTA monitoring and some degree of participation (e.g., construction of operationally based use cases and scenarios). OTA documentation of testing results conceivably could complement OT assessments if conducted in representative OT environments.

3.5.3.2 Configuration Descriptions and OT&E Objectives

OT&E events will test operationally deployed production configurations of CDM systems. Segments of the CDM system that will participate in OTs include Agency sensors and tools, CMaaS elements, Agency CDM dashboards (across deployed hierarchies), and the Federal dashboard (active and standby sites in either their initial or final configurations). Also included will be all associated operators, users, and required logistical support personnel and equipment (per the CDM Integrated Logistics Support Plan (ILSP)[44]). In every OT&E event, resident CDM functionalities and supporting processes will be exercised (e.g., CDM sensors and tools will monitor operationally deployed computers, laptops, printers, and other HW/SW objects). Consistent with the planned scope of an OT&E event, processes integral to the performance of CDM capabilities will be observed and evaluated by the OTA (including controlled injections of network defects to assess the capability of CDM to detect those defects). For IOT&E and FOT&E events involving the CDM Federal dashboard, and earlier OAs as feasible, interfaces with one or more of the oversight user organizations and cybersecurity analysis groups identified in Table 1-1 will be tested.

For OAs, the extent of the CDM system participating in any event and the tested functionality will be limited to what can be addressed reasonably at that stage of the acquisition timeline. The primary objective will be to conduct *some* opportune and informative operationally relevant testing, vice waiting for a critical mass of CDM assets to be deployed and for a comprehensive examination of some major portion of the COIs to be undertaken.

The particular objectives to be associated with individual OT&E events will evolve as the CDM acquisition program matures. The OTA will develop a detailed test plan for each OTA-directed OT&E event, prescribing test objectives and mappings to OTA constructed measures and documenting traceability from KPPs and COIs. The IEF will guide detailed test planning for

[44] Integrated Logistics Support Plan (ILSP) for CDM, Version 1.2, 30 September 2014

addressing specific OE, OS, and cybersecurity objectives.[45] The OTA is not expecting to utilize any M&S in its OT&E.[46] CDM system reliability evaluations will be based on performance observed in individual test events, with potential aggregation across test events and operational periods as appropriate. Per the rationale given in Section 3.2.6, there is no anticipation of using reliability growth models to estimate or project reliability performance.

3.5.3.3 Data Collection and Deficiency Report Generation

As described in Section 1.5.2.3, the Operational Tester is responsible for the execution of OT&E events (including dry runs), including ensuring compliance with test set-up and execution rules, recording and collecting prescribed quantitative and qualitative descriptive data, and distributing and collecting operator/user survey questionnaires.

The parent Agency in which the OT&E event is being conducted will generate defect/deficiency reports (DRs)[47] for CDM system failures and problem areas identified during testing. The OTA and the CDM Test Team will track deficiencies as part of their assessment procedures. Feedback from all participating stakeholders will be leveraged in the prioritization of DRs.

3.5.3.4 OT&E Events

3.5.3.4.1 Notional Timeline of OT&E Events

Figure 3-6 is a notional timeline of OT&E events grouped by the individual sets of phased program capabilities. It aligns with the more detailed Integrated Master T&E Schedule depicted in Figure 1-1.

---

45 Section 3.5.3.4 describes cybersecurity OT&E activities.

46 No CDM system performance M&S has been developed by the CDM PMO or any contactors, and the OTA has no plans to develop such. If any Level-2 testing emerges, M&S could be expected to be a critical element thereof, and the OTA would explore the prospects of monitoring conducted associated testing and analyses, as well as possibly further exploiting the M&S. Section 3.5.4 discusses some M&S-based studies of CDM risk scoring algorithms that, if pursued, could reduce program risk.

47 The terminology “defect” is common within technical testing settings; DHS MD-026-06 utilizes “deficiencies” within the context of an OTRR.

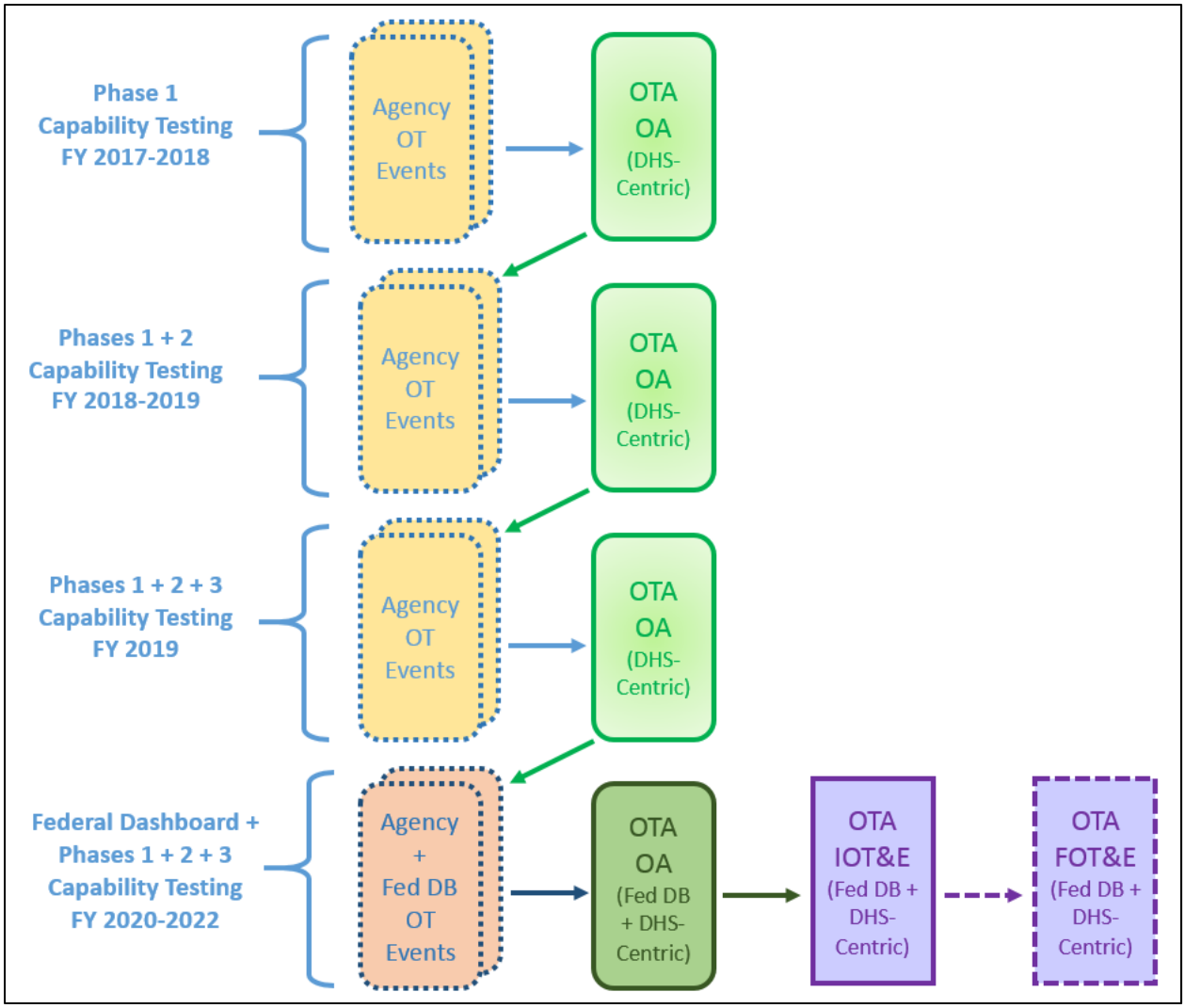


Figure 3-6 – Notional Timeline of CDM OT&E Events

Each set of phased capabilities has an associated dedicated OA to be conducted in DHS within one to two quarters after the attainment of DHS ORR. Entrance criteria for each OA include the ability to perform sustained multi-day operations that exercise the subject CDM capabilities. The OTA will design the OTA scope, following the construct of the IEF, to encompass OE, OS, and cybersecurity issues commensurate with the current state of deployments within DHS (see Section 3.5.3.4.3 for additional descriptions). The first OA will test Phase 1 capabilities, the second OA will test both Phase 1 and Phase 2 capabilities (including identified Phase 1 deficiencies), and the third OA will test all three phases of CDM capabilities (including deficiencies observed in the initial OAs). A fourth OTA will focus on CDM Federal dashboard performance in conjunction with all of the Phase 1, Phase 2, and Phase 3 capabilities. The demonstration of CDM operational performance capabilities in the OAs may reduce the scope required for the IOT&E event. After completion of the program-level IOT&E, unresolved operational performance issues and COIs will be addressed in the formal FOT&E to be executed by the OTA.

In addition to the OTA-led OT&E events, there are prospects for Agency-designated and Federal dashboard-centric OT events, spanning the multiple CDM TOs and of varying operational fidelity and OTA involvement (as described in Section 3.5.3.1). For each collection of CDM capabilities, these are depicted in Figure 3-6 as preceding the corresponding OTA's OA. Some, however, could follow afterwards (given the sequencing of the various CDM TOs relative to each other). Ideally, late stage Agency-based OT events would involve interactions with the Federal dashboard (as depicted in the bottom row of Figure 3-6).

3.5.3.4.2 Alignment with CDM Program IOCs and FOC

The ORD prescribes the attainment of CDM Program IOC and FOC dates via the degree of incremental CDM functional capabilities deployed across Federal networks:

- IOC 1: The CDM Program has made available to at least five Agencies the ability to manage their networks via Phase 1 capabilities, an Agency dashboard to receive and display Phase 1 data feeds, and *a Federal dashboard* to receive, aggregate and display summary data received from Agency dashboards and to transmit to Agencies policy and other requests, as appropriate.[48] [*emphasis added*]
- IOC 2: identical to IOC 1, with the addition of Phase 2 capabilities for determining who is on their networks.
- IOC 3: identical to IOC 2, with the addition of Phase 3 capabilities for determining what is happening on their networks.
- FOC: identical to IOC 3, with at least five Agencies *fully participating* in the CDM program [*emphasis added*].

For establishing the attainment of an IOC, the breadth of CDM presence within a given Agency can be minimal – *some* CDM sensors/tools must be represented in a portion of the Agency, and they must interface with *an* Agency CDM dashboard, which in turn interfaces with *a* Federal dashboard (Cyberscope or possibly an initial configuration of the CDM Federal dashboard). Attaining IOC, following the CDM-specific formal definitions, is not tantamount to establishing full operational capabilities for the subject Phase level. Indeed, as depicted in Figure 1-1, the OTA's Phase 1 OA will not be conducted until more than a year after IOC 1 was declared.

For establishing FOC, the representation of CDM within an Agency must be comprehensive – sensors/tools *throughout the entire envisioned extent of CDM within the Agency*, a *full complement of Agency CDM dashboards* (within a hierarchical structure, as needed), and reporting by *all* of the highest echelon Agency dashboard(s) to the (final configuration) CDM Federal dashboard.

---

[48] Per the ORD, Cyberscope is considered the Federal dashboard of record until the CDM Federal dashboard is operational (projected to occur in the second quarter of Fiscal Year 2018). Differences exist between the capabilities of Cyberscope and the Federal dashboard. The ORD does not apply to Cyberscope and only describes the dashboard capabilities. The interpretation taken in this TEMP is that the complete functionality of the CDM Federal dashboard will need to be demonstrated within the course of the OT&E program, but that the CDM PMO can determine the testing sequence for specific sets of operational performance requirements.

3.5.3.4.3 Scope of OTs

IOT&E and FOT&E events predominantly will involve monitoring extended periods of CDM system performance and supporting processes under live operating conditions – for sensors/tools and Agency CDM dashboards within DHS components, and for the CDM Federal dashboard (initial or final configuration, or Cyberscope before the deployment of CDM Federal dashboard configurations). Cybersecurity OT&E, as detailed in Section 3.5.3.5, will entail additional dedicated testing. Supplemental focused testing may be prescribed by the OTA to verify particular corrective actions taken in response to observed CDM system deficiencies, to augment limited test data obtained for particular operational performance metrics, or to demonstrate specific required CDM system capabilities that have been insufficiently exercised.

The specific compositions of DHS components and elements engaged in and the earlier OTA OAs and Agency-level OTs remains to be determined, and may vary from test to test. They will depend on the evolution of acquisition and deployment timelines, the representativeness of CDM system architectures, and the status of unresolved operational performance issues.

The installation of new hardware or software, the Federal level distribution of policy and scoring rule updates, and the Federal level execution of custom queries may occur serendipitously during live operations that overlap dedicated OT&E testing periods. The incidence of such events, however, likely will be low. To accommodate comprehensive OT&E, requisite events appropriate to the CDM phase under test will be injected in a controlled manner (introduced by OT&E test control, and coordinated with and approved by the involved operational organizations).

3.5.3.4.4 Operational Test Readiness Reviews

Before entering any OTA-led OT&E event, an OTRR will be conducted by the CDM PMO to determine readiness for proceeding to that particular test event. The review will consider OTA inputs on a number of subjects: readiness of operational and test personnel, dedicated test equipment, outstanding DRs, external agency readiness to participate, and overall system readiness for test. The CDM PMO will provide the data, documentation, personnel, and funding required for conducting the OTRR. For major OT&E events, i.e., IOT&E or FOT&E, the OTRR will be chaired by the NPPD CAE or designee.[49] For OAs, the OTRR will be chaired by the CDM Program Manager or designated PMO representative.

Transition to an OTA-led OT&E event will be determined during the corresponding OTRR and will be contingent upon successfully meeting designated appropriate subsets of the operational test entrance criteria (adapted in part from DHS MD-026-06) delineated below.

The master list of OTRR entrance criteria for IOT&E and FOT&E events includes:

- Formal authorization to operate (e.g., ATO, Interim ATO, Interim Authority To Test, or Restricted Authority To Connect) granted to all planned participating CDM operating and support systems, up to and including the Federal dashboard.

[49] Technical Review Guide, Version 2.0, DHS, Systems Engineering Center of Excellence, December 2015.

- No open category 1 information assurance severity reports; category 2 severity risks appropriately addressed in the Plan of Action and Milestones.
- DOT&E approval of the associated test plan document.
- Delivery of Level-1, Level-2, and Level-3 test reports and Agency-led OTs for preceding CDM testing.
- Demonstration during Level-1, Level-2, and Level-3 testing, to include supporting data, of compliance with CTPs and system functionality and performance requirements prescribed in program requirements documents.
- No open Priority 1 or Priority 2 DRs (all resolved or mitigated).
- No known DRs that could adversely impact safety or security, or could affect the accomplishment of CDM's critical or essential capabilities (within the planned OA/OT scope).
- All Priority 3 DRs have documented workarounds accepted and validated by the National Cybersecurity and Communication Integration Center (NCCIC) for operations.
- Requisite MOAs between DOT&E and CDM hosts and interfaces involved in testing are in place.
- As required to support specific planned test objectives, completed training for all O&M personnel across CDM echelons – Federal dashboard and Agency dashboards, sensors, tools, and CMaaS.
- Completed training for all test personnel and related data collectors.
- As required to support specific planned test objectives, CDM operating, maintenance and training documentation, to include the CONOPS and SOPs, are completed and provided to the OTA no less than 30 days prior to the OTRR.
- Accreditation and authorization[50] for any cybersecurity test activities and scenario injects planned to be utilized in the OT&E event (or in an associated IT&E event if the data collected will be used to support resolution of OT&E objectives).
- IV&V is completed for any planned incorporation of cyber range testing during the OT&E event (or in associated IT&E if the data collected will be used to support resolution of OT&E objectives). If data from the upcoming OT&E event are essential to completion of the IV&V process, the OTA will document the risk to the OT&E event and any ensuing program decision of proceeding based on the approved IV&V concept and analysis plan.
- The integrated CDM systems comprise production-ready equipment available in sufficient quantities to support the OT&E event, consistent with OT&E objectives.
- The CDM system configuration must be stable no less than 30 days prior to start of any OT&E activity.
- At least five Agencies must be participating in the CDM Program in accordance with the ORD-prescribed conditions defining attainment of the pertinent IOC/FOC status.
- Organizations actively participating in the IOT&E/FOT&E will include Agency sensors/tools, Agency dashboards in appropriate hierarchies, the Federal dashboard (final configuration), and designated CDM user groups, in accordance with minimum CDM representation requirements to be prescribed in the DOT&E-approved test plan.

[50] From the CDM PMO, DHS Risk executive, and other required personnel

- Resources are identified and are available, including funding, personnel (operational and test), and logistic support as outlined in the DOT&E-approved test plan.
- Resolution of any outstanding OT&E limitations critical to the execution of the planned OT&E.

For limited scope OAs, non-safety OTRR requirements may be relaxed provided that test objectives remain achievable. Specific acceptable deletions from the above master list of OTRR entrance criteria will be established no later than seven days prior to the scheduled OTRR.

3.5.3.5 Cybersecurity

This section presents the OTA's cybersecurity evaluation framework and serves as a possible foundation for developing the OTA's cybersecurity test plans for CDM OT&E.[51] The framework outlines cybersecurity testing activities, including Blue Team and Red Team participation,[52] and identifies measures for evaluating cybersecurity.[53] The current OTA structure is applicable to all CDM Program phases and future requirement and system modifications. It is anticipated that DHS user communities will authenticate the scoping of reference threats identified in the CDM Threat Assessment (once that assessment is finalized).

The Blue Team is a group of individuals that conduct operational network vulnerability evaluations and provide mitigation techniques to customers who have a need for an independent technical review of their network security posture. The Blue Team identifies security threats and risks in the operating environment, and in cooperation with the customer, analyzes the network environment and its current state of security readiness. Based on the Blue Team findings and expertise, they provide recommendations that integrate into an overall community security solution to increase the customer's cyber security readiness posture. Often times a Blue Team is employed by itself or prior to a Red Team employment to ensure that the customer's networks are as secure as possible before having the Red Team test the systems.

The Red Team, with authorization, emulates a potential adversary's attack or exploitation capabilities against an enterprise's security posture. The Red Team's objective is to improve enterprise Information Assurance by demonstrating the impacts of successful attacks and by demonstrating what works for the defenders (i.e., the Blue Team) in an operational environment.

The OTA's evaluation of cybersecurity (COI 7) will build on existing DHS and Agency ST&E, acceptance testing, and security risk assessment processes, leveraging these results in scoping the OTA's cybersecurity OT&E activities.[54] It also will draw upon the dedicated cybersecurity IT&E events shown in Figure 1-1, i.e., the Federal dashboard penetration testing scheduled towards the end of FY17 and the subsequent cybersecurity tests associated with each of the four following OAs spanning FY18 to FY22. In concert with the PMO, the OTA will participate in

---

51 Procedures for OT&E of Cybersecurity, DHS DOT&E Memorandum, 15 October 2015.

52 Committee on National Security Systems (CNSS) Instruction No. 4009, National Information Assurance (IA) Glossary, 26 April 2010.

53 Cyber Security Metrics and Measures, NIST Manuscript Publication, 2 March 2009.

54 The CDM PMO should ensure that relevant major cybersecurity findings for the DHS environment are shared, as appropriate, broadly across Agencies.

the planning for each of these individual cybersecurity tests. Additionally, the OTA will monitor the testing and report on results.

As described in Section 3.4.2.1, the Phase 1 OA cybersecurity scenarios will address the potential exfiltration of vulnerability data from Agency object-level database, as well as attacks aimed at degrading CDM performance to interfere with Agency situational awareness. For the Phase 2 OA, scenarios will examine attempts to corrupt CDM master user record data to mask inappropriate account privilege escalation, in addition to the deliberate degradation of CDM performance to undermine an Agency's ability to manage people and accounts. The scope of the Phase 3 OA scenarios will encompass CDM-based exploitations of network and physical access controls, and intentional degradations of CDM Phase 3 capabilities for purposes of compromising CDM's contributions to the Agency's management of what is happening on its networks. In conjunction with the last OA, a Recover/Continuity of Operations (COOP) exercise will be conducted to assess the capability of CDM and host network defenders to recover CDM mission effectiveness following successful adversarial attacks against CDM's subsystems and data.

As required to expand upon the cybersecurity IT&E events and to support comprehensive evaluation, supplementary Red/Blue Team and OT&E cybersecurity activities will be undertaken during the program-level IOT&E and FOT&E. These would include in turn a System Security or Blue Team preparation of the system against known vulnerabilities in conjunction with the ST&E, a Blue Team conducting cooperative testing and compliance auditing to identify CDM cyber deficiencies, and penetration testing (i.e., compliance validation) and threat-based offensive cyber operations against CDM systems and networks. Prior to penetration testing, opportunities would be provided to correct known deficiencies. An adaptive Red Team, operating under PMO approved Rules of Engagement (ROE), will be used in OT&E to portray threat activities against CDM. The Red Team may also advise the cooperative testing in identifying and prioritizing vulnerabilities.

3.5.3.5.1 DT&E/ST&E Activities

3.5.3.5.1.1 Identify Cybersecurity Requirements

Per DHS-4300A,[55] the first step in the cybersecurity process is to identify cybersecurity requirements for the CDM Program. DHS cybersecurity policy provides the foundational guidance for identifying compliance-based requirements and implementing the risk management framework (RMF).[56] Authoritative references for DHS cybersecurity policy include the FISMA,

[55] DHS 4300A Sensitive Systems Handbook, Version 11.0, January 14, 2015.

[56] DHS Security Authorization Process Guide, Office of the Chief Information Security Officer (CISO), Version 11.1, March 16, 2015.

OMB Circular A-130,[57] various Federal Information Processing Standards (FIPS), and the guidelines and standards in the NIST SP 800-series of documents.[58]

3.5.3.5.1.2 Cybersecurity Risks and Verify Security Controls

The OTA will monitor CDM through IV&V and DT&E and be cognizant of any issues that may affect operations discovered prior to initiating operational evaluation. In particular, the OTA will be cognizant of the CDM information security plan developed in accordance with NIST SP 800-18, Revision 1,[59] which shall include the security controls defined in NIST SP 800-53, Revision 4 and assigned in accordance with NIST FIPS Publication 199,[60] FIPS-200,[61] and NIST SP 800-53A, Revision 4. The OTA will consider the status of CDM security controls as a key component of its evaluation of CDM cybersecurity. In support of this evaluation, the OTA expects to leverage results from CDM Security ST&E.

3.5.3.5.1.3 Cybersecurity Readiness for Operational Deployment

The OTA will evaluate results from Level-3 testing, focusing on evaluating system security's ability to support CDM missions in an operationally realistic environment and assessing readiness for operational implementation. If the system/segment under test is adequately mature, the Level-3 testing may be an integrated DT/OT event with the OTA participating in test planning. If approved and funded by the PMO, the Level-3 test environment could incorporate simulated threats to the key mission threads that the CDM system intends to support, including organizational structures, operators, and network defenders. The OTA anticipates that such testing could allow operators to react to simulated threats in controlled test conditions. Cyber threat teams, if approved and funded, would participate cooperatively to advise on potential threat actions and to contribute to vulnerability characterizations. If the system/segment under test is sufficiently mature, the OTA recommends that Level-3 testing include adversarial Red Team testing of the CDM system in order to provide early characterization and prioritization of CDM's vulnerabilities as a function of the Red Team's experience, attack vector, and type of exploits. If undertaken, the adversarial testing should utilize a certified Red Team in realistic cyber environments (e.g., to include traffic generation). This testing could be conducted in a distributed live-virtual-constructive environment with a network of Agency and Federal level users.

---

57 OMB Circular A-130, Section 8b(3), Securing Agency Information Systems, 1985 – as analyzed in Appendix IV: Analysis of Key Sections, with supplemental information in Appendix III, Security of Federal Automated Information Resources.

58 The NIST Special Publications that specify key requirements and artifacts include (not exhaustively): NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems, 2010; NIST Special Publication 800-37, Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems, 2010; NIST Special Publication 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, 2014; NIST Special Publication 800-53A, Revision 4, Assessing Security and Privacy Controls in Federal Information Systems and Organizations, 2014.

59 NIST Special Publication 800-18, Revision 1, Guide for Developing Security Plans for Federal Information Systems, 2006.

60 FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems, NIST, 2004.

61 FIPS PUB 200, Minimum Security Requirements for Federal Information and Information Systems, 2006.

The OTA plans to evaluate results of any Level-3 contingency plan testing and incident response testing, encompassing aggressive and exhaustive "exploitation testing" of the CDM system in networked but controlled environments. Test cases could include systems with and without local network defenders and network defense capabilities (e.g., a Computer Network Defense Service Provider).

3.5.3.5.2 OT&E Activities

The purpose of CDM cybersecurity OT&E is to characterize the operational resilience of CDM, examining operational cybersecurity risks to CDM and to the networks and hosts it resides on (i.e., not introducing additional major vulnerabilities) as CDM is deployed to the networks. Cybersecurity OT&E identifies critical cybersecurity operational issues prior to CDM acquisition milestones and builds confidence in the degree to which CDM will be cyber secure in operations. CDM OT&E will focus on providing decision quality information to PMO risk reduction processes. The following paragraphs offer a recommended minimum set of steps for the OT&E of CDM cybersecurity.[62]

3.5.3.5.2.1 Cooperative Assessment of Vulnerability, Penetration, and Operational Risk

Prior to dedicated OTs, the OTA will review all cybersecurity testing results to assess residual CDM cybersecurity risks and inform the level and scope of cybersecurity OT&E. The OTA's derived test plans will encompass evaluations of protection, detection, response, and recovery functions for CDM that resides organically on the CDM and/or in the network enterprise that hosts CDM. The test plans will build on the results of the control assessment check of whether the controls enabling operational resilience have been implemented in a manner that make it likely that the System Under Test (SUT) will be cyber secure.[63]

The OTA will conduct a comprehensive, overt, and cooperative penetration and vulnerability assessment of CDM in its intended operational environment.[64] "Overt and cooperative" means the assessments will be conducted in coordination and/or cooperation with CDM integrators, operators, and users. Red Teams, Blue Teams, and System security Teams should work in concert and cooperatively to characterize and analyze CDM vulnerabilities based on a thorough review and analysis of the CDM system architecture, CONOPs, SOPs, the host-network security environment, and characterizations of likely cyber threats to CDM and Federal networks and hosts. This step should include evaluations of:

- Configuration management and system cybersecurity tools
- New equipment and cybersecurity training
- Cybersecurity incident response

---

62 Derived from DoD guidance: Procedures for OT&E of IA in Acquisition Programs, DOT&E, 21 January 2009.

63 The only controls that the OTA should evaluate are those that are not part of the baseline required for the Assessment and Authorization (A&A), but identified as mitigations to the risks from the threat assessment. However, if the cybersecurity testing requirements are effectively coordinated, even these non-baseline controls will be reviewed by the OTA as part of the risked based tailoring of the controls.

64 Encompassing both Cooperative Vulnerability and Penetration (CVPA) and A&A activities.

- Patch management and network access controls
- Inherited controls[65]
- Protect, detect, respond, and recover capabilities and limitations.

3.5.3.5.2.2 Adversarial Testing and Evaluation of Protection, Detection, Response, and Recovery

The cybersecurity T&E steps outlined thus far focus on evaluations of systems *preparedness*. In order to evaluate CDM system *performance* in a hostile cyber environment, the OTA should assess cybersecurity vulnerabilities encompassing and going beyond those discovered in the previous step, and including likelihood of their exploitation by representative cyber threats and ultimate impact on the CDM mission. The adversarial assessment should evaluate the ability of CDM to conduct its assigned mission in the presence of cyber threat activities consistent with threats validated by CDM threat assessment reports and described in the CDM TEMP. If such threat descriptions are absent or inadequate, the adversarial testing should adopt a threat profile validated for similar systems in similar operational environments.

Certified Red Teams,[66] i.e., adversarial cyber operations teams, independent from the developer should conduct comprehensive exploitation tests in realistic operational environments. The adversarial testing should be designed to characterize and prioritize CDM's vulnerabilities as a function of the Red Team's experience, attack vector, and type of exploits to evaluate the following CDM cybersecurity components (as defined in the CDM TEMP):

- Protect: CDM and host network defenders protect CDM's subsystems and data against adversarial activities, including pivoting attacks against the cybersecurity of interfaced systems from CDM subsystems.
- Detect: CDM and host network defenders detect adversarial activities against CDM's subsystems and data.
- Respond: CDM and host network defenders mitigate detected adversarial activities against CDM's subsystems and data.
- Recover/Continuity of Operations (COOP): CDM and host network defenders recover CDM mission effectiveness following successful adversarial attacks against CDM's subsystems and data.
- Mission: CDM effectively conducts its assigned mission in the presence of adversarial activities against CDM's subsystems and data.

---

65 As assigned in accordance with Appendix I of NIST SP 800-37, Revision 1.

66 Red Team testing should be adversarial in nature and representative of hostile cyber threats. Entrance criteria for progressing into testing include the requirement that the system or segment under test is sufficiently mature and has implemented necessary security controls prescribed in accordance with FIPS. The type of threat and risk will drive the type of "adversarial teaming". It could range, for example, from National Security Agency (NSA) black hat aggression to the OTA leading a tabletop exercise.

The design of a comprehensive penetration and exploitation adversarial test should include the following key considerations:[67]

- Because of limited test durations in OT&E events, CDM system information and interconnections may be provided to the penetration/exploitation Blue/Red Team to facilitate the cybersecurity evaluation (vice having the team seek to discover the required information/interconnections as part of the evaluation). This is much more likely to be the case for Blue Teams. In some instances, it may be plausible to give a Red Team the main entry point.
- CDM's ability to facilitate user and system/network administrator detection of and reaction to penetrations and exploitations should be evaluated, supporting the determination of how well cybersecurity measures support mission accomplishment.
- Existing CDM operations incident-handling reports can be reviewed to support the evaluation of detect, respond, and recover functions.
- Findings should address operational impact and implications for achieving the intended mission of the SUT.

3.5.4 Test Limitations

CDM OT&E limitations and potential mitigations are described below. Revisions are anticipated as CDM development, deployments, and test plans evolve towards the IOT&E and FOT&E to be conducted in four to five years. Early OT opportunities, including narrowly focused OAs, likely can be expected to be subject to additional constraints curtailing the scope of possible assessment insights. The OTA and T&E WIPT continually will evaluate program risks and monitor deployment timetables and available levels of resources for developing and implementing specific mitigation steps. While the limitations discussed here are addressed on a one-at-a-time basis, combinations of tested and untested variables will be examined when assessing program risks.

3.5.4.1 DHS-Centric OT&E

Comprehensive CDM IOT&E and FOT&E will be conducted at DHS, coincident with DOT&E authority and initial deployments of CDM phases. The feasibility of executing multiple parallel sets of IOT&Es/FOT&Es in non-DHS Agencies is limited due to resource demands and approval and coordination requirements. DHS also will host a progression of Agency-level OAs leading up to the program-level IOT&E. Based on preliminary consultations, the OTA anticipates that (1) numerous non-DHS Agencies will organize their operational analyses and associated demonstration activities supporting required PIRs into structured OT events, and (2) the OTA will have invited roles in the planning for and reporting on a subset of these OTs.

The OTA will work with the PMO and CMaaS providers to identify specific opportunities and options. As the number of Agencies is large and their characterizations involve multiple attributes, i.e., commonalities and differences, the OTA will develop a structured scheme for

[67] Derived from DoD guidance: Procedures for OT&E of IA in Acquisition Programs, DOT&E, 21 January 2009.

tracking what has been tested and assessed, and for supporting decisions on where and when to focus its operational testing resources (recognizing that such decisions will need to respond to fluid acquisition schedules). Fundamental Agency descriptors to consider include CMaaS provider, size, sensor/tool suites, architecture, and unique mission and operational aspects. A similar approach also will be pursued by the OTA to guide its monitoring of Agency-specific integration and acceptance testing to be executed by CMaaS providers and Agencies, for purposes of eliminating intra-system anomalies and verifying inter-system connections prior to Agency declarations that CDM instantiations are formally fully operational.

Table 3-1 is the current configuration of the OTA's sampling plan, depicting for each CDM TO the specific Agencies or choices of Agencies to be sampled – either directly in OTA-led formal OT&E (presently limited to DHS) or indirectly via reviews of Agency-controlled operational performance testing/reporting and/or responses to OTA survey questionnaires. The plan calls for a minimum of 27 Agencies to be sampled. The designations for TO2B, TO2D, and TO2E do not span the entirety of the Agencies encompassed by the subject parent TO; any non-listed Agencies are eligible for inclusion into the OTA's evaluations and are displayed as "Optional." The table entries incorporate considerations of sensor/tool combinations, Agency size, and number of Agency dashboards. When a lone Agency appears in a line of the table accompanied by an asterisk ("*"), it corresponds to a combination of sensors/tools that is unique to that particular Agency and CMaaS provider. Inability to obtain data from that Agency would constitute an OT&E limitation.

Table 3-1. Initial OTA Sampling Plan

CDM TO	Agencies
TO2A	• DHS
TO2B	• OPM* • USDA* • USDOT or VA • Optional: DOE, DOI, and EOP
TO2C	• DOJ • DOC or DOL • DOS or USAID
TO2D	• GSA • NASA or SSA • Treasury or HHS • Optional: USPS
TO2E	• ED* • SBA* • EPA or NRC • Optional: HUD and NSF
TO2F	• TVA, SEC, or NARA • 4 of the following: Peace Corps, BBG, USPSOIG, PBGC, EEOC, FCC, CFPB, FERC, FTC, CFTC, NLRB, and CSOSA • RRB • 8 of the following: FHFA, CNCS, CPSC, FEC, USITC, OPIC, MCC, NTSB, EXIM, DOS-OIG, FCA, MSPB, NEH, SSS, NEA, IBWC, OSC, ABMC, DNFSB, OGE, PRC, FMC, USADF, OSHRC,

	NCPC, USAB, CIGIE, and PCLOB

* Unique combination of sensors/tools for the subject CDM TO and CMaaS provider

3.5.4.2 Testing Subsets of CDM Configurations

The OTA's information tracking approach also will facilitate addressing the limitation (all COIs) that dedicated OT&E will not be able to encompass every combination of deployed sensor/tool suites, CMaaS integrations, and dashboard hierarchies external to and within DHS. It will enable systematic tracking of the demonstrated performance of specific CDM system elements and configurations as they are tested throughout DT&E and Agency deployments, permit structured sampling options for future testing to be formulated, and support the construction of rudimentary similarity metrics to make inferences on particular CDM system instantiations that have not been directly tested.

3.5.4.3 Network Capacity and Loading Constraints in Testing

CDM systems, at Agency and Federal dashboard levels, must be designed and integrated to accommodate total network and peak load demands (COI 4). As CDM will be deployed incrementally, what can be directly tested in any individual DT&E or OT&E event will be limited. The extent of any such limitation is not presently quantifiable, but design studies undertaken by CMaaS providers and the Federal level dashboard developer, PMO reviews, and DHS IV&V processes would be informative.[68] As OAs will be undertaken prior to the complete deployment and maturation of CDM, network capacity issues at the Agency and Federal dashboard levels in those OT&Es events necessarily will be unrepresentative of future operations.

This limitation may be mitigated by drawing on cyber range testing opportunities (e.g., using the CDM-specific network emulation testbed at JHU/APL[69]) and/or DT&E, or deferring to later OT&E testing. The OTA in conjunction with the PMO will continue to explore these options.

3.5.4.4Operational Constraints during Testing

CDM operational considerations will constrain network testing and curtail insights on performance under non-benign and non-routine circumstances during OT&E (COI 1 and COI 7). CDM is required to detect and report unapproved Hardware/Software (HW/SW), and, more generally across the spectrum of all CDM functional capabilities, find deviations from "desired states." This essential ability of CDM can be fully demonstrated directly in formal OT&E events only if deviations are present on tested networks and are known a priori to testers. While CDM's discovery of defects that were unknown certainly would provide demonstrations of CDM's utility, quantitative assessments of ORD-prescribed system performance requirements (e.g.,

---

68 A recently completed contractor report offers some insight: CDM Agency Dashboard Performance Benchmark Analysis, Version 1.0, Metrica Team Venture, February 2017. Follow-on analyses continue to be pursued at the contractor, Agency, and PMO levels. Results are anticipated to guide both deployment and T&E decisions.

69 There presently are no PMO plans to pursue such testing. A relevant testing concept had been developed by the CDM Test Team: CDM Test Plan for Level 2 Testing, Version 1.3, JHU/APL, December 2016.

detecting a threshold/objective percentage of true defects) cannot be determined without precise counts of actual defects on the network. To determine verifiable truth data for accurately characterizing HW/SW inventories, configurations, and vulnerabilities, Agency mapping and scanning tools (separate and independent from CDM systems) would be required.

Potential mitigation steps that could be pursued include DT simulations, dedicated integration and acceptance testing, and focused cyber range testing. To address this limitation directly in OT&E events, controlled injects of specific departures from baseline HW/SW inventories and other desires state configurations can be undertaken – but only after appropriate advance coordination and approval. The OTA and CDM Test Team will continue to explore the viability of the controlled scenario injections throughout the evolution of CDM OAs.

3.5.4.5Fixed Dashboard Risk Scoring Rules

Formal CDM OT&E events are envisioned to overlap periods of operation at DHS locations. CDM scoring rules can be expected to be fixed during such times, or possibly vary minimally. No extended implementations of alternative sets of scoring rules could reasonably be foreseen. Consequently, the OTA will not be able to assess the optimality of CDM's specific designation of Federal-wide scoring rules. Nor will the OTA be capable of testing the proficiency of the scoring rules in responding to undesirable security circumstances that may arise in individual Agencies or collectively across sectors of .gov networks.

There are no planned T&E initiatives to address these concerns, and no analysis-based study of the merits of alternative sets of scoring rules is available. Cyber range testing would offer a mechanism for examining broad sets of prospective operational circumstances and enabling comprehensive evaluations of the extent to which different CDM scoring rules and implementations enhance the security posture of Federal .gov networks (COI 1). Required resources would not be minimal, and a strong commitment from the PMO would be required. Some effort along these lines naturally could be integrated into the ongoing process of developing CDM scoring rules.

3.5.4.6Data Aggregation

Any single OT&E event is of limited duration and likely will not provide a stand-alone opportunity to comprehensively examine all OS issues (COI 6). Test data and insights, when appropriate, will be assimilated across individual OT&E events. Additionally, operational performance during non-dedicated OTs will be considered as warranted. As needed, maintenance demonstrations may be arranged.

3.5.4.7Lack of Agency Baseline Performance Characterizations

CDM KPPs quantify the required performance levels for particular aspects of CDM system performance. They do not, however, by themselves address the degree to which the deployment of CDM capabilities enhances the ability of Agencies to accomplish their security monitoring and risk management and reporting missions. Direct measurements of such (COIs 1-3) would necessitate knowledge of Agency baseline performance characterizations, i.e., pre-CDM. Examples of such analyses could include relative comparisons of manpower needs supporting

FISMA reporting, incidence rates for detecting unauthorized HW/SW and other deviations from desired states, and mean times to discover and mitigate vulnerabilities present on networks.

The OTA will work with the CDM Test Team, PMO, and Agency user representatives to determine the feasibility of establishing baselines of current inventory and control management performance using historical audits and evaluations. Baselines could be determined for the initial advent of CDM into Agencies or for early demonstrated performance in OAs.

3.5.4.8 Survey Response Rates

CDM personnel will be given survey questionnaires, but the response rate and quality of individual responses cannot be guaranteed (all COIs). Mitigation approaches include follow-on survey instruments, one-on-one interviews, or narrowly focused demonstration events. Also, surveys will be utilized in sequences of OAs preceding IOT&E/FOT&E, providing additional data and supporting progressive enhancements in the quality of survey instruments.

3.5.5 Reports

For each of its dedicated CDM OT&E events, the OTA will author test plans and associated test reports. These will be submitted to the CDM T&E WIPT for review. The OTA additionally will observe other DT&E and Agency-level test events that potentially can enlighten its OT&E planning and augment evaluation of CDM COIs. For tests that the OTA deems to be substantively informative or upon request from the CDM PMO or DOT&E, the OTA will record observations, results, and insights in the form of LOOs forwarded to the CDM Test Team Lead and the DOT&E Test Area Manager (TAM).

The OTA will be responsible for the OT&E portions of the TEMP, encompassing updates as prescribed in the Executive Summary and as needed prior to milestone events. The TEMP is subject to review and approval by DOT&E. Updated TEMPs will support the construction of detailed OTA test plan documents – SEPs, OAPs, and OTPs). All formal OTA test plans will follow guidelines in DHS Instruction 102-01-103[70] and will require DOT&E approval. The OTA will document results from evaluations of major OT&E events (program- or Agency-level) via Operational Assessment Reports (OARs), and Operational Test Reports (OTRs).

The DOT&E is responsible for providing Letters of Assessment (LOAs) addressing the adequacy of program-level OT&E events and providing assessments and conclusions at the appropriate ADEs to the ADA.

All CDM performance results and evaluations will be considered to be sensitive and treated as For Official Use Only.

[70] DHS Guidebook, 102-01-103-01, Systems Engineering Life Cycle Guidebook, DHS, April 2016.

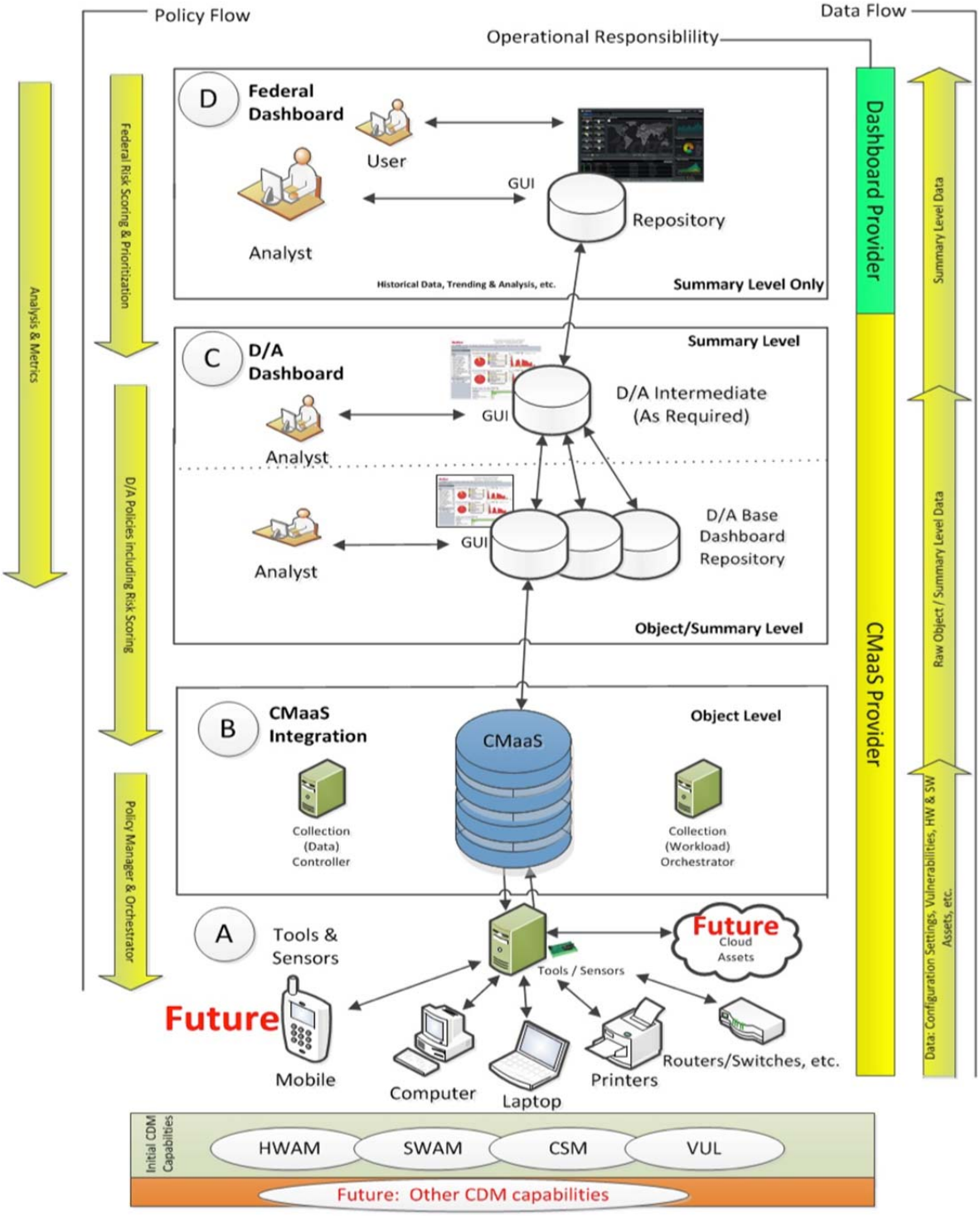
Table 3-2. CDM OT&E Documentation

Event	Document Type	Originating Organization	Document Timeline
Level-1, Level-2, and Level-3 Test[a]	LOO (for select events)	OTA	30 days after receipt of DT&E data
Phase IOC and/or as needed	TEMP Update[b]	CDM Test Team & OTA (for OT&E portion)	60 days before event, or as needed
	SEP	OTA	60 days before associated IOC OA
OAs, IOT&E, and FOT&E	TEMP Update[b]	CDM Test Team & OTA (for OT&E portion)	60 days before ADE-3, or as needed
	OA/OT Plan	Operational Tester	60 days before OT&E event
	OTRR Report	OTA	10 days after OTRR
	OA/OT Report	OTA	45 days after receipt of event data and at least 45 days prior to any ADE being supported by the subject test event
	LOA	DOT&E	30 days after receipt of OA/OT Report and at least 14 days prior to any ADE or other major decision event being supported by the subject test event

[a] OTA observation of events that support OT&E planning and assessments
[b] Approved by DOT&E

ANNEX 1: Operational View

The following figure depicts the CDM Operational View:



ANNEX 2: Critical Technical Parameters

The following table lists the CTPs for CDM:

CTP	Test Event	Technical Threshold	Technical Objective	Test Location	Test Schedule	Decision Supported
Timeliness of Information	Demonstration & Analysis	72 hours	72 hours	Solution Provider Facility	DT	Production Readiness Review (PRR)
Coverage of IT assets	Demonstration & Analysis	>80% in two successive scans	>95% in two successive scans	Solution Provider Facility	DT	PRR
Coverage of IT vulnerabilities	Demonstration & Analysis	80%	95%	Solution Provider Facility	DT	PRR
Network Performance	Demonstration & Analysis	TBD[71]	TBD	Solution Provider Facility	DT	PRR
Accuracy	Demonstration & Analysis	< 0.1% false positives or negatives	< 0.01% false positives or negatives	Solution Provider Facility	DT	PRR
Scalability	Demonstration & Analysis	> 1M devices	> 1M devices	Solution Provider Facility	DT	PRR

NOTE: Data in this table originates from CMaaS tools Requirements, Section 9, Attachment N

71 The environment owner (DHS or each Agency) will determine the technical threshold for network performance.

ANNEX 3: Key Performance Parameters

The following table lists the KPPs[6] for CDM:

Note: KPPs are defined as achieving 72 hour currency relative to collecting data on network devices.			
Cybersecurity Framework Functions and Associated CDM KPPs	**CDM Measures**		
	Statement	**Threshold**	**Objective**
1. IDENTIFY – Asset Management; Risk Assessment. Shall provide complete inventories of all hardware assets, software assets, configuration settings, and vulnerabilities. *[CDM Capabilities 1-4]*	1.1. Percentage of authorized (unauthorized) hardware assets, software assets, and configuration settings that CDM correctly identifies as "authorized" ("unauthorized")	80%	95%
	1.2. Percentage of authorized (unauthorized) software assets that CDM correctly associates with the specific parent hardware platform		
	1.3. Percentage of vulnerabilities that CDM correctly identifies		
2a. PROTECT – Access Control; Awareness and Training. Shall manage accounts for people and services. *[CDM Capabilities 5-9]*	2a. Percentage of compliant (non-compliant) accounts that CDM correctly identifies as "compliant" ("non-compliant")	80%	95%
2b. PROTECT – Information Protection Processes and Procedures. Shall manage preparations for contingencies and incidents. *[CDM Capabilities 10-11]*	2b. Percentage of implemented (non-implemented) desired contingency and incident preparation attributes that CDM correctly identifies as "implemented" ("non-implemented")	80%	95%
2c. PROTECT – Data Security; Protection Technology. Shall design for and maintain cybersecurity resiliency in the presence of realistic CDM-specific cybersecurity threats. *[CDM Capabilities 12-13 & CDM Critical Operational Issue 7 – Cybersecurity]*	2c. Percentage of implemented (non-implemented) desired network security design attributes that CDM correctly identifies as "implemented" ("non-implemented")	80%	95%
2d. PROTECT – Maintenance. Shall support sustained operations. *[Sustainability – CDM Critical Operational Issue 6]*	2d.1. Mean time between operational mission failures for individual CDM elements	100 hours	200 hours
	2d.2. Operational availability of individual CDM elements	99.5%	99.9%

3a. DETECT – Anomalies and Events; Security Continuous Monitoring. Shall aggregate CDM scanning and defect detection results and display associated summaries and risk scoring compilations at Agency Dashboards and the Federal Dashboard. *[CDM Capabilities 1-15 & "CDM Capability 0" – Dashboards]*	3.a. Percentage of timely, complete, and accurate object level, summary level, and risk scoring compilations at Agency Dashboards and the Federal Dashboard	80%	95%
3b. DETECT – Security Continuous Monitoring. Shall automate FISMA compliance reporting. *[CDM Critical Operational Issue 3]*	3.b. Percentage of timely (72 hours), complete, and accurate FISMA reports	80%	95%
4. RESPOND – Response Planning; Analysis; Mitigation; Improvements. Ability to check Agency planning for conducting effective responses to incidents and attacks and limit their impacts. *[CDM Capabilities 10-11 and 14-15]*	4.1 Percentage of implemented (non-implemented) desired contingency and incident response attributes, manage audit information attributes, and manage operation security attributes that CDM correctly identifies as "implemented" ("non-implemented**")**	80%	95%
	4.2. Severity of incidents in maintaining the confidentiality, integrity, and availability of CDM hardware, software, and data to acceptable levels	No Category I[72]	No Category I or II[73]
5. RECOVER – Recovery Planning; Improvements. Ability to check Agency planning for conducting effective recoveries from incidents and attacks. *[CDM Capabilities 10-11 and 14-15]*	5. Percentage of implemented (non-implemented) desired recovery attributes that CDM correctly identifies as "implemented" ("non-implemented")	80%	95%

[72] Category I is defined as any vulnerability, the exploitation of which will, directly and immediately result in loss of Confidentiality, Availability, or Integrity.

[73] Category II is defined as any vulnerability, the exploitation of which has a potential to result in loss of Confidentiality, Availability, or Integrity.

ANNEX 4: Critical Operational Issues

The full text versions of the COIs, MOEs, MOSs, and MOCs for CDM are presented in Table A4-1. The COIs, extracted from the ORD, are listed as questions and the measures, taken from the IEF, are presented as statements. These are linked to specific enumerations of ORD-specified requirements and KPPs.

Table A4-1: CDM List of COIs, MOEs, MOSs, and MOCs

	COIs	MOEs/MOSs/MOCs	Section from CDM ORD (Version 3.0)
Operational Effectiveness	**1. Situational Awareness:** Does CDM deployed at the Department, Agency, and Federal levels improve situational awareness?	**1.1 Manage Assets:** CDM improves situational awareness supporting IT management by providing complete inventories of all hardware assets, software assets, configurations, and vulnerabilities.	3.4.1, 5.0 (KPP 1.1, 1.2, 1.3)
		1.2 Manage Accounts for People and Services: CDM improves situational awareness by managing trust in people granted access, security related behavior, credentials, and account access.	3.4.2, 5.0 (KPP 2a)
		1.3 Manage Events and Security Lifecycle: CDM improves situational awareness by managing network access, events, and security lifecycle.	3.4.3, 5.0 (KPP 2b, 2c, 4.1, 4.2, 5)
	2. Security Posture: Do CDM information exchanges, scoring rules, and implementations improve the security posture of government networks?	**2.1 Agency Security Posture:** CDM information exchanges, scoring rules, and implementations improve the security posture of agency networks.	3.4.5 (KPP 3a)
		2.2 Federal Security Posture: CDM information exchanges, scoring rules, and implementations improve the security posture of Federal networks.	3.4.4, 3.4.5 (KPP 3a)
		2.3 Dashboard – Dashboard Interoperability: CDM information exchanges improve the security posture of agency and Federal networks.	3.4.4, 3.4.5, 4.2 (KPP 3a)
	3. Reporting FISMA Metrics: Does CDM improve the efficiency of reporting FISMA metrics?	**3.1 Timeliness:** CDM improves the timeliness of FISMA reports and analyses.	3.4.4 (KPP 3b)
		3.2 Accuracy: CDM improves the accuracy of FISMA reports and analyses.	3.4.4 (KPP 3b)
		3.3 Completeness: CDM improves the completeness of FISMA reports and analyses.	3.4.4 (KPP 3b)
		3.4 Manpower: CDM reduces the manpower required to produce FISMA reports and analyses.	3.4.4
Operational Suitability	**4. System Design:** Does the CDM system design support current and envisioned future operations?	**4.1 Human Factors:** CDM system designs (including user and maintainer equipment and processes) support straightforward operations.	4.3.3, 6.0
		4.2 Compatibility: CDM does not degrade Agency operations and can adapt to future technologies.	4.1, 6.0
		4.3 Scalability: CDM network loading and growth potential can incorporate architecture expansions.	4.1, 6.0

	COIs	MOEs/MOSs/MOCs	Section from CDM ORD (Version 3.0)
	5. Documentation & Training: Do CDM technical manuals, Standard Operating Procedures (SOPs), and training programs support users and maintainers?	**5.1 Technical Manuals:** CDM technical manuals and reference documentation support CDM users and maintainers.	4.6, 6.0
		5.2 SOPs: CDM operating instructions and guidance for interpreting and responding to emerging results support CDM analysts and managers.	4.6, 6.0
		5.3 Training Programs: CDM training programs support the development and sustainment of user and maintainer skill sets.	4.6, 6.0
	6. Sustainability: Do CDM reliability, availability, and maintainability support system operation?	**6.1 Reliability:** CDM performs its mission reliably, without excessive hardware/software (HW/SW) failures or degradation of capabilities.	4.2.2, 4.4, 6.0 (KPP 2d.1)
		6.2 Availability: CDM is available, i.e., accessible and useable on demand, to support operating profiles.	4.2.1, 4.4, 6.0 (KPP 2d.2)
		6.3 Maintainability: CDM HW/SW maintenance, repair, and replacement processes support operational availability.	4.2.2, 4.4, 4.5, 6.0 (KPP 2d.2)
Cybersecurity	**7. Resiliency:** Are CDM systems and networks resilient to cyber threats?	**7.1 Protect:** CDM and host network defenders protect CDM's subsystems and data against adversarial activities, including pivoting attacks.	6.0 (KPP 4.2)
		7.2 Detect: CDM and host network defenders detect adversarial activities against CDM's subsystems and data.	6.0
		7.3 Respond: CDM and host network defenders mitigate detected adversarial activities against CDM's subsystems and data.	6.0
		7.4 Recover/Continuity of Operations: CDM and host network defenders recover CDM mission effectiveness following successful adversarial attacks against CDM's subsystems and data.	6.0
		7.5 Mission: CDM effectively conducts its assigned mission in the presence of adversarial activities against CDM's subsystems and data.	6.0

ANNEX 5: Interface Requirements

The CDM program currently has no recorded interface requirements other than those any applicable requirements identified in program Functional Requirements Documentation (FRDs).

ANNEX 6: Failure Definition and Scoring Summary

See Section 1.6.3.1 for the failure definition and scoring summary used by the CDM T&E community.

ANNEX 7: Resource Summary

Note: In this section, IT&E is decomposed into DT&E and OT&E for funding purposes.

The CDM PMO will review the solution provider's system engineering design and test plans to assure alignment with the KPPs, CTP, and the ORD and functional requirements. Based on this review the government will provide comments and recommendations to the solution provider(s) prior to acceptance of design and test plans. This acceptance may place emphasis on planned tests and include recommendations for additional tests, if needed. Solution providers will provide their own personnel for testing. The CDM PMO will provide government employee SME's and contractor SME's. The solution provider is responsible for analysis of test results and delivery of test reports. The CDM PMO will produce test reports for comparative analysis with that of the solution provider/tester. This will serve as the government's validation for the functional and technical requirement of the solutions. Discrepancies or deficiencies must be resolved by the solution provider and test reports updated before the PMO will formally accept the test results. User organizations will be involved in the review process, follow-on operational testing, and other exercises as necessary.

Table A7-1 contains the estimate by fiscal year of the funding required for planned testing. T&E funding estimates are aligned with the CDM life-cycle cost estimate for labor costs and do not include potential materiel requirements. The following sections identify resources necessary to conduct test.

Table A7-1: Summary of T&E Funding Requirements ($K)

WBS Description	Prior Years	Current Year	FYHSP Years					Future	TOTAL
(TY$M 50%CL*)	FY12-FY16	FY17	FY18	FY19	FY20	FY21	FY22	FY23-FY31	FY12-FY31
Total Testing	**$ 31.826**	**$ 29.382**	**$ 18.503**	**$ 5.278**	**$ 7.079**	**$ 7.531**	**$ 5.349**	**$ 15.154**	**$ 120.103**
PMO	$ 8.701	$ 2.393	$ 2.483	$ 0.501	$ 0.559	$ 0.570	$ 0.581	$ 5.785	$ 21.575
DT&E	$ 17.344	$ 20.242	$ 12.015	$ 3.583	$ 4.890	$ 5.221	$ 3.576	$ 7.027	$ 73.896
OT&E	$ 5.781	$ 6.747	$ 4.005	$ 1.194	$ 1.630	$ 1.740	$ 1.192	$ 2.342	$ 24.632

**Note that Phase 3 is being managed at the 80%CL*

NOTES:

- T&E funding requirements as estimated in the LCCE v5.3, February 21, 2017
- PMO costs include federal program staff and contractors providing DT and OT activities on behalf of the program
- DT&E costs cover estimated testing and integration provided by CDM integrators
- OT&E costs cover estimated operational costs as supported by CDM integrators
- Actual budget information is available under separate cover.

Test Articles

The test articles and testing schedule vary by test, DT&E, IV&V and OT&E. The CDM segments under test include the CMaaS solution, the Agency CDM Dashboard, the Federal Dashboard, and combinations of these components. Selection of test articles for DT&E for a specific solution will vary depending on many factors as further specified in Section C. Section

3.5 specifies the CDM OT&E program is focused on identified assets and associated operating and support processes that reside within DHS, which coincides with where DOT&E has full OT&E authority. The CDM PMO may accept the DT&E and/or OT&E test role for testing conducted in the Agency environment if the CMaaS solution being implemented is DHS funded, upon request by the Agency, approved by the DHS OGC, and with required documentation. As the need for assessment becomes apparent and agreements are made, the articles chosen for evaluation will become evident, but only compliant with DHS authority limited to DHS systems and whatever organizations agree to provide their systems for test.

Test Sites/Instrumentation/Airspace/Spectrum

- Level-1 IT&E will be conducted at the CMaaS solution provider's development location
- The CDM PMO will determine the location for any Level-2 IT&E (TBD)
- Level-3 IT&E will be conducted at the Agency location
- The Federal Dashboard will be tested in the DHS Mission Operations Environment (MOE).

Test Support Equipment

TBD

Threat Systems/Simulators

For operational testing, potential supplementary data sources include Red/Blue Team activities, cyber range testing, and simulated scenario injects. Any Red/Blue Team activities will be defined in the test plans and cyber range testing will be at a developer site or a government designated test bed.

Test Targets and Expendables

No test targets or expendables are required for these tests.

Operational Program Test Support

Only operationally deployed production configurations of CDM systems will participate in OT&E events. The test articles will include:

- Principal CDM system elements (i.e., sensors and tools, CMaaS, and different levels of dashboards) located at their respective D/As and at the site of the federal dashboard
- Associated operations and logistics support equipment and activities at these locations
- All necessary fully trained personnel (operators, users, and maintainers) supporting operations at these locations.

A number of CDM OT&E resource sizing issues cannot be resolved definitely at this point in time. Initial projections will be specified in the SEP and updated based on DT&E and OT&E results and insights, experience in collecting performance data during early CDM operational and testing periods, and T&E WIPT deliberations. Required levels are anticipated to grow as OT&E progresses from the initial OA to the IOT&E. Unresolved CDM OT&E resource requirements presently include:

- Specific minimum numbers of particular CDM entities and requisite interfaces
- Counts of and training requirements for OT&E data collectors
- Counts of and training requirements for any Red/Blue Team members
- Reliance on cyber range testing

Dedicated cyber range testing is identified in Level-2 IT&E testing as a means for mitigating limitations inherent to evaluating several CDM operational performance issues. The SEP will describe potential CDM T&E concepts for incorporating cyber range testing progressively into the OT&E program and will outline a formal validation process to be executed by the OTA.

At this time, there are no OT&E-specific resource requirements for CDM test support equipment, instrumentation capabilities, threat systems/simulators, test targets and expendables, dedicated operational program test support (beyond the CDM operators, users, and maintainers integral to day-to-day operations at Agencies and CDM hosts and interfaces), and administrative and facilities support.

Simulations, Models, and Test Beds

- The CMaaS provider will provide the Level-1 IT&E testbed as per TO requirements.
- The CDM PMO will determine the environment for any Level-2 IT&E (TBD).
- The Agency will provide their pre-deployment environment and/or production environment for Level-3 IT&E.
- The Federal Dashboard will be tested in the DHS Mission Operations Environment (MOE).

T&E Administrative Support

TBD

Manpower and Training

TBD

Investment Requirements

TBD

Resource Summary Updates

The PMO needs further discussion and planning with the OTA in order to project key resources needed to accomplish DT&E and OT&E for the CDM program. The T&E WIPT will develop and maintain a master test schedule and resource plan.

Updates will be made as the testing approach matures, and the TO awards are made. Updates to the following will also be made as program and resource changes prompt changes to the Program or PMO approach to testing:

- **Test Articles –** Artifacts provided by the solutions providers including test plans and reports.

- **Test Sites –** Solution provider will provide a laboratory for development testing; the Agency will provide a development/test and staging area; the government may provide a designated test area for L-2 testing, if needed. This includes integration and test labs.

- **Test Support Equipment –** Provided by the solution providers for Level-1 IT&E; provided by the CDM test team and solution provider for Level-2 IT&E; provided by the Agency for internal testing conducive to Level-3 IT&E.

- **M&S Resources –** Are provided by the solution provider as part of Level-1 IT&E

T&E Administration Support – The solution providers will provide support facilities to house testing and IV&V personnel for each test event; CDM PMO will provide T&E WIPT meeting support, review and compile test artifacts, and observation or witness of testing events.

ANNEX 8: Decision Support Matrix and Integrated Evaluation Framework

Initial DSM for CDM Phase 1

DSM_4-Feb-2016.xlsx

Initial IEF for CDM Phase 1

A. Operational Effectiveness

The initial IEF for assessing CDM OE appears in Table A8-1 (derived primarily from the current OTA SEP). It builds on the OTA's evaluation methodology introduced in Section 3.5 and details supporting operational issues, measures, data elements, and test events. It also traces MOE statements and quantitative MOP requirements back to corresponding sections in the CDM ORD and in the list of CTPs. The objective is to construct a conceptual framework for guiding the future development of specific detailed OT&E plans. As the CDM program evolves, adjustments and refinements will be incorporated.

For COI 2, Security Posture, CDM user communities will be integrated into the process for developing further subordinate MOPs and information sources. This MOE addresses whether CDM supports security enhancement operations of CDM users across Agency and Federal levels.[74] CDM program acquisition documents and strategic DHS performance reports[75,76] presently do not prescribe any high-level metrics that could quantify the contributions of CDM to improving the government-wide security posture.

The footnotes for Table A8-1 make three points. First, to simplify the exposition, the column content throughout encompasses, as appropriate, each of the tools and sensors level, CMaaS level, Agency base Dashboard (DB) level, Agency intermediate DB levels, and Federal DB level. Second, each reference to CDM scanning results covers, as appropriate, a 72-hour reporting window and an Agency enclave. Third, more important MOEs, MOPs, and associated items are highlighted.

Descriptions of the contents of individual table columns follow:

1. **COI**: Provides the full text of the ORD's COI. Each COI has associated MOEs.
2. **MOE**: Provides the full text of each MOE. Related sections from the CDM ORD follow the MOE statement. Each MOE has associated MOPs.

---

[74] Evaluations for MOE 2.2 will consider cybersecurity impacts. Otherwise, quantitative OE and OS performance data will exclude consequences of and results attributable to malicious attacks.

[75] U.S. Department of Homeland Security Annual Performance Report Fiscal Years 2013 – 2015, Appendix B: Program Evaluations, Department of Homeland Security, June 2014

[76] Fiscal Years 2014-2018 Strategic Plan, Department of Homeland Security, 2014

3. **MOP**: Provides the full text for the MOP. If there are any related quantitative requirements from the CDM ORD, they follow the MOP statement. Each MOP also has at least one associated data element. Observed OT&E data will be summarized as MOP point estimates and associated 80 percent confidence limits/bounds.
4. **Data Element/Type**: Provides the specific data item(s) supporting each MOP (typically "Number of" or "Time of/for"), and/or characterizes the non-testing means for obtaining such data (e.g., documentation reviews, interview summaries, or survey results).
5. **Test Event**: Indicates whether a data element will be based on OT (OA, IOT&E, or FOT&E), DT (Level-1, Level-2, or Level-3 IT&E), Early Deployment (ED), Special Test Event (SpTE), or some combination thereof. SpTEs include events like Maintenance Demonstrations (M-Demos) and Disaster Recovery Demonstrations (DR-Demos).
6. **Notes**: Provides additional information to clarify the associated COI, MOE, MOP, Data Element/Type, or Test Event.

FOR OFFICIAL USE ONLY

Table A8-1. Initial IEF Structure for CDM OE

COI	MOE	MOP		Data Element/Type	Test Event	Notes
1 Situational Awareness: Does CDM deployed at the Agency and federal levels improve situational awareness?	**1.1 Manage Assets:** CDM improves situational awareness supporting IT management by providing complete inventories of all hardware assets, software assets, configurations, and vulnerabilities. **ORD 3.4.1, 5.0** **(KPP 1)** ***1.1.H Hardware Asset Management:*** *Discover unauthorized or unmanaged hardware on a network.*	**1.1.H.1** Percentage of authorized hardware assets connected to the network that CDM identifies as "authorized" **KPP 1.1:** Threshold = 80% Objective = 95%		**1.1.H.1.1** Number of authorized hardware assets connected to the network that CDM identifies as "authorized"	OT/ED/DT (System Logs, System Reports)	All hardware related MOPs may be evaluated across the network or broken down by device role.
				1.1.H.1.2 Number of authorized hardware assets connected to the network	OT/ED/DT (Documentation)	
		1.1.H.2 Percentage of unauthorized hardware assets connected to the network that CDM identifies as "unauthorized" **KPP 1.1:** Threshold = 80% Objective = 95%		**1.1.H.2.1** Number of unauthorized hardware assets connected to the network that CDM identifies as "unauthorized"	OT/ED/DT (System Logs, System Reports)	This MOP will depend on DT results. Any OT results will require the presence and independent awareness of unauthorized hardware assets on the network.
				1.1.H.2.2 Number of unauthorized hardware assets connected to the network	OT/ED/DT (Documentation, Test Agent Log)	
		1.1.H.3 Percentage of hardware assets in the CDM hardware desired state list		**1.1.H.3.1** Number of hardware assets in the CDM hardware desired state list that are part of a system that	OT/ED (System Logs, System Reports,	"The CDM hardware desired state list" is based on the CDM's

FOR OFFICIAL USE ONLY

COI	MOE	MOP		Data Element/Type	Test Event	Notes
		that are part of a system that has an authority to operate (ATO)		has an ATO	Documentation)	ingestion of the ATO list provided by the Agency. It does not reflect the results of CDM scanning.
				1.1.H.3.2 Number hardware assets in the CDM hardware desired state list	OT/ED (Documentation)	
		1.1.H.4 Percentage of hardware assets that are part of a system with an ATO that are included in the CDM hardware desired state list		**1.1.H.4.1** Number of hardware assets that are part of a system with an ATO that are included in the CDM hardware desired state list	OT/ED (System Logs, System Reports, Documentation)	
				1.1.H.4.2 Number of hardware assets that are part of a system with an ATO	OT/ED (Documentation)	
		1.1.H.5 Percentage of authorized hardware assets that are scanned by CDM hardware scanners		**1.1.H.5.1** Number of authorized hardware assets that are scanned by CDM hardware scanners	OT/ED/DT (System Logs, System Reports, Documentation)	This MOP requires an independent knowledge of the hardware ground truth state.
				1.1.H.5.2 Number of authorized hardware assets	OT/ED/DT (Documentati	

FOR OFFICIAL USE ONLY

COI	MOE	MOP		Data Element/Type	Test Event	Notes
					on)	
		1.1.H.6 Percentage of unauthorized hardware assets that are scanned by CDM hardware scanners		**1.1.H.6.1** Number of unauthorized hardware assets that are scanned by CDM hardware scanners	OT/ED/DT (System Logs, System Reports, Documentation)	
				1.1.H.6.2 Number of unauthorized hardware assets	OT/ED/DT (Documentation)	
		1.1.H.7 Percentage of hardware assets scanned by CDM hardware scanners that do not exist		**1.1.H.7.1** Number of hardware assets scanned by CDM hardware scanners that do not exist	OT/ED/DT (System Logs, System Reports, Documentation)	This MOP requires an independent knowledge of the hardware ground truth state.
				1.1.H.7.2 Number of hardware assets that are scanned by CDM hardware scanners [Identical to 1.1.H.5.1]	OT/ED/DT (System Logs, System Reports, Documentation)	
		1.1.H.8 Percentage of		**1.1.H.8.1** Number of authorized hardware assets	OT/ED	Consult NIST IR 7693 for

FOR OFFICIAL USE ONLY

COI	MOE	MOP		Data Element/Type	Test Event	Notes
		authorized hardware assets that are accurately/uniquely identified		that are accurately/uniquely identified	(System Logs, System Reports, Documentation)	precise details on accurately and uniquely identifying hardware assets.
				1.1.H.8.2 Number of authorized hardware assets [Identical to 1.1.H.1.2]	OT/ED (Documentation)	
		1.1.H.9 Percentage of unauthorized hardware assets that are accurately/uniquely identified		**1.1.H.9.1** Number of unauthorized hardware assets that are accurately/uniquely identified	OT/ED (System Logs, System Reports, Documentation)	Consult NIST IR 7693 for precise details on accurately and uniquely identifying hardware assets.
				1.1.H.9.2 Number of unauthorized hardware assets [Identical to 1.1.H.2.2]	OT/ED (Documentation)	
		1.1.H.10 Percentage of hardware assets that are actively managed		**1.1.H.10.1** Number of hardware assets that are actively managed	OT/ED (System Logs, System Reports, Documentation)	Actively managed hardware requires that an individual has been identified as being

FOR OFFICIAL USE ONLY

COI	MOE	MOP		Data Element/Type	Test Event	Notes
				1.1.H.10.2 Number of hardware assets [Identical to 1.1.H.5.2]	OT/ED (Documentation)	responsible for management of a hardware asset.
		1.1.H.11 Existence of a process for creating and maintaining an inventory of authorized hardware assets		**1.1.H.11.1** Review of documentation, processes and procedures, and output from the authorized hardware inventory creation process	OT/ED (System Logs, System Reports, Documentation)	
				1.1.H.11.2 Review of documentation, processes and procedures, and output from the authorized hardware inventory maintenance process	OT/ED (System Logs, System Reports, Documentation)	
		1.1.H.12 Mean/Max time before discovery of a change in hardware asset actual state		**1.1.H.12.1** Time of insertion of hardware assets in actual state	OT/ED (Test Agent Logs)	
				1.1.H.12.2 Time of discovery of change of hardware assets actual state	OT/ED (System Logs, System Reports, Test Agent Logs)	

FOR OFFICIAL USE ONLY

COI	MOE	MOP		Data Element/Type	Test Event	Notes
		1.1.H.13 Mean/Max time before discovery of a change in desired state hardware asset list		**1.1.H.13.1** Time of change of desired state hardware asset list	OT/ED (Test Agent Logs)	
				1.1.H.13.2 Time of discovery of authorized hardware asset list	OT/ED (System Logs, System Reports, Test Agent Logs)	
	1.1.S Software Asset Management: *Discover unauthorized or unmanaged software configuration items (SWCI) in IT assets on a network.*	**1.1.S.1** Percentage of authorized software assets on network connected IT assets that CDM identifies as "authorized" **KPP 1.1:** Threshold = 80% Objective = 95%		**1.1.S.1.1** Number of authorized software assets on network connected IT assets that CDM identifies as "authorized"	OT/ED/DT (System Logs, System Reports)	All software related MOPs may be evaluated across the network or broken down by hardware object or device role. Software products are roughly equivalent to the software identified by the NIST Common Product Enumeration (CPE). Executables are specific
				1.1.S.1.2 Number of authorized software assets on network connected IT assets	OT/ED/DT (Documentation)	

FOR OFFICIAL USE ONLY

COI	MOE	MOP		Data Element/Type	Test Event	Notes
						files in persistent memory that can be loaded into active memory and executed by the CPU. This MOP requires an independent knowledge of the software ground truth state.
		1.1.S.2 Percentage of unauthorized software assets on network connected IT assets that CDM identifies as "unauthorized" **KPP 1.1:** Threshold = 80% Objective = 95%		**1.1.S.2.1** Number of unauthorized software assets on network connected IT assets that CDM identifies as "unauthorized"	OT/ET/DT (System Logs, System Reports)	This MOP will depend on DT results. Any OT results will require the presence and independent awareness of unauthorized software assets on the network.
				1.1.S.2.2 Number of unauthorized software assets on network connected IT assets	OT/ET/DT (Documentation, Test Agent Logs)	
		1.1.S.3 Percentage of software		**1.1.S.3.1** Number of software products/executables in the	OT/ED (System Logs,	The "CDM authorized software list" is

FOR OFFICIAL USE ONLY

COI	MOE	MOP		Data Element/Type	Test Event	Notes
		products/executables in the CDM authorized software list that are authorized		CDM authorized software list that are authorized	System Reports, Documentation)	based on the ingestion of the ATO list provided by the Agency. It does not reflect the results of CDM scanning.
				1.1.S.3.2 Number of software products/executables in the CDM authorized software list	OT/ED (Documentation)	
		1.1.S.4 Percentage of software products/executables that are authorized that are included in the CDM authorized software list		**1.1.S.4.1** Number of software products/executables that are authorized that are included in the CDM authorized software list	OT/ED (System Logs, System Reports, Documentation)	
				1.1.S.4.2 Number of software products/executables that are authorized	OT/ED (Documentation)	
		1.1.S.5 Percentage of authorized software products/executables that are scanned by CDM scanners		**1.1.S.5.1** Number of authorized software products/executables that are scanned by CDM scanners	OT/ED/DT (System Logs, System Reports, Documentation)	This MOP requires an independent knowledge of the software ground truth state.
				1.1.S.5.2 Number of authorized software	OT/ED/DT	

FOR OFFICIAL USE ONLY

COI	MOE	MOP		Data Element/Type	Test Event	Notes
				products/executables	(Documentation)	
		1.1.S.6 Percentage of unauthorized software products/executables that are scanned by CDM scanners		**1.1.S.6.1** Number of unauthorized software products/executables that are scanned by CDM scanners	OT/ED/DT (System Logs, System Reports, Documentation)	This MOP requires an independent knowledge of the software ground truth state.
				1.1.S.6.2 Number of unauthorized software products/executables	OT/ED/DT (Documentation)	
		1.1.S.7 Percentage of software products/executables that are scanned by CDM scanners that do not exist		**1.1.S.7.1** Number of software products/executables that are scanned by CDM scanners that do not exist	OT/ED/DT (System Logs, System Reports, Documentation)	This MOP requires an independent knowledge of the software ground truth state.
				1.1.S.7.2 Number of software products/executables that are scanned by CDM scanners [Identical to 1.1.S.5.1]	OT/ED/DT (System Logs, System Reports, Documentation)	

FOR OFFICIAL USE ONLY

COI	MOE	MOP		Data Element/Type	Test Event	Notes
		1.1.S.8 Percentage of authorized software assets on network connected IT assets that CDM correctly associates with the specific parent hardware platform **KPP 1.2:** Threshold = 80% Objective = 95%		**1.1.S.8.1** Number of authorized software assets on network connected IT assets that CDM correctly associates with the specific parent hardware platform	OT/ED (System Logs, System Reports, Documentation)	
				1.1.S.8.2 Number of authorized software assets on network connected IT assets [Identical to 1.1.S.1.2]	OT/ED (Documentation)	
		1.1.S.9 Percentage of unauthorized software assets on network connected IT assets that CDM correctly associates with the specific parent hardware platform **KPP 1.2:** Threshold = 80% Objective = 95%		**1.1.S.9.1** Number of unauthorized software assets on network connected IT assets that CDM correctly associates with the specific parent hardware platform	OT/ED (System Logs, System Reports, Documentation)	Any OT results will require the presence and independent awareness of unauthorized software assets on the network.
				1.1.S.9.2 Number of unauthorized software assets on network connected IT assets [Identical to 1.1.S.2.2]	OT/ED (Documentation)	

FOR OFFICIAL USE ONLY

COI	MOE	MOP		Data Element/Type	Test Event	Notes
		1.1.S.10 Percentage of software products/executables that are actively managed		**1.1.S.10.1** Number of software products/executables that are actively managed	OT/ED (System Logs, System Reports, Documentation)	Actively managed software requires that an individual has been identified as being responsible for management of the software assets on a hardware asset.
				1.1.S.10.2 Number of software products/executables [Identical to 1.1.S.5.2]	OT/ED (Documentation)	
		1.1.S.11 Existence of a process for creating and maintaining an inventory of authorized software products/executables		**1.1.S.11.1** Review of documentation, processes and procedures, and output from the software inventory creation process	OT/ED (System Logs, System Reports, Documentation)	
				1.1.S.11.2 Review of documentation, processes and procedures, and output from the software inventory maintenance process	OT/ED (System Logs, System Reports, Documentation)	
		1.1.S.12 Mean/Max time before discovery of		**1.1.S.12.1** Time of insertion of software	OT/ED (Test Agent	

FOR OFFICIAL USE ONLY

COI	MOE	MOP		Data Element/Type	Test Event	Notes
		a change in software products/executables actual state		products/executables	Logs)	
				1.1.S.12.2 Time of discovery of software products/executables	OT/ED (System Logs, System Reports, Test Agent Logs)	
		1.1.S.13 Mean/Max time before discovery of a change in desired state software products/executables list		**1.1.S.13.1** Time of change in desired state software products/executables list	OT/ED (Test Agent Logs)	
				1.1.S.13.2 Time of discovery of desired state software products/executables list	OT/ED (System Logs, System Reports, Test Agent Logs)	
	1.1.C Configuration Management: *Reduce misconfiguration of IT assets including misconfigurations of hardware devices (to include physical, virtual, and*	**1.1.C.1** Percentage of authorized configurations on network connected IT assets that CDM identifies as "authorized" **KPP 1.1:** Threshold = 80%		**1.1.C.1.1** Number of authorized configurations on network connected IT assets that CDM identifies as "authorized"	OT/ED/DT (System Logs, System Reports)	
				1.1.C.1.2 Number of authorized configurations on network connected IT assets	OT/ED/DT (Documentation)	

FOR OFFICIAL USE ONLY

COI	MOE	MOP		Data Element/Type	Test Event	Notes
	operating system) and software.	Objective = 95%				
		1.1.C.2 Percentage of unauthorized configurations on network connected IT assets CDM identifies as "unauthorized" **KPP 1.1:** Threshold = 80% Objective = 95%		**1.1.C.2.1** Number of unauthorized configurations on network connected IT assets CDM identifies as "unauthorized"	OT/ED/DT (System Logs, System Reports)	
				1.1.C.2.2 Number of unauthorized configurations on network connected IT assets	OT/ED/DT (Documentation, Test Agent Log)	
		1.1.C.3 Percentage of configurations in the CDM approved configurations list that are authorized		**1.1.C.3.1** Number of configurations in the CDM approved configurations list that are authorized	OT/ED (System Logs, System Reports, Documentation)	"The CDM approved configurations setting list" is based on the CDM's ingestion of the authorized list provided by the Agency. It does not reflect the results of CDM scanning.
				1.1.C.3.2 Number of configurations in the CDM approved configurations list	OT/ED (Documentation)	
		1.1.C.4 Percentage of		**1.1.C.4.1** Number of configurations that are	OT/ED	

FOR OFFICIAL USE ONLY

COI	MOE	MOP		Data Element/Type	Test Event	Notes
		configurations that are authorized that are included in the CDM approved configurations list		authorized that are included in the CDM approved configurations list	(System Logs, System Reports, Documentation)	
				1.1.C.4.2 Number of configurations that are authorized	OT/ED (Documentation)	
		1.1.C.5 Percentage of authorized IT assets connected to the network that CDM checks for conformance		**1.1.C.5.1** Number of authorized IT assets connected to the network that CDM checks for conformance	OT/ED/DT (System Logs, System Reports, Documentation)	This MOP requires an independent and authoritative configuration settings scanner.
				1.1.C.5.2 Number authorized IT assets connected to the network	OT/ED/DT (Documentation)	
		1.1.C.6 Percentage of unauthorized IT assets connected to the network that CDM checks for conformance		**1.1.C.6.1** Number of unauthorized IT assets connected to the network that CDM checks for conformance	OT/ED/DT (System Logs, System Reports, Documentation)	

FOR OFFICIAL USE ONLY

COI	MOE	MOP		Data Element/Type	Test Event	Notes
				1.1.C.6.2 Number of unauthorized IT assets connected to the network	OT/ED/DT (Documentation)	
		1.1.C.7 Percentage of configurations identified by CDM configuration scanners that do not exist		**1.1.C.7.1** Number of configurations identified by CDM configuration scanners that do not exist	OT/ED/DT (System Logs, System Reports, Documentation)	This MOP requires an independent authoritative configuration scanner.
				1.1.C.7.2 Number of configurations identified by the CDM configuration scanners	OT/ED/DT (System Logs, System Reports, Documentation)	
		1.1.C.8 Percentage of CDM declarations of conformance that CDM correctly associates with the specific parent IT asset		**1.1.C.8.1** Number of CDM declarations of conformance that CDM correctly associates with the specific parent IT asset	OT/ED (System Logs, System Reports, Documentation)	
				1.1.C.8.2 Number of CDM declarations of conformance	OT/ED (Documentation)	

FOR OFFICIAL USE ONLY

COI	MOE	MOP		Data Element/Type	Test Event	Notes
		1.1.C.9 Percentage of CDM declarations of nonconformance that CDM correctly associates with the specific parent IT asset		**1.1.C.9.1** Number of CDM declarations of nonconformance that CDM correctly associates with the specific parent IT asset	OT/ED (System Logs, System Reports, Documentation)	
				1.1.C.9.2 Number of CDM declarations of nonconformance	OT/ED (Documentation)	
		1.1.C.10 Percentage of configurations under active configuration management		**1.1.C.10.1** Number of configurations under active configuration management	OT/ED (System Logs, System Reports, Documentation)	This assumes that configuration settings management is done by hardware object. Separate MOPs may be calculated by device role.
				1.1.C.10.2 Number of configurations	OT/ED (Documentation)	
		1.1.C.11 Existence of a process for creating and maintaining an inventory of authorized configurations		**1.1.C.11.1** Review of documentation, processes and procedures, and output from the authorized configurations creation process	OT/ED (System Logs, System Reports, Documentation)	

FOR OFFICIAL USE ONLY

COI	MOE	MOP		Data Element/Type	Test Event	Notes
				1.1.C.11.2 Review of documentation, processes and procedures, and output from the authorized configurations maintenance process	OT/ED (System Logs, System Reports, Documentation)	
		1.1.C.12 Mean/Max time before discovery of a change in the configuration actual state		**1.1.C.12.1** Time of insertion of configuration in actual state	OT/ED (Test Agent Logs)	
				1.1.C.12.2 Time of discovery of change of configuration actual state	OT/ED (System Logs, System Reports, Test Agent Logs)	
		1.1.C.13 Mean/Max time before discovery of a change in the configuration desired state		**1.1.C.13.1** Time of insertion of configuration in desired state	OT/ED (Test Agent Logs)	
				1.1.C.13.2 Time of discovery of configuration in desired state	OT/ED (System Logs, System Reports, Test Agent Logs)	

FOR OFFICIAL USE ONLY

COI	MOE	MOP		Data Element/Type	Test Event	Notes
	1.1.V Vulnerability Management: *Discover and support remediation of vulnerabilities in IT assets on a network.*	**1.1.V.1** Percentage of network connected IT assets without vulnerabilities that are scanned by and correctly identified by CDM as having no vulnerabilities		**1.1.V.1.1** Number of network connected IT assets without vulnerabilities that are scanned by and correctly identified by CDM as having no vulnerabilities	OT/ED/DT (System Logs, System Reports)	
				1.1.V.1.2 Number of network connected IT assets without vulnerabilities	OT/ED/DT (Documentation)	
		1.1.V.2 Percentage of vulnerabilities on network connected IT assets that CDM detects and reports **KPP 1.3:** Threshold = 80% Objective = 95%		**1.1.V.2.1** Number of vulnerabilities on network connected IT assets that CDM detects and reports	OT/ED/DT (System Logs, System Reports)	This MOP will depend on DT results. Any OT results will require insertions of vulnerabilities on network connected IT assets or an independent vulnerability scanner.
				1.1.V.2.2 Number of vulnerabilities on network connected IT assets	OT/ED/DT (Documentation, Test Agent Log)	
		1.1.V.3 Percentage of vulnerabilities in the CDM vulnerability list that are listed in the National Vulnerabilities		**1.1.V.3.1** Number of vulnerabilities in the CDM vulnerability list that are listed in the National Vulnerabilities Database (NVD)	OT/ED (System Logs, System Reports, Documentation)	The “CDM vulnerability list” is based on CDM’s ingestion of the NVD vulnerabilities (and other

FOR OFFICIAL USE ONLY

COI	MOE	MOP		Data Element/Type	Test Event	Notes
		Database (NVD)		**1.1.V.3.2** Number of vulnerabilities in the CDM vulnerability list	OT/ED (Documentation)	sources) list. It does not reflect the results of CDM scanning.
		1.1.V.4 Percentage of vulnerabilities in the NVD that are on the CDM vulnerabilities list		**1.1.V.4.1** Number of vulnerabilities in the NVD that are on the CDM vulnerabilities list	OT/ED (System Logs, System Reports, Documentation)	
				1.1.V.4.2 Number of vulnerabilities in the NVD	OT/ED (Documentation)	
		1.1.V.5 Percentage of authorized network connected IT assets that CDM scans for vulnerabilities		**1.1.V.5.1** Number of authorized network connected IT assets that CDM scans for vulnerabilities	OT/ED/DT (System Logs, System Reports, Documentation)	
				1.1.V.5.2 Number of authorized network connected IT assets	OT/ED/DT (Documentation)	

FOR OFFICIAL USE ONLY

COI	MOE	MOP		Data Element/Type	Test Event	Notes
		1.1.V.6 Percentage of unauthorized network connected IT assets that CDM scans for vulnerabilities		**1.1.V.6.1** Number of unauthorized network connected IT assets that CDM scans for vulnerabilities	OT/ED/DT (System Logs, System Reports, Documentation)	
				1.1.V.6.2 Number of unauthorized network connected IT assets	OT/ED/DT (Documentation)	
		1.1.V.7 Percentage of vulnerabilities identified by CDM that do not exist		**1.1.V.7.1** Number of vulnerabilities identified by CDM that do not exist	OT/ED/DT (System Logs, System Reports, Documentation)	
				1.1.V.7.2 Number of vulnerabilities identified by CDM	OT/ED/DT (System Logs, System Reports, Documentation)	
		1.1.V.8 Percentage of CDM vulnerability detections that CDM correctly		**1.1.V.8.1** Number of CDM vulnerability detections that CDM correctly associates with the specific parent IT	OT/ED (System Logs, System Reports,	

FOR OFFICIAL USE ONLY

COI	MOE	MOP		Data Element/Type	Test Event	Notes
		associates with the specific parent IT asset		asset	Documentation)	
				1.1.V.8.2 Number of CDM vulnerability detections	OT/ED (Documentation)	
		1.1.V.9 Percentage of authorized hardware assets with active vulnerability management		**1.1.V.9.1** Number of authorized hardware assets with active vulnerability management	OT/ED (System Logs, System Reports, Documentation)	This MOP assumes that vulnerability management is done at the hardware asset level.
				1.1.V.9.2 Number of authorized hardware assets	OT/ED (Documentation)	
		1.1.V.10 Existence of a process for creating and maintaining an inventory of authoritative vulnerabilities		**1.1.V.10.1** Review of documentation, processes and procedures, and output from the vulnerability list creation process	OT/ED (System Logs, System Reports, Documentation)	
				1.1.V.10.2 Review of documentation, processes and procedures, and output from the vulnerabilities list	OT/ED (System Logs, System	

FOR OFFICIAL USE ONLY

COI	MOE	MOP		Data Element/Type	Test Event	Notes
				maintenance process	Reports, Documentation)	
		1.1.V.11 Mean/Max time before discovery of a change in the vulnerability actual state		**1.1.V.11.1** Time of insertion of vulnerability	OT/ED (Test Agent Logs)	
				1.1.V.11.2 Time of discovery of vulnerability	OT/ED (System Logs, System Reports, Test Agent Logs)	
		1.1.V.12 Mean/max time before discovery of a change in the desired state vulnerability list		**1.1.V.12.1** Time of change in the desired state vulnerability list	OT/ED (Test Agent Logs)	
				1.1.V.12.2 Time of discovery of a change in the desired state vulnerability list	OT/ED (System Logs, System Reports, Test Agent Logs)	
	1.2 Manage Accounts for People and Services: CDM improves	**1.2.T.1** Percentage of authorized user/service accounts that have		**1.2.T.1.1** Number of authorized user/service accounts that have appropriate trust credentials that CDM correctly identifies	OT/ED/DT (System Logs, System	Trust credentials refer to authoritative exhibits

FOR OFFICIAL USE ONLY

COI	MOE	MOP		Data Element/Type	Test Event	Notes
	situational awareness by managing trust in people granted access, security related behavior, credentials, and account access. **ORD 3.4.2, 5.0** **(KPP 2a)**	appropriate trust credentials that CDM correctly identifies as being authorized **KPP 2a:** Threshold = 80% Objective = 95%		as being authorized	Reports)	demonstrating trust while trust attributes refer to the trust status recorded in the trusted user list.
				1.2.T.1.2 Number of authorized user/service accounts that have appropriate trust credentials	OT/ED/DT (Documentation)	
	1.2.T Manage Trust in People Granted Access: *CDM screens new and existing persons granted access for evidence that access might be abused.*	**1.2.T.2** Percentage of unauthorized user/service accounts without appropriate trust credentials that CDM correctly identifies as being unauthorized **KPP 2a:** Threshold = 80% Objective = 95%		**1.2.T.2.1** Number of unauthorized user/service accounts without appropriate trust credentials that CDM correctly identifies as being unauthorized	OT/ED/DT (System Logs, System Reports)	
				1.2.T.2.2 Number of unauthorized user/service accounts without appropriate trust credentials	OT/ED/DT (Documentation, Test Agent Log)	
		1.2.T.3 Percentage of user/service accounts on the CDM trusted users list that have		**1.2.T.3.1** Number of user/service accounts on the CDM trusted users list that have appropriate trust credentials	OT/ED (System Logs, System Reports, Documentatio	The "CDM trusted user list" is based on the ingestion of the list of

FOR OFFICIAL USE ONLY

COI	MOE	MOP		Data Element/Type	Test Event	Notes
		appropriate trust credentials			n)	users that have been authoritatively determined to be trusted.
				1.2.T.3.2 Number of user/service accounts on the CDM trusted users list	OT/ED (Documentation)	
		1.2.T.4 Percentage of user/service accounts with appropriate trust credentials that are included on the CDM trusted user list		**1.2.T.4.1** Number of user/service accounts with appropriate trust credentials that are included on the CDM trusted users list	OT/ED (System Logs, System Reports, Documentation)	
				1.2.T.4.2 Number of user/service accounts with appropriate trust credentials	OT/ED (Documentation)	
		1.2.T.5 Percentage of user/service accounts that are checked for conformance by the CDM trust scanner		**1.2.T.5.1** Number of user/service accounts that are checked for conformance by the CDM trust scanner	OT/ED/DT (System Logs, System Reports, Documentation)	
				1.2.T.5.2 Number of user/service accounts	OT/ED/DT (Documentation)	

FOR OFFICIAL USE ONLY

COI	MOE	MOP		Data Element/Type	Test Event	Notes
		1.2.T.6 Percentage of user/service accounts that are checked for conformance by the CDM trust scanner that do not exist		**1.2.T.6.1** Number of user/service accounts that are checked for conformance by the CDM trust scanner that do not exist	OT/ED/DT (System Logs, System Reports, Documentation)	
				1.2.T.6.2 Number of user/service accounts that are checked for conformance by the CDM trust scanner	OT/ED/DT (System Logs, System Reports, Documentation)	
		1.2.T.7 Percentage of authorized (trust) user/service accounts that are accurately/uniquely identified		**1.2.T.7.1** Number of authorized (trust) user/service accounts that are accurately/uniquely identified	OT/ED (System Logs, System Reports, Documentation)	
				1.2.T.7.2 Number of authorized user/service accounts	OT/ED (Documentation)	
		1.2.T.8 Percentage of unauthorized (trust) user/service accounts that are		**1.2.T.8.1** Number of unauthorized (trust) user/service accounts that are accurately uniquely	OT/ED (System Logs, System Reports,	

FOR OFFICIAL USE ONLY

COI	MOE	MOP		Data Element/Type	Test Event	Notes
		accurately uniquely identified		identified	Documentation)	
				1.2.T.8.2 Number of unauthorized user/service accounts	OT/ED (Documentation)	
		1.2.T.9 Percentage of user/service accounts with active trust account management		**1.2.T.9.1** Number of user/service accounts with active trust account management	OT/ED (System Logs, System Reports, Documentation)	
				1.2.T.9.2 Number of user/service accounts	OT/ED (Documentation)	
		1.2.T.10 Existence of a process for creating and maintaining an inventory of trusted user/service accounts		**1.2.T.10.1** Review of documentation, processes and procedures, and output from the trusted user/service account inventory creation process	OT/ED (System Logs, System Reports, Documentation)	
				1.2.T.10.2 Review of documentation, processes and procedures, and output from the trusted user/service	OT/ED (System Logs, System	

FOR OFFICIAL USE ONLY

COI	MOE	MOP		Data Element/Type	Test Event	Notes
				account inventory maintenance process	Reports, Documentation)	
		1.2.T.11 Mean/Max time before discovery of a change in the trust actual state		**1.2.T.11.1** Time of insertion of a change in the trust actual state	OT/ED (Test Agent Logs)	
				1.2.T.11.2 Time of discovery of a change in the trust actual state	OT/ED (System Logs, System Reports, Test Agent Logs)	
		1.2.T.12 Mean/Max time before discovery of a change in the trust desired state		**1.2.T.12.1** Time of insertion a change in the trust desired state	OT/ED (Test Agent Logs)	
					OT/ED (System Logs, System Reports, Test Agent Logs)	
				1.2.T.12.2 Time of discovery of a change in the trust desired state		
	1.2.B Manage Security Related Behavior: *CDM prevents general users from taking*	**1.2.B.1** Percentage of authorized user/service accounts that have		**1.2.B.1.1** Number of authorized user/service accounts that have appropriate security-related behavior credentials that	OT/ED/DT (System Logs, System	Appropriate security-related behavior credentials are

FOR OFFICIAL USE ONLY

COI	MOE	MOP		Data Element/Type	Test Event	Notes
	unnecessary risks to prevent attackers from exploiting network and application users via social engineering scams.	appropriate security-related behavior credentials that CDM correctly identifies as being authorized **KPP 2a:** Threshold = 80% Objective = 95%		CDM correctly identifies as being authorized	Reports)	defined by CDM as user agreements, training, job requirements, or similar evidence.
				1.2.B.1.2 Number of authorized user/service accounts that have appropriate security-related behavior credentials	OT/ED/DT (Documentation)	
		1.2.B.2 Percentage of unauthorized user/service accounts without appropriate security-related behavior credentials that CDM correctly identifies as being unauthorized **KPP 2a:** Threshold = 80% Objective = 95%		**1.2.B.2.1** Number of unauthorized user/service accounts without appropriate security-related behavior credentials that CDM correctly identifies as being unauthorized	OT/ED/DT (System Logs, System Reports)	
				1.2.B.2.2 Number of unauthorized user/service accounts without appropriate security-related behavior credentials	OT/ED/DT (Documentation, Test Agent Log)	
		1.2.B.3 Percentage of		**1.2.B.3.1** Number of user/service accounts on the	OT/ED	The "CDM security-

FOR OFFICIAL USE ONLY

COI	MOE	MOP		Data Element/Type	Test Event	Notes
		user/service accounts on the CDM security-related users list that have appropriate security-related behavior credentials		CDM security-related behavior users list that have appropriate security-related credentials	(System Logs, System Reports, Documentation)	related behavior user list" is based on the ingestion of the list of users that have been authoritatively determined to have appropriate security-related attributes.
				1.2.B.3.2 Number of user/service accounts on the CDM security-related behavior users list	OT/ED (Documentation)	
		1.2.B.4 Percentage of user/service accounts with appropriate security-related behavior credentials that are included on the CDM security-related behavior user list		**1.2.B.4.1** Number of user/service accounts with appropriate security-related behavior credentials that are included on the CDM security-related behavior users list	OT/ED (System Logs, System Reports, Documentation)	
				1.2.B.4.2 Number of user/service accounts with appropriate security-related behavior credentials	OT/ED (Documentation)	
		1.2.B.5 Percentage of user/service accounts that are checked for		**1.2.B.5.1** Number of user/service accounts that are checked for conformance by the CDM security-related behavior	OT/ED/DT (System Logs, System Reports,	

FOR OFFICIAL USE ONLY

COI	MOE	MOP		Data Element/Type	Test Event	Notes
		conformance by the CDM security-related behavior scanner		scanner	Documentation)	
				1.2.B.5.2 Number of user/service accounts [Identical to 1.2.T.5.2]	OT/ED/DT (Documentation)	
		1.2.B.6 Percentage of user/service accounts identified by the CDM security-related behavior scanner that do not exist		**1.2.B.6.1** Number of user/service accounts identified by the CDM security-related behavior scanner that do not exist	OT/ED/DT (System Logs, System Reports, Documentation)	
				1.2.B.6.2 Number of user/service accounts identified by the CDM security-related behavior scanner	OT/ED/DT (System Logs, System Reports, Documentation)	
		1.2.B.7 Percentage of authorized (behavior) user/service accounts that are accurately/uniquel		**1.2.B.7.1** Number of authorized (behavior) user/service accounts that are accurately/uniquely identified	OT/ED (System Logs, System Reports, Documentation)	

FOR OFFICIAL USE ONLY

COI	MOE	MOP		Data Element/Type	Test Event	Notes
		y identified		**1.2.B.7.2** Number of authorized (behavior) user/service accounts	OT/ED (Documentation)	
		1.2.B.8 Percentage of unauthorized (behavior) user/service accounts that are accurately/uniquely identified		**1.2.B.8.1** Number of unauthorized (behavior) user/service accounts that are accurately/uniquely identified	OT/ED (System Logs, System Reports, Documentation)	
				1.2.B.8.2 Number of unauthorized (behavior) user/service accounts	OT/ED (Documentation)	
		1.2.B.9 Percentage of user/service accounts with active behavior account management		**1.2.B.9.1** Number of user/service accounts with active behavior account management	OT/ED (System Logs, System Reports, Documentation)	
				1.2.B.9.2 Number of user/service accounts [Identical to 1.2.T.5.2]	OT/ED (Documentation)	
		1.2.B.10 Existence of a process for		**1.2.B.10.1** Review of documentation, processes	OT/ED	

FOR OFFICIAL USE ONLY

COI	MOE	MOP		Data Element/Type	Test Event	Notes
		creating and maintaining an inventory of security-related behavior authorized user/service accounts		and procedures, and output from the security-related behavior authorized user/service account inventory creation process	(System Logs, System Reports, Documentation)	
				1.2.B.10.2 Review of documentation, processes and procedures, and output from the security-related behavior authorized user/service account inventory maintenance process	OT/ED (System Logs, System Reports, Documentation)	
		1.2.B.11 Mean/Max time before discovery of a change in the behavior actual state		**1.2.B.11.1** Time of insertion of a change in the behavior actual state	OT/ED (Test Agent Logs)	
				1.2.B.11.2 Time of discovery of a change in the behavior actual state	OT/ED (System Logs, System Reports, Test Agent Logs)	
		1.2.B.12 Mean/Max time before discovery of a change in the behavior desired		**1.2.B.12.1** Time of insertion a change in the behavior desired state	OT/ED (Test Agent Logs)	

FOR OFFICIAL USE ONLY

COI	MOE	MOP		Data Element/Type	Test Event	Notes
		state		**1.2.B.12.2** Time of discovery of a change in the behavior desired state	OT/ED (System Logs, System Reports, Test Agent Logs)	
	1.2.C Manage Credentials and Authentication: *CDM prevents (a) the binding of credentials to or (b) the user of credentials by other than the rightful owner (person or service) by careful management of credentials, preventing attackers from using hijacked credentials to gain unauthorized control of resources, especially administrative rights.*	**1.2.C.1** Percentage of authorized user/service accounts that have appropriate credential associated attributes that CDM correctly identifies as being authorized **KPP 2a:** Threshold = 80% Objective = 95%		**1.2.C.1.1** Number of authorized user/service accounts that have appropriate credential associated attributes that CDM correctly identifies as being authorized	OT/ED/DT (System Logs, System Reports)	
				1.2.C.1.2 Number of authorized user/service accounts that have appropriate credential associated attributes	OT/ED/DT (Documentation)	
		1.2.C.2 Percentage of unauthorized user/service accounts without appropriate credential associated		**1.2.C.2.1** Number of unauthorized user/service accounts without appropriate credential associated attributes that CDM correctly identifies as being unauthorized	OT/ED/DT (System Logs, System Reports)	

FOR OFFICIAL USE ONLY

COI	MOE	MOP		Data Element/Type	Test Event	Notes
		attributes that CDM correctly identifies as being unauthorized **KPP 2a:** Threshold = 80% Objective = 95%		**1.2.C.2.2** Number of unauthorized user/service accounts without appropriate credential associated attributes	OT/ED/DT (Documentation, Test Agent Log)	
		1.2.C.3 Percentage of user/service accounts on the CDM credential-related users list that have appropriate credential associated attributes		**1.2.C.3.1** Number of user/service accounts on the CDM credential-related users list that have appropriate credential associated attributes	OT/ED (System Logs, System Reports, Documentation)	The "CDM credential-related user list" is based on the ingestion of the list of users that have been authoritatively determined to have appropriate credential associated attributes.
				1.2.C.3.2 Number of user/service accounts on the CDM credential-related users list	OT/ED (Documentation)	
		1.2.C.4 Percentage of user/service accounts with appropriate credential associated		**1.2.C.4.1** Number of user/service accounts with appropriate credential associated attributes that are included on the CDM credential-related users list	OT/ED (System Logs, System Reports, Documentatio	

FOR OFFICIAL USE ONLY

COI	MOE	MOP		Data Element/Type	Test Event	Notes
		attributes that are included on the CDM credential-related user list			n)	
				1.2.C.4.2 Number of user/service accounts with appropriate credential associated attributes	OT/ED (Documentation)	
		1.2.C.5 Percentage of user/service accounts that are checked for conformance by the CDM credential scanner		**1.2.C.5.1** Number of user/service accounts that are checked for conformance by the CDM credential scanner	OT/ED/DT (System Logs, System Reports, Documentation)	
				1.2.C.5.2 Number of user/service accounts [Identical to 1.2.T.5.2]	OT/ED/DT (Documentation)	
		1.2.C.6 Percentage of user/service accounts that are checked for conformance by the CDM credential scanner that do not exist		**1.2.C.6.1** Number of user/service accounts checked for conformance by the CDM credential scanner that do not exist	OT/ED/DT (System Logs, System Reports, Documentation)	
				1.2.C.6.2 Number of user/service accounts identified by the CDM credential scanner	OT/ED/DT (System Logs, System Reports,	

FOR OFFICIAL USE ONLY

COI	MOE	MOP		Data Element/Type	Test Event	Notes
					Documentation)	
		1.2.C.7 Percentage of authorized (credential) user/service accounts that are accurately/uniquely identified		**1.2.C.7.1** Number of authorized (credential) user/service accounts that are accurately/uniquely identified	OT/ED (System Logs, System Reports, Documentation)	
				1.2.C.7.2 Number of authorized user/service accounts	OT/ED (Documentation)	
		1.2.C.8 Percentage of unauthorized (credential) user/service accounts that are accurately/uniquely identified		**1.2.C.8.1** Number of unauthorized (credential) user/service accounts that are accurately/uniquely identified	OT/ED (System Logs, System Reports, Documentation)	
				1.2.C.8.2 Number of unauthorized user/service accounts	OT/ED (Documentation)	
		1.2.C.9 Percentage of user/service accounts with		**1.2.C.9.1** Number of user/service accounts with active credential account	OT/ED (System Logs, System	

FOR OFFICIAL USE ONLY

COI	MOE	MOP		Data Element/Type	Test Event	Notes
		active credential account management		management	Reports, Documentation)	
				1.2.C.9.2 Number of user/service accounts	OT/ED (Documentation)	
		1.2.C.10 Existence of a process for creating and maintaining an inventory of credential-related authorized user/service accounts		**1.2.C.10.1** Review of documentation, processes and procedures, and output from the credential-related authorized user/service account inventory creation process	OT/ED (System Logs, System Reports, Documentation)	
				1.2.C.10.2 Review of documentation, processes and procedures, and output from the credential-related authorized user/service account inventory maintenance process	OT/ED (System Logs, System Reports, Documentation)	
		1.2.C.11 Mean/Max time before discovery of a change in the credential actual state		**1.2.C.11.1** Time of insertion of a change in the credential actual state	OT/ED (Test Agent Logs)	
				1.2.C.11.2 Time of discovery of a change in the credential	OT/ED (System Logs,	

FOR OFFICIAL USE ONLY

COI	MOE	MOP		Data Element/Type	Test Event	Notes
				actual state	System Reports, Test Agent Logs)	
		1.2.C.12 Mean/Max time before discovery of a change in the credential desired state		**1.2.C.12.1** Time of insertion a change in the credential desired state	OT/ED (Test Agent Logs)	
				1.2.C.12.2 Time of discovery of a change in the credential desired state	OT/ED (System Logs, System Reports, Test Agent Logs)	
	1.2.P Manage Account Access: *CDM prevents access beyond what is needed to meet business mission by limiting account access and eliminating unneeded accounts to prevent attackers from gaining unauthorized access to*	**1.2.P.1** Percentage of authorized user/service accounts that have appropriate privilege associated attributes that CDM correctly identifies as being authorized **KPP 2a:** Threshold = 80%		**1.2.P.1.1** Number of authorized user/service accounts that have appropriate privilege associated attributes that CDM correctly identifies as being authorized	OT/ED/DT (System Logs, System Reports)	
				1.2.P.1.2 Number of authorized user/service accounts that have appropriate privilege associated attributes	OT/ED/DT (Documentation)	

FOR OFFICIAL USE ONLY

COI	MOE	MOP		Data Element/Type	Test Event	Notes
	sensitive data.	Objective = 95%				
		1.2.P.2 Percentage of unauthorized user/service accounts without appropriate privilege associated attributes that CDM correctly identifies as being unauthorized **KPP 2a:** Threshold = 80% Objective = 95%		**1.2.P.2.1** Number of unauthorized user/service accounts without appropriate privilege associated attributes that CDM correctly identifies as being unauthorized	OT/ED/DT (System Logs, System Reports)	
				1.2.P.2.2 Number of unauthorized user/service accounts without appropriate privilege associated attributes	OT/ED/DT (Documentation, Test Agent Log)	
		1.2.P.3 Percentage of user/service accounts on the CDM privilege-related users list that have appropriate privilege associated attributes		**1.2.P.3.1** Number of user/service accounts on the CDM privilege-related users list that have appropriate privilege associated attributes	OT/ED (System Logs, System Reports, Documentation)	
				1.2.P.3.2 Number of user/service accounts on the CDM privilege-related users list	OT/ED (Documentation)	

FOR OFFICIAL USE ONLY

COI	MOE	MOP		Data Element/Type	Test Event	Notes
		1.2.P.4 Percentage of user/service accounts with appropriate privilege associated attributes that are included on the CDM privilege-related user list		**1.2.P.4.1** Number of user/service accounts with appropriate privilege associated attributes that are included on the CDM privilege-related users list	OT/ED (System Logs, System Reports, Documentation)	
				1.2.P.4.2 Number of user/service accounts with appropriate privilege associated attributes	OT/ED (Documentation)	
		1.2.P.5 Percentage of user/service accounts that are checked for conformance by the CDM privilege scanner		**1.2.P.5.1** Number of user/service accounts that are checked for conformance by the CDM privilege scanner	OT/ED/DT (System Logs, System Reports, Documentation)	
				1.2.P.5.2 Number of user/service accounts [Identical to 1.2.T.5.2]	OT/ED/DT (Documentation)	
		1.2.P.6 Percentage of user/service accounts that are checked for conformance by the CDM privilege scanner that do		**1.2.P.6.1** Number of user/service accounts that are checked for conformance by the CDM privilege scanner that do not exist	OT/ED/DT (System Logs, System Reports, Documentation)	

FOR OFFICIAL USE ONLY

COI	MOE	MOP		Data Element/Type	Test Event	Notes
		not exist		**1.2.P.6.2** Number of user/service accounts that are checked for conformance by the CDM privilege scanner	OT/ED/DT (System Logs, System Reports, Documentation)	
		1.2.P.7 Percentage of authorized (privilege) user/service accounts that are accurately/uniquely identified		**1.2.P.7.1** Number of authorized (privilege) user/service accounts that are accurately/uniquely identified	OT/ED (System Logs, System Reports, Documentation)	
				1.2.P.7.2 Number of authorized (privilege) user/service accounts	OT/ED (Documentation)	
		1.2.P.8 Percentage of unauthorized (privilege) user/service accounts that are accurately/uniquely identified		**1.2.P.8.1** Number of unauthorized (privilege) user/service accounts that are accurately/uniquely identified	OT/ED (System Logs, System Reports, Documentation)	
				1.2.P.8.2 Number of unauthorized (privilege) user/service accounts	OT/ED (Documentation)	

FOR OFFICIAL USE ONLY

COI	MOE	MOP		Data Element/Type	Test Event	Notes
		1.2.P.9 Percentage of user/service accounts with active privilege account management		**1.2.P.9.1** Number of user/service accounts with active privilege account management	OT/ED (System Logs, System Reports, Documentation)	
				1.2.P.9.2 Number of user/service accounts	OT/ED (Documentation)	
		1.2.P.10 Existence of a process for creating and maintaining an inventory of privilege-related authorized user/service accounts		**1.2.P.10.1** Review of documentation, processes and procedures, and output from the privilege-related authorized user/service account inventory creation process	OT/ED (System Logs, System Reports, Documentation)	
				1.2.P.10.2 Review of documentation, processes and procedures, and output from the privilege-related authorized user/service account inventory maintenance process	OT/ED (System Logs, System Reports, Documentation)	
		1.2.P.11 Mean/Max time before discovery of a change in the privilege actual		**1.2.P.11.1** Time of insertion of a change in the privilege actual state	OT/ED (Test Agent Logs)	

FOR OFFICIAL USE ONLY

COI	MOE	MOP		Data Element/Type	Test Event	Notes
		state		**1.2.P.11.2** Time of discovery of a change in the privilege actual state	OT/ED (System Logs, System Reports, Test Agent Logs)	
		1.2.P.12 Mean/Max time before discovery of a change in the privilege desired state		**1.2.P.12.1** Time of insertion a change in the privilege desired state	OT/ED (Test Agent Logs)	
				1.2.P.12.2 Time of discovery of a change in the privilege desired state	OT/ED (System Logs, System Reports, Test Agent Logs)	
	1.3 Manage Events and Security Lifecycle CDM improves situational awareness by managing network access, events, and the security lifecycle. **ORD 3.4.3, 5.0**	**1.3.B.1** Percentage of authorized network connections that have appropriate network connection attributes that CDM correctly identifies as being authorized.				

FOR OFFICIAL USE ONLY

COI	MOE	MOP		Data Element/Type	Test Event	Notes
	(KPP 2b, 2c, 4.1, 5)					
2 Security Posture: Do CDM information exchanges, scoring rules, and implementations improve the security posture of government networks?	**2.1 Agency Security Posture:** CDM information exchanges, scoring rules, and implementations improve the security posture of Agency networks. **ORD 3.4.5** **(KPP 3a)**	**2.1.1** Percent of CDM users that believe CDM has enhanced the security operations of Agency networks		**2.1.1.1** Results from survey questionnaires given to CDM users	OT/ED	Considerations should include the impact of reduced workload, ad hoc reporting and changes in reporting periodicity on risk scores and on the integrity of composite pictures developed from non-synchronized data.
				2.1.1.2 Reviews of relevant studies and documentation		
		2.1.2 Change in Agency overall risk scores (adjusted for scoring rule changes) over time		**2.1.2.1** Agency overall risk scores over time	OT/ED	
				2.1.2.2 Scoring rule changes over time		
		2.1.3 Mean/Max time before discovery of unauthorized		**2.1.3.1** Times of insertions of unauthorized hardware assets	OT/ED (Test Agent	Any OT results will require the presence and independent

FOR OFFICIAL USE ONLY

COI	MOE	MOP		Data Element/Type	Test Event	Notes
		hardware assets			Logs)	awareness of unauthorized hardware assets on the network.
				2.1.3.2 Times of discoveries of unauthorized hardware assets	OT/ED (System Logs, System Reports, Test Agent Logs)	
		2.1.4 Mean/Max time to take action concerning unauthorized hardware assets from the network		**2.1.4.1** Times of discoveries of unauthorized hardware assets [Identical to 2.1.3.2]	OT/ED (System Logs, System Reports, Test Agent Logs)	Any OT results will require the presence and independent awareness of unauthorized hardware assets on the network.
				2.1.4.2 Times of actions concerning unauthorized hardware assets	OT/ED (System Logs, System Reports, Test Agent Logs)	
		2.1.5 Percentage of unauthorized hardware assets identified by CDM as unauthorized that lead to follow-on events (e.g., removal or addition to authorized list)		**2.1.5.1** Number of unauthorized hardware assets identified by CDM as unauthorized that lead to follow-on events	OT/ED (System Logs, System Reports, Test Agent Logs)	Any OT results will require the presence and independent awareness of unauthorized hardware assets on the network.
				2.1.5.2 Number of unauthorized hardware assets identified by CDM as	OT/ED (System Logs,	

FOR OFFICIAL USE ONLY

COI	MOE	MOP		Data Element/Type	Test Event	Notes
				unauthorized	System Report)	
		2.1.6 Mean/Max time before discovery of unauthorized software products/executables		**2.1.6.1** Times of insertion of unauthorized software products/executables	OT/ED (Test Agent Logs)	Any OT results will require the presence and independent awareness of unauthorized software assets on the network.
				2.1.6.2 Times of discovery of unauthorized software products/executables	OT/ED (System Logs, System Reports, Test Agent Logs)	
		2.1.7 Mean/Max time to take action concerning unauthorized software products/executables		**2.1.7.1** Times of discovery of unauthorized software products/executables [Identical to 2.1.6.2]	OT/ED (System Logs, System Reports, Test Agent Logs)	Any OT results will require the presence and independent awareness of unauthorized software assets on the network.
				2.1.7.2 Times of actions concerning unauthorized software products/executables	OT/ED (System Logs, System Reports, Test Agent Logs)	
		2.1.8 Percentage of unauthorized software products/executabl		**2.1.8.1** Number of unauthorized software products/executables identified by CDM as	OT/ED (System Logs, System	Any OT results will require the presence and independent

FOR OFFICIAL USE ONLY

COI	MOE	MOP		Data Element/Type	Test Event	Notes
		es identified by CDM as unauthorized that lead to follow-on events (e.g., removal or addition to authorized list)		unauthorized that lead to follow-on events (e.g., removal or addition to authorized list)	Reports, Test Agent Logs)	awareness of unauthorized software assets on the network.
				2.1.8.2 Number of unauthorized software products/executables identified by CDM as unauthorized	OT/ED (System Logs, System Reports)	
		2.1.9 Mean/Max time before discovery of unauthorized configurations		**2.1.9.1** Times of insertion of unauthorized configurations	OT/ED (Test Agent Logs)	This MOP will require the insertion of unauthorized configuration settings into the network.
				2.1.9.2 Times of discovery of unauthorized configurations	OT/ED (System Logs, System Reports, Test Agent Logs)	
		2.1.10 Mean/Max time to take action concerning unauthorized configurations		**2.1.10.1** Times of discovery of unauthorized configurations [Identical to 2.1.9.2]	OT/ED (System Logs, System Reports, Test Agent Logs)	This MOP will require the insertion of unauthorized configuration settings into the enclave.
				2.1.10.2 Times of taking action concerning	OT/ED (System Logs,	

FOR OFFICIAL USE ONLY

COI	MOE	MOP		Data Element/Type	Test Event	Notes
				unauthorized configurations	System Reports, Test Agent Logs)	
		2.1.11 Percentage of CDM declarations of nonconformance that lead to follow-on corrective actions		**2.1.11.1** Number of CDM declarations of nonconformance that lead to follow-on corrective actions	OT/ED (System Logs, System Reports, Test Agent Logs)	
				2.1.11.2 Number of CDM declarations of nonconformance	OT/ED (System Logs, System Report)	
		2.1.12 Mean/Max time before discovery of a vulnerability		**2.1.12.1** Times of vulnerability insertions	OT/ED (Test Agent Logs)	This MOP will depend on DT results. Any OT results will require insertions of vulnerabilities into the network or an independent vulnerability scanner.
				2.1.12.2 Times of vulnerability discoveries	OT/ED (System Logs, System Reports, Test Agent Logs)	
		2.1.13 Mean/Max time to take action concerning a		**2.1.13.1** Times of vulnerability discovery [Identical to 2.1.12.2]	OT/ED (System Logs, System	This MOP will depend on DT results. Any OT results will

FOR OFFICIAL USE ONLY

COI	MOE	MOP		Data Element/Type	Test Event	Notes
		vulnerability			Reports, Test Agent Logs)	require insertions of vulnerabilities into the network or an independent vulnerability scanner.
				2.1.13.2 Times of taking action concerning vulnerability	OT/ED (System Logs, System Reports, Test Agent Logs)	
		2.1.14 Percentage of CDM identified vulnerabilities that lead to follow-on corrective action		**2.1.14.1** Number of CDM identified vulnerabilities that lead to follow-on corrective action	OT/ED (System Logs, System Reports, Test Agent Logs)	
				2.1.14.2 Number of CDM identified vulnerabilities	OT/ED (System Logs, System Report)	
		2.1.15 Mean/Max time before discovery of a user/service account without appropriate trust credentials		**2.1.15.1** Times of insertion of a user/service account without appropriate trust credentials	OT/ED (Test Agent Logs)	
				2.1.15.2 Times of discovery of user/service accounts without appropriate trust credentials	OT/ED (System Logs, System Reports, Test	

FOR OFFICIAL USE ONLY

COI	MOE	MOP		Data Element/Type	Test Event	Notes
					Agent Logs)	
		2.1.16 Mean/Max time to take action concerning the user/service account without appropriate trust credentials		**2.1.16.1** Times of discovery of user/service account without appropriate trust attributes [Identical to 2.4.15.2]	OT/ED (System Logs, System Reports, Test Agent Logs)	
				2.1.16.2 Times of taking action concerning the user/service account without appropriate trust credentials	OT/ED (System Logs, System Reports, Test Agent Logs)	
		2.1.17 Percentage user/service accounts CDM identifies as unauthorized (trust) that lead to follow-on corrective actions		**2.1.17.1** Number of user/service accounts CDM identifies as unauthorized (trust) that lead to follow-on corrective actions	OT/ED (System Logs, System Reports, Test Agent Logs)	This MOP refers to trust-related authorizations.
				2.1.17.2 Number of user/service accounts that CDM identifies as unauthorized (trust)	OT/ED (System Logs, System Report)	
		2.1.18 Mean/Max time before discovery of a		**2.1.18.1** Times of insertion of a user/service account without appropriate security-	OT/ED (Test Agent	

FOR OFFICIAL USE ONLY

COI	MOE	MOP		Data Element/Type	Test Event	Notes
		user/service account without appropriate security-related behavior credentials		related behavior credentials	Logs)	
				2.1.18.2 Times of discovery of user/service accounts without appropriate security-related behavior credentials	OT/ED (System Logs, System Reports, Test Agent Logs)	
		2.1.19 Mean/Max time to take action concerning the user/service account without appropriate security-related behavior credentials		**2.1.19.1** Times of discovery of user/service account without appropriate security-related behavior attributes [Identical to 2.1.18.2]	OT/ED (System Logs, System Reports, Test Agent Logs)	
				2.1.19.2 Times of taking action concerning the user/service account without appropriate security-related behavior credentials	OT/ED (System Logs, System Reports, Test Agent Logs)	
		2.1.20 Percentage user/service accounts CDM identifies as unauthorized (behavior) that lead to follow-on corrective actions		**2.1.20.1** Number of user/service accounts CDM identifies as unauthorized (behavior) that lead to follow-on corrective actions	OT/ED (System Logs, System Reports, Test Agent Logs)	This MOP refers to behavior related authorizations.
				2.1.20.2 Number of user/service accounts that CDM identifies as (behavior)	OT/ED (System Logs,	

FOR OFFICIAL USE ONLY

COI	MOE	MOP		Data Element/Type	Test Event	Notes
				unauthorized	System Report)	
		2.1.21 Mean/Max time before discovery of a user/service account without appropriate credential associated attributes		**2.1.21.1** Times of insertion of a user/service account without appropriate credential associated attributes	OT/ED (Test Agent Logs)	
				2.1.21.2 Times of discovery of user/service accounts without appropriate credential associated attributes	OT/ED (System Logs, System Reports, Test Agent Logs)	
		2.1.22 Mean/Max time to take action concerning the user/service account without appropriate credential associated attributes		**2.1.22.1** Times of discovery of user/service account without appropriate credential associated attributes [Identical to 2.1.21.2]	OT/ED (System Logs, System Reports, Test Agent Logs)	
				2.1.22.2 Times of taking action concerning the user/service account without appropriate credential associated attributes	OT/ED (System Logs, System Reports, Test Agent Logs)	
		2.1.23 Percentage user/service accounts CDM		**2.1.23.1** Number of user/service accounts CDM identifies as unauthorized	OT/ED (System Logs,	

FOR OFFICIAL USE ONLY

COI	MOE	MOP		Data Element/Type	Test Event	Notes
		identifies as unauthorized (credential) that lead to follow-on corrective actions		(credential) that lead to follow-on corrective actions	System Reports, Test Agent Logs)	
				2.1.23.2 Number of user/service accounts that CDM identifies as (credential) unauthorized	OT/ED (System Logs, System Report)	
		2.1.24 Mean/Max time before discovery of a user/service account without appropriate privilege associated attributes		**2.1.24.1** Times of insertion of a user/service account without appropriate privilege associated attributes	OT/ED (Test Agent Logs)	
				2.1.24.2 Times of discovery of user/service accounts without appropriate privilege associated attributes	OT/ED (System Logs, System Reports, Test Agent Logs)	
		2.1.25 Mean/Max time to take action concerning the user/service account without appropriate privilege associated attributes		**2.1.25.1** Times of discovery of user/service account without appropriate privilege associated attributes [Identical to 2.1.24.2]	OT/ED (System Logs, System Reports, Test Agent Logs)	
				2.1.25.2 Times of taking action concerning the user/service account without appropriate privilege	OT/ED (System Logs, System	

FOR OFFICIAL USE ONLY

COI	MOE	MOP		Data Element/Type	Test Event	Notes
				associated attributes	Reports, Test Agent Logs)	
		2.1.26 Percentage user/service accounts CDM identifies as unauthorized (privilege) that lead to follow-on corrective actions		**2.1.26.1** Number of user/service accounts CDM identifies as unauthorized (privilege) that lead to follow-on corrective actions	OT/ED (System Logs, System Reports, Test Agent Logs)	
				2.1.26.2 Number of user/service accounts that CDM identifies as (privilege) unauthorized	OT/ED (System Logs, System Report)	
	2.2 Federal Security Posture: CDM information exchanges, scoring rules, and implementations improve the security posture of agency networks. **ORD 3.4.4, 3.4.5** **(KPP 3a)**	**2.2.1** Percent of CDM users that believe CDM has enhanced the security operations of Federal networks		**2.2.1.1** Results from survey questionnaires given to CDM users	OT/ED	Considerations should include the impact of reduced workload, ad hoc reporting and changes in reporting periodicity on risk scores and on the integrity of composite pictures developed from non-synchronized
				2.2.1.2 Reviews of relevant studies and documentation		

FOR OFFICIAL USE ONLY

COI	MOE	MOP		Data Element/Type	Test Event	Notes
						data.
		2.2.2 Change in Federal overall risk scores (adjusted for scoring rule changes) over time		**2.2.2.1** Federal overall risk scores over time	OT/ED	
				2.2.2.2 Scoring rule changes over time		
	2.3 Dashboard – Dashboard Interoperability: CDM information exchanges improve the security posture of federal networks. **ORD 3.4.4, 3.4.5, 4.2** **(KPP 3a)**	**2.3.1** Percentage of CDM capabilities available for participating Agencies to implement that Agencies successfully report to the Federal Dashboard **KPP 5:** Threshold = 80% Objective = 95%		**2.3.1.1** Number of CDM capabilities available for participating Agencies to implement that Agencies successfully report to the Federal Dashboard	DT/ED/OT (System Logs, System Reports)	
				2.3.1.2 Number of CDM capabilities available for participating Agencies to implement		
		2.3.2 Percentage CDM capabilities available for participating Agencies to implement that Agencies		**2.3.2.1** Number of CDM capabilities available for participating Agencies to implement that Agencies successfully report to the Federal Dashboard and the Federal Dashboard	DT/ED/OT (System Logs, System Reports)	

FOR OFFICIAL USE ONLY

COI	MOE	MOP		Data Element/Type	Test Event	Notes
		successfully report to the Federal Dashboard and the Federal Dashboard accurately aggregates **KPP 6:** Threshold = 80% Objective = 95%		accurately aggregates		
				2.3.2.2 Number of CDM capabilities available for participating Agencies to implement [Identical to 2.3.1.2]		
		2.3.3 Percentage of CDM capabilities available for participating Agencies to implement that Agencies accurately report to the Federal Dashboard		**2.3.3.1** Number of CDM capabilities available for participating Agencies to implement that Agencies accurately report to the Federal Dashboard	DT/ED/OT (System Logs, System Reports)	
				2.3.3.2 Number of CDM capabilities available for participating Agencies to implement [Identical to 2.3.1.2]		
		2.3.4 Mean/Max time between data collection and display by the Federal Dashboard of data		**2.3.4.1** Time of data collection of data from CDM capabilities available for participating Agencies to implement that Agencies report to the Federal	DT/ED/OT (System Logs, System	

FOR OFFICIAL USE ONLY

COI	MOE	MOP		Data Element/Type	Test Event	Notes
		from CDM capabilities available for participating Agencies to implement that Agencies report to the Federal Dashboard		Dashboard	Reports)	
				2.3.4.2 Time of display by the Federal Dashboard of data from CDM capabilities available for participating Agencies to implement that Agencies report to the Federal Dashboard		
		2.3.5 Percentage of scoring rules and changes that are received by the Agency dashboards		**2.3.5.1** Number of scoring rules and changes that are received by Agency dashboards	DT/ED/OT (System Logs, System Reports)	
				2.3.5.2 Number of scoring rules and changes that are transmitted by the Federal Dashboard		
		2.3.6 Percentage of risk scoring rules and changes that are implemented by the Agency dashboard		**2.3.6.1** Number of scoring rules and changes that are implemented by the Agency dashboard	DT/ED/OT (System Logs, System Reports)	
				2.3.6.2 Number of scoring rules and changes that are received by Agency dashboards [Identical to 2.3.5.1]		

FOR OFFICIAL USE ONLY

COI	MOE	MOP		Data Element/Type	Test Event	Notes
		2.3.7 Percentage of scoring rules and changes in reporting categories that are accurately received by the Agency dashboards		**2.3.7.1** Number of scoring rules and changes in reporting categories accurately that are received by Agency dashboards	DT/ED/OT (System Logs, System Reports)	
				2.3.7.2 Number of scoring rules and changes that are transmitted by the Federal Dashboard [Identical to 2.3.5.2]		
		2.3.8 Percentage of risk scoring policy changes that are accurately implemented by the Agency dashboard		**2.3.8.1** Number of risk scoring policy changes that are accurately implemented by the agency dashboard	DT/ED/OT (System Logs, System Reports)	
				2.3.8.2 Number of risk scoring policy changes that are implemented by the agency dashboard		
		2.3.9 Mean/Max time between transmission of scoring rules and changes in reporting categories from Federal dashboard and implementation by Agency		**2.3.9.1** Times of transmissions of scoring rules and changes in categories from the Federal dashboard	OT/ED/DT (System Logs, System Reports)	
				2.3.9.2 Times of receipts of scoring rules and changes in categories by the Agency dashboards		

FOR OFFICIAL USE ONLY

COI	MOE	MOP		Data Element/Type	Test Event	Notes
		dashboards				
		2.3.10 Percentage of custom queries that are transmitted to Agency dashboards		**2.3.10.1** Number of custom queries that are transmitted to Agency dashboards	OT/ED/DT	
				2.3.1.2 Number of custom queries		
		2.3.11 Percentage of custom queries that are received by the Agency dashboard		**2.3.11.1** Number of custom queries that are received by the Agency dashboard	OT/ED/DT	
				2.3.11.2 Number of custom queries that are transmitted by the Federal dashboard		
		2.3.12 Percentage of custom queries that are accurately transmitted to Agency dashboards		**2.3.12.1** Number of custom queries that are accurately received by Agency dashboards	OT/ED/DT	
				2.3.12.2 [Identical to 2.3.1.2]		
		2.3.13 Percentage of custom queries that are accurately processed by the Agency dashboard		**2.3.13.1** Number of custom queries that are accurately processed by the Agency dashboard	OT/ED/DT	
				2.3.13.2 [Identical to 2.3.1.2]		

FOR OFFICIAL USE ONLY

COI	MOE	MOP		Data Element/Type	Test Event	Notes
		2.3.14 Mean/Max time between transmission of custom queries by the Federal dashboard and processing by Agency dashboards		**2.3.14.1** Times of receipts of custom queries by Agency dashboards	OT/ED/DT	
				2.3.14.2 Times of transmission of custom queries from the Federal dashboard		
3 Reporting FISMA Metrics: Does CDM improve the efficiency of reporting FISMA metrics?	**3.1 Timeliness:** CDM improves the timeliness of FISMA reports and analyses. **ORD 3.4.4** **(KPP 3a)**	**3.1.1** Mean/Max time between request for FISMA report and generation of FISMA report		**3.1.1.1** Times of requests for FISMA report	OT/ED	
				3.1.1.2 Times of completion of FISMA reports		
				3.1.1.3 Baseline data for current timeliness of FISMA report generation		
		3.1.2 Percent of CDM users that believe CDM has improved the timeliness of FISMA reports and analyses		**3.1.2.1** Results from survey questionnaires given to CDM users	OT/ED	
				3.1.2.2 Reviews of relevant studies and documentation		
	3.2 Accuracy:	**3.2.1** Percentage reduction of number of		**3.2.1.1** Number of inaccuracies in manually-generated FISMA reports	OT/ED	

FOR OFFICIAL USE ONLY

COI	MOE	MOP		Data Element/Type	Test Event	Notes
	CDM improves the accuracy of FISMA reports and analyses. **ORD 3.4.4** **(KPP 3a)**	inaccuracies in FISMA reports and analyses		and analyses		
				3.2.1.2 Number of inaccuracies in CDM-generated FISMA reports and analyses		
		3.2.2 Percent of CDM users that believe CDM has improved the accuracy of FISMA reports and analyses		**3.2.2.1** Results from survey questionnaires given to CDM users.	OT/ED	
				3.2.2.2 Reviews of relevant studies and documentation		
	3.3 Completeness: CDM improves the completeness of FISMA reports and analyses. **ORD 3.4.4** **(KPP 3a)**	**3.3.1** Percentage increase in the number of FISMA reportable systems that are included in FISMA reports		**3.3.1.1** Number of FISMA reportable systems included in manually-generated FISMA reports and analyses.	OT/ED	This MOP will be repeated for all relevant FISMA metrics.
				3.3.1.2 Number of FISMA reportable systems included in CDM-generated FISMA reports and analyses that would not have been reported with manual reporting		
		3.3.2 Percentage of CDM users that believe CDM has improved the		**3.3.2.1** Results from survey questionnaires given to CDM users	OT/ED	

FOR OFFICIAL USE ONLY

COI	MOE	MOP		Data Element/Type	Test Event	Notes
		completeness of FISMA reports and analyses		**3.3.2.2** Reviews of relevant studies and analyses		
	3.4 Manpower: CDM reduces the manpower required to produce FISMA reports and analyses. **ORD 3.4.4** **(KPP 3a)**	**3.4.1** Reduction in the manpower required to produce FISMA reports and analyses		**3.4.1.1** Number of man-hours previously required to produce FISMA reports and analyses	OT/ED	
				3.4.1.2 Number of man-hours CDM requires to produce FISMA reports and analyses		
		3.4.2 Percentage of CDM users that believe that CDM has reduced the manpower required to produce FISMA reports and analyses		**3.4.2.1** Results from survey questionnaires given to CDM users	OT/ED	
				3.4.2.2 Reviews of relevant studies and analyses		

NOTE 1: Columns encompass, as appropriate, each of the Tools and Sensors Level, CMaaS Level, Agency Base Dashboard (DB) Level, Agency Intermediate DB Levels, and Federal DB Level.
NOTE 2: All CDM scanning results cover, as appropriate, a 72-hour reporting window and Agency enclave.
NOTE 3: Critical COIs, MOEs, and associated items are highlighted.

B. Operational Suitability

Table A8-2 presents the initial IEF for assessing CDM OS (derived primarily from the current OTA SEP). It follows the formatting used in Table A8-1, except that MOEs are replaced by MOSs. Again, the table entries address, as appropriate, each of the tools and sensors level, CMaaS level, Agency base DB level, Agency intermediate DB levels, and Federal DB level.

No FDSC have been delineated to date for the CDM Program. These will need to be formally developed by the OTA and the CDM T&E WIPT to support quantitative assessments of operational reliability, availability, and maintainability (RAM). These will not consider consequences of and results attributable to malicious attacks.

FOR OFFICIAL USE ONLY

Table A8-2. Initial IEF Structure for CDM OS

COI	MOS	MOP	Data Element/Type	Test Event	Notes
4 System Design: Does the CDM system design support current and envisioned future operations?	**4.1 Human Factors:** CDM system designs (including user and maintainer equipment and processes) support straightforward operations. **ORD 4.3, 6.0**	**4.1.1** User and maintainer opinion on critical or substantial operational problems created by CDM system complexities or limitations	**4.1.1.1** Results from survey questionnaires given to CDM users and maintainers	OT/ED	Problem prioritization per prescribed ordinal ranking. Results reported by user and maintainer categories.
			4.1.1.2 Reviews of relevant studies and documentation	OT/ED/DT	
		4.1.2 User and maintainer opinion on whether there is a significant increase in knowledge, skill, and ability requirements (relative to pre-CDM demands)	**4.1.2.1** Results from survey questionnaires given to CDM users and maintainers	OT/ED	
			4.1.2.2 Reviews of relevant studies and documentation	OT/ED/DT	
		4.1.3 User and maintainer opinion on the adequacy of manpower allotted to CDM operations and sustainment	**4.1.3.1** Results from survey questionnaires given to CDM users and maintainers	OT/ED	At Agency level for operating and maintaining CDM. At Federal level for operating and maintaining Federal-level DB and for assisting Agencies in implementing, operating, and maintaining DBs, sensors, and interfaces.
			4.1.3.2 Summaries of interviews of pertinent Agency- and Federal-level managers	OT/ED/DT	
			4.1.3.3 Reviews of relevant studies and documentation	OT/ED	

FOR OFFICIAL USE ONLY

COI	MOS	MOP	Data Element/Type	Test Event	Notes
		4.1.4 CDM compliance with Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998	**4.1.4.1** Reviews of Section 508 certifications, inspection results, and compliance plans/documentation	OT/ED/DT	
		4.1.5 CDM compliance with Operational Safety and Health Administration (OSHA) rules and regulations	**4.1.5.1** Reviews of OSHA certifications, inspection results, and compliance plans/documentation	OT/ED/DT	
		4.1.6 CDM compliance with applicable statues, regulations, and policies related to environmental considerations	**4.1.6.1** Reviews of certifications, inspection results, and compliance documentation concerned with environmental considerations	OT/ED/DT	
	4.2 Compatibility: CDM does not degrade Agency operations and can adapt to future technologies. **ORD 4.1, 6.0**	**4.2.1** Agency operator and maintainer opinion on whether or not CDM induces workflow degradations and if they pose critical or substantial operational problems	**4.2.1.1** Results from survey questionnaires given to Agency operators and maintainers	OT/ED	Problem prioritization per prescribed ordinal ranking. Results reported by operator and maintainer categories.
		4.2.2 Average percent degradation of Agency workflows attributable to the incorporation of the CDM system	**4.2.2.1** Results from survey questionnaires given to Agency operators and maintainers	OT/ED	
			4.2.2.2 Reviews of pertinent CDM documentation, studies, and supporting tests	OT/ED/DT	
		4.2.3 Existence of explicit CDM capabilities and architecture	**4.2.3.1** Interviews with Solution Provider leads and government ISOs	OT/ED	

FOR OFFICIAL USE ONLY

COI	MOS	MOP	Data Element/Type	Test Event	Notes
		implementations for accommodating emerging technologies	**4.2.3.2** Reviews of pertinent CDM documentation, studies, and supporting tests	OT/ED/DT	
	4.3 Scalability: CDM network loading and growth potential can incorporate architecture expansions. **ORD 4.1, 6.0**	**4.3.1** Adequacy of CDM capabilities and architecture implementations for accommodating architecture expansions	**4.3.1.1** Interviews with Solution Provider leads and Agency managers	OT/ED	
			4.3.1.2 Reviews of pertinent documentation, studies, and supporting test results	OT/ED/DT	
5 Documentation & Training: Do CDM technical manuals, Standard Operating Procedures (SOPs), policies, and training programs support users and maintainers?	**5.1 Technical Manuals:** CDM technical manuals and reference documentation support CDM users and maintainers. **ORD 4.1, 6.0**	**5.1.1** Adequacy and currency of CDM technical manuals and reference documentation supporting CDM user and maintainer activities	**5.1.1.1** Results from survey questionnaires given to CDM users and maintainers	OT/ED	For each category of CDM user and maintainer activities
			5.1.1.2 Review of pertinent CDM user and maintainer documentation	OT/ED/DT	
	5.2 SOPs and Policies: CDM operating instructions and guidance for interpreting and responding to emerging results support CDM users and maintainers.	**5.2.1** Adequacy and currency of CDM SOPs and policies for supporting users and maintainers in operating CDM and in interpreting and responding to emerging results provided by CDM.	**5.2.1.1** Results from survey questionnaires given to CDM users and maintainers	OT/ED	For each category of CDM analyst and manager activities. These SOPs should include updating and maintaining hardware and software.
			5.2.1.2 Review of pertinent CDM user and maintainer documentation	OT/ED/DT	

FOR OFFICIAL USE ONLY

COI	MOS	MOP	Data Element/Type	Test Event	Notes
	ORD 4.1, 6.0	**5.2.2** Ability to modify CDM SOPs and policies to respond to lessons learned and inter-Agency governance board direction	**5.2.2.1** Results from survey questionnaires given to CDM users and maintainers	OT/ED	
			5.2.2.2 Review of pertinent CDM user and maintainer documentation	OT/ED/DT	
	5.3 Training Programs: CDM training programs support the development and sustainment of CDM user and maintainer skill sets. **ORD 4.6, 6.0**	**5.3.1** Adequacy and currency of CDM training manuals and instructional programs supporting CDM user and maintainer activities	**5.3.1.1** Results from survey questionnaires given to CDM users and maintainers	OT/ED	For each category of CDM user and maintainer activities
			5.3.1.2 Review of pertinent CDM user and maintainer documentation	OT/ED/DT	
6 Sustainability:	**6.1 Reliability:** CDM performs its mission reliably, without excessive hardware/software (HW/SW) failures or degradation of capabilities. **ORD 4.2, 4.4, 6.0**	**6.1.1** Mean Time Between Failures (MTBF) **CDM Elements:** Threshold = 100 hours Objective = 200 hours	**6.1.1.1** Timelines of CDM object capability states (fully capable, partially capable with non-substantive degradation, partially capable with substantive degradation, no capability)	OT/ED/ Maintenance-Demonstration (M-Demo)/ Disaster Recovery Demonstration (DR-Demo)	May only be able to get general system failure data especially in early OA.
			6.1.1.2 Timelines of CDM object demand states (called upon to function, not called upon to function)		
			6.1.1.3 Timelines of CDM object operating profile state (core business hours, continuous operating hours, disaster recovery periods)		

FOR OFFICIAL USE ONLY

COI	MOS	MOP	Data Element/Type	Test Event	Notes
Do CDM reliability, availability, and maintainability support system operation?		**6.1.2** Mean Time Between Operational Mission Failures (MTBOMF) = Total CDM object/system "operating time" divided by total number of "operational mission failures (OMFs)" **KPP 2d.1:** Threshold = 10,000 hours Objective = 20,000 hours	**6.1.2.1** Timelines of CDM object capability states (fully capable, partially capable with non-substantive degradation, partially capable with substantive degradation, no capability) **6.1.2.2** Timelines of CDM object demand states (called upon to function, not called upon to function) **6.1.2.3** Timelines of CDM object operating profile state (core business hours, continuous operating hours, disaster recovery periods)	OT/ED/ M-Demo/ DR-Demo	MTBOMFs reported by sets of "operating", operating profiles, OMF, and CDM object types. "Operating" = (on and fully capable, on and at least partially capable with non-substantive degradation, available (on or off) and fully capable, available (on or off) and at least partially capable with non-substantive degradation). OMF = (any reduction to less than fully capable, any reduction to less than partially capable with non-substantive degradation capability).

FOR OFFICIAL USE ONLY

COI	MOS	MOP	Data Element/Type	Test Event	Notes
	6.2 Availability: CDM is available, i.e., accessible and usable on demand, to support operating profiles. **ORD 4.2, 4.4, 6.0**	**6.2.1** Operational Availability (A_0) = Total CDM object/system available time divided by total number of planned CDM object/system hours **KPP 2d.2:** Threshold = 99.5% Objective = 99.9%	**6.2.1.1** [Identical to 6.1.1.1] **6.2.1.2** [Identical to 6.1.1.2] **6.2.1.3** [Identical to 6.1.1.3]	OT/ED/M-Demo/DR-Demo	Data elements collected for individual CDM objects. A_0's reported for object/system types and by combinations of definitions of "available", operating profiles, and CDM object types. "Available" = (fully capable, fully capable or partially capable with non-substantive degradation). Operating profile = (core business hours, continuous operating hours, disaster recovery periods).
		6.2.2 CDM user and maintainer opinion of CDM availability shortcomings as posing critical or substantial operational problems	**6.2.2.1** Results from survey questionnaires given to CDM users	OT/ED/ M-Demo/ DR-Demo	Problem prioritization per prescribed ordinal ranking. Results reported by CDM object/system/ user types.
	6.3 Maintainability: CDM HW/SW maintenance, repair, and replacement	**6.3.1** Fraction of CDM object/system type non-availability time attributable to CDM	**6.3.1.1** [Identical to 6.1.1.1] **6.3.1.2** [Identical to 6.1.1.2] **6.3.1.3** [Identical to 6.1.1.3]	OT/ED/M-Demo/DR-Demo	Data elements collected for individual CDM objects. Results

FOR OFFICIAL USE ONLY

COI	MOS	MOP	Data Element/Type	Test Event	Notes
	processes support operational availability. **ORD 4.2, 4.4, 4.5, 6.0**	HW/SW maintenance, repair, and replacement processes (Fraction of Time System Under Repair)	**6.3.1.4** Timelines of CDM object maintenance states (inactive and no Help Desk ticket generated, inactive and Help Desk ticket generated but not completed, active and Help Desk ticket generated but not completed, inactive and Help Desk ticket generated and completed) during core business hours		reported by CDM object/system type and by combinations of definitions of "non-availability" and operating profile.
		6.3.2 Maximum CDM object/system type non-availability time attributable to CDM HW/SW maintenance, repair, and replacement processes (Max Time to Repair) **CDM Program:** Maintenance must be conducted no later than next business day	**6.3.2.1** [Identical to 6.1.1.1]	OT/ED/M-Demo/DR-Demo	
			6.3.2.2 [Identical to 6.1.1.2]		
			6.3.2.3 [Identical to 6.1.1.3]		
			6.3.2.4 [Identical to 6.3.1.4]		
		6.3.3 Fraction of CDM object/system non-availability time attributable to CDM Help Desk delays before maintenance, repair, and replacement activities are initiated and after maintenance, repair, and replacement activities are completed	**6.3.3.1** [Identical to 6.1.1.1]	OT/ED/ M-Demo/ DR-Demo	
			6.3.3.2 [Identical to 6.1.1.2]		
			6.3.3.3 [Identical to 6.1.1.3]		
			6.3.3.4 [Identical to 6.3.1.4]		

FOR OFFICIAL USE ONLY

COI	MOS	MOP	Data Element/Type	Test Event	Notes
		6.3.4 Mean Time to Repair	**6.3.4.1** [Identical to 6.3.1.4]	OT/ED/ M-Demo/ DR-Demo	
		6.3.5 Mean Time between Repairs	**6.3.5.1** [Identical to 6.3.1.4]		
		6.3.6 Mean Time to Repair all Failures	**6.3.6.1** [Identical to 6.3.1.4]		
		6.3.7 Success rate for update and patch deployment	**6.3.7.1** Number of patches/updates required	OT/ED/ M-Demo/ DR-Demo	
			6.3.7.2 Number of patches/updates attempted		
			6.3.7.3 Number of patches/updates successfully deployed		
			6.3.7.4 Results from survey questionnaires given to CDM users and maintainers		
		6.3.8 Mean Time to Service Help Desk Tickets	**6.3.8.1** Time tickets opened	OT/ED	
			6.3.8.2 Time tickets closed		
			6.3.8.3 Results from survey questionnaires given to CDM users and maintainers		
	6.4 Mission Success Probability: CDM processes support mission accomplishment	**6.4.1** Probability that all CDM objects successfully perform their required Mission Essential Functions within a 3-day mission cycle	**6.4.1.1** System Data	OT/ED	
			6.4.1.2 Results from survey questionnaires given to CDM users and maintainers		

NOTE 1: Columns encompass, as appropriate, the Tools and Sensors Level, CMaaS Level, Agency Base DB Level, Agency Intermediate DB Levels, and Federal DB Level.
NOTE 2: Related ORD Sections appear in the "MOS" column. Critical COIs, MOSs, and associated items are highlighted.
NOTE 3: Related ORD-prescribed quantitative Operational Suitability requirements and KPPs appear in the "MOP" column.

C. Cybersecurity

Table A8-3 presents the initial IEF for assessing CDM Cybersecurity (derived primarily from the current OTA SEP with some modest updates). It follows the formatting used in Table A8-1, except that MOEs are replaced by MOCs. Again, the table entries address, as appropriate, each of the tools and sensors level, CMaaS level, Agency base DB level, Agency intermediate DB levels, and Federal DB level.

The development of detailed cybersecurity test plans will be guided by further decomposition of the MOPs in Table A8-3 into relevant exploit types, to include unauthorized data access (read, write, delete), arbitrary code execution, denial of service, and others consistent with the validated CDM threats. The evaluation of defender activities should consider a complete set of possible threat actions and effects consistent with validated threats. One way to achieve this is to assess the performance of protect, detect, respond, and recover activities against a logically decomposed threat kill chain (e.g., performance of "detect" against a specific element of threat kill chain).

A possible decomposition of the threat kill chain is described in a 2011 paper presented at the International Conference on Information Warfare and Security:[77]

1. Reconnaissance - Research, identification and selection of targets, using, for example, crawling internet sites for conference proceedings, email addresses, social relationships, or information on specific technologies.

2. Weaponization - Coupling a remote access trojan with an exploit into a deliverable payload, typically by means of an automated tool (weaponizer). For instance, client application data files such as Adobe Portable Document Format or Microsoft Office documents can serve as the weaponized deliverable.

3. Delivery - Transmission of the weapon to the targeted environment using, for example, email attachments, websites, and removable media.

4. Exploitation - After the weapon is delivered to victim host, exploitation triggers intruders' code. Most often, exploitation targets an application or operating system vulnerability, but it could also more simply exploit the users themselves or leverage an operating system feature that auto-executes code.

5. Installation - Installation of a remote access trojan or backdoor on the victim system allows the adversary to maintain persistence inside the environment.

6. Command and Control (C2) - Typically, compromised hosts must beacon outbound to an Internet controller server to establish a C2 channel. Advanced Persistent Threat malware

[77] "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," E.M. Hutchins, M,J. Cloppert, R.M. Amin, Presented at the 6th Annual International Conference on Information Warfare and Security, Washington, DC, 2011.

especially requires manual interaction rather than conduct activity automatically. Once the C2 channel establishes, intruders have "hands on the keyboard" access inside the target environment.

7. Actions on Objectives - Only now, after progressing through the first six phases, can intruders take actions to achieve their original objectives. Typically, this objective is data exfiltration that involves collecting, encrypting, and extracting information from the victim environment; violations of data integrity or availability are potential objectives as well. Alternatively, the intruders may only desire access to the initial victim box for use as a hop point to compromise additional systems and move laterally inside the network.

Table A8-3. Initial IEF Structure for CDM Cybersecurity

COI	MOC	MOP	Data Element/Type	Test Event	Notes
7 Resiliency: Are CDM systems and networks resilient to cyber threats?	**7.1 Protect:** CDM and host network defenders protect CDM's subsystems and data against adversarial activities, including pivoting attacks. **ORD 6.0**	**7.1.1** Performance of CDM and host network protection against adversarial activities **KPP 4.2:** Threshold: No Category I severity of incidents in maintaining the confidentiality, integrity, and availability of CDM hardware, software, and data to acceptable levels. Objective: No Category I or II severity of incidents in maintaining the confidentiality, integrity, and availability of CDM hardware, software, and data to acceptable levels. Category I (II) is defined as any vulnerability, the exploitation of which will, directly and immediately result in (has the potential to result in) loss of	**7.1.1.1** Description of adversarial activities including techniques, targets, and attack objectives. **7.1.1.2** Level of difficulty of attacks. **7.1.1.3** Time for Red Teams to execute attacks. **7.1.1.4** Count of successes and failures of attacks **7.1.1.5** Scored severity of incidents in maintaining the confidentiality, integrity, and availability of CDM hardware, software, and data to acceptable levels.	OT	Certified Red Teams independent from the developer shall conduct adversarial activities to simulate validated CDM threats as articulated in the CDM TEMP. Range of adversarial activities could include all steps in the threat's kill chain: Reconnaissance, weaponization, delivery, exploitation, installation, command and control, and execution of objective. Attack objectives should include exfiltration of CDM sensitive data, denial of CDM services, and corruption of CDM data and processes. Scope of adversarial attacks should include pivoting (island

COI	MOC	MOP	Data Element/Type	Test Event	Notes
		Confidentiality, Availability, or Integrity.			hoping) attacks that either targets or exploits CDM subsystems and data. The data elements for MOP 7.1.2 could support test planning. MOP determinations will be parsed by kill chain steps.
		7.1.2 Preparedness to protect CDM from attack **KPP 4.2:** Threshold: No Category I severity of incidents in maintaining the confidentiality, integrity, and availability of CDM hardware, software, and data to acceptable levels. Objective: No Category I or II severity of incidents in maintaining the confidentiality, integrity, and availability of CDM hardware, software, and data to acceptable levels.	**7.1.2.1** Review the completeness and accuracy of protection-related measures in ST&E results and other relevant artifacts generated by the DHS and agency Security Authorization Process.	OT/ED/DT	These processes and artifacts are described in: DHS 4300A Sensitive Systems Handbook, Version 11.0, January 14, 2015. DHS Security Authorization Process Guide, CISO, Version 11.1, March 16, 2015.
			7.1.2.2 Survey results from SMEs and users		
			7.1.2.3 Results of comprehensive, overt, and cooperative vulnerability assessment of CDM in its intended operational environment		The cooperative vulnerability assessment should characterize penetrations including techniques and results of attempted intrusions, privilege escalation, exploitation, and password cracks.

COI	MOC	MOP	Data Element/Type	Test Event	Notes
			7.1.2.4 Survey of open source and publicly available information that could aid in exploitation		This data element directly addresses susceptibility to exploits and indirectly addresses the preparedness to protect.
	7.2 Detect: CDM and host network defenders detect adversarial activities against CDM's subsystems and data. **ORD 6.0**	**7.2.1** Percentage of delivered exploits against CDM that were detected	**7.2.1.1** Number of delivered exploits that were detected	OT	
			7.2.1.2 Number of delivered exploits		
		7.2.2 Ability of Detect function to support operations	**7.2.2.1** Time for defenders to detect adversarial activities including intrusion, escalation of privilege, and exploitation.	OT	Time will be parsed by kill chain steps.
			7.2.2.2 For undetected exploits, assessment of accrued, likely, and possible damage		
			7.2.2.3 Survey and observed adequacy of detection times in support of operations		
			7.2.2.4 Review of logs for detected log-in failures, unauthorized data-access attempts, etc.	OT/ED	
			7.2.2.5 Review of relevant MOPs for health and status monitoring		
			7.2.2.6 Review of log audit processes		

COI	MOC	MOP	Data Element/Type	Test Event	Notes
			in place		
		7.2.3 Preparedness to detect CDM exploits as they occur	**7.2.3.1** Review the completeness and accuracy of detection-related measures in ST&E results and other relevant artifacts generated by the DHS and agency Security Authorization Process.	OT/ED/DT	These processes and artifacts are described in: DHS 4300A Sensitive Systems Handbook, Version 11.0, January 14, 2015. DHS Security Authorization Process Guide, CISO, Version 11.1, March 16, 2015. Firewall, Intrusion Detection System, and Intrusion Prevention System rulesets.
			7.2.3.2 Survey results from SMEs and users		
	7.3 Response: CDM and host network defenders mitigate detected adversarial activities against CDM's subsystems and data. **ORD 6.0**	**7.3.1** Percentage of successful responses to detected exploits	**7.3.1.1** Number of successful responses	OT	Definitions for "successful" will need to be developed.
			7.3.1.2 [Identical to 7.2.1.1]		
		7.3.2 Ability of Response function to support operations	**7.3.2.1** For unsuccessful response to detected exploits, assessment of accrued, likely, and possible damage	OT	
			7.3.2.2 Time from successful exploit to response		
			7.3.2.3 Time from successful detection to		

COI	MOC	MOP	Data Element/Type	Test Event	Notes
			response		
			7.3.2.4 Survey and observed adequacy of response times in support of operations		
		7.3.3 Preparedness to react to CDM exploits as they occur	**7.3.2.1** Review the completeness and accuracy of react-related measures in ST&E results and other relevant artifacts generated by the DHS and agency Security Authorization Process.	OT/ED/DT	These processes and artifacts are described in: DHS 4300A Sensitive Systems Handbook, Version 11.0, January 14, 2015. DHS Security Authorization Process Guide, CISO, Version 11.1, March 16, 2015.
			7.3.2.2 Survey results from SMEs and users		
	7.4 Recover/Continuity of Operations: CDM and host network defenders recovery CDM mission effectiveness following successful adversarial attacks against CDM's subsystems and data. **ORD 6.0**	**7.4.1** Percentage of attempted recoveries that were successful	**7.4.1.1** Number of successful recoveries	OT	Definitions for "successful" will need to be developed.
			7.4.1.2 Number of attempted recoveries		
		7.4.2 Ability of Recover function to support operations	**7.4.2.1** Number of backups of official component configuration information	OT	
			7.4.2.2 Total time for recovery		
			7.4.2.3 Number of critical data backups		
			7.4.2.4 Availability and adequacy of off-line backup and storage facilities		
			7.4.2.5 Time from		

COI	MOC	MOP	Data Element/Type	Test Event	Notes
			successful exploit to recovery		
			7.4.2.6 Time from successful detection to recovery		
			7.4.2.7 Survey and observed adequacy of recovery times in support of operations		
		7.4.3 Success rate for COOP plan execution	**7.4.3.1** Number of unsuccessful COOP plan executions	OT	It remains to be determined what type(s) of COOP will be executed – hot site, warm site, or cold site. CDM operational effectiveness determinations should drive the type of COOP.
			7.4.3.2 Number of attempted COOP plan executions		
		7.4.4 Adequacy of COOP execution in support of operations	**7.4.4.1** Time to execute COOP plan	OT	
			7.4.4.2 Survey and observed adequacy of COOP execution times in support of operations		
		7.4.5 Adequacy of COOP planning	**7.4.5.1** Review of COOP plans	OT/ED/DT	
			7.4.5.2 Review of regular COOP exercises		
			7.4.5.3 Review of architecture for design resiliency		

COI	MOC	MOP	Data Element/Type	Test Event	Notes
	7.5 Mission: CDM effectively conducts its assigned mission in the presence of adversarial activities against CDM's subsystems and data.	**Identical to Operational Effectiveness MOPs** **1.1.H.1-3.4.2**	**Identical to Operational Effectiveness Data Element/Type** **1.1.H.1.1-3.4.2.2**	OT/ED	The Mission MOE addresses the effectiveness of CDM in the presence cyber threat activities. The MOP and Data Element/Type are identical to those under the Situational Awareness, Federal Dashboard & Interoperability, and Reporting FISMA Metrics COIs that comprise operational effectiveness. These data should be collected during cyber threat activities and compared to a baseline absent of cyber threat activities. The baseline data may be collected during ED.

NOTE 1: Columns encompass, as appropriate, each of the Tools and Sensors Level, CMaaS Level, Agency Base DB Level, Agency Intermediate DB Levels, and Federal DB Level.
NOTE 2: There are no related ORD sections corresponding to Cybersecurity Resiliency. Critical COIs, MOCs, and associated items are highlighted.

ANNEX 9: Functional Requirements Documents

The following documents make up the CDM functional requirements:

- Functional / Technical Requirements
  - Dashboard TO Attachment I
  - Phase 1 CMaaS TO Attachment N
  - Phase 2 CMaaS TO Attachment N2
  - Solution Provider Derived Requirements as delivered in their Requirements Traceability Matrix (RTM)
    - Note: If approved by the PMO, the functional requirements listed in the Solution Provider RTM becomes the official CDM FRD for that respective Task Order (e.g. The MTV V12 requirements document was the “official” FRD for the Agency Dashboard Release 1 as opposed to Attachment I upon approval from the CDM PMO)
  - CDM Test Team Derived Requirements

ANNEX 10: CDM RAM Rationale Document

The attached document is the Reliability, Availability, Maintainability Rationale – Performance Plan 1.0 for CDM.

RAM Rationale_CDM Performance Plan_V1

Reliability Availability Maintainability Rationale Performance Plan 1.0
for
Continuous Diagnostics and Mitigation Program
(CDM)

By
Garfield Jones CTEP (DHS)
Dr. Arthur Fries (IDA)

January 2017
Office of Cybersecurity & Communications
Network Security Deployment

ANNEX 11: Acronyms

ACRONYM	DESCRIPTION
ABMC	American Battle Monuments Commission
ADE	Acquisition Decision Event
AO	Authorizing Official
APB	Acquisition Program Baseline
ARB	Acquisition Review Board
AT	Acceptance Testing
ATO	Authority to Operate
BAH	Booz Allen Hamilton
BBG	Broadcasting Board of Governors
BPA	Blanket Purchase Agreement
CA	Cybersecurity Assurance
CAE	Component Acquisition Executive
CDM	Continuous Diagnostics & Mitigation
CFPB	Consumer Financial Protection Bureau
CFTC	Commodity Futures Trading Commission
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
CISO	Chief Information System Officer
CM	Continuous Monitoring
CMaaS	Continuous Monitoring-as-a-Service
CNCS	Corporation for National and Community Service
COI	Critical Operational Issue
CONOPS	Concept of Operations
CO	Contracting Officer
COOP	Continuity of Operations
COR	Contracting Officer's Representative
COTS	Commercial off-the-shelf
CPSC	Consumer Product Safety Commission
CSM	Configuration Settings Management
CSOSA	Court Services and Offender Supervision Agency
CTPs	Critical Technical Parameters
DAG	Data Authentication Group
DHS	Department of Homeland Security
DNFSB	Defense Nuclear Facilities Safety Board
DOC	Department of Commerce

ACRONYM	DESCRIPTION
DOE	Department of Energy
DOI	Department if Interior
DOJ	Department of Justice
DOL	Department of Labor
DOS	Department of State
DOSOIG	U.S. Department of State Office of Inspector General
DOT&E	Director, Office of Test & Evaluation
DR	Defect/Deficiency Report
DRD	Deficiency Report Document
DSM	Decision Support Matrix
DSQ	Decision Support Questions
DT	Developmental Test (or Testing)
DT&E	Developmental Test and Evaluation
DTP	Detailed Test Plans
DTRR	Developmental Test Readiness Review
ED	Department of Education
ED	Early Deployment
EDPs	Event Design Plans
EEOC	Equal Employment Opportunity Commission
EOAP	Early Operational Assessment Plan
EOAR	Early Operational Assessment Report
EOP	Executive Office of the President
EPA	Environmental Protection Agency
FCA	Farm Credit Administration
FDFC	Failure Definition and Scoring Criteria
FEC	Federal Election Commission
FERC	Federal Energy Regulatory Commission
FEDSIM	Federal Systems Integration Management Center
FHFA	Federal Housing Finance Agency
FISMA	Federal Information Security Management Act
FMC	Federal Maritime Commission
FNR	Federal Network Resilience
FNS	Federal Network Security
FOC	Final Operational Capability
FOT&E	Follow-on Operational Test and Evaluation
FRD	Functional Requirements Document
FTC	Federal Trade Commission

ACRONYM	DESCRIPTION
GSA	General Service Administration
HHS	Health and Human Services
HPE	Hewlitt Packard Enterprise Services
HUD	Housing and Urban Development
HWAM	Hardware Asset Management
IA	Information Assurance
IBWC	International Boundary and Water Commission
ICD	Interface Control Document
IDA	Institute for Defense Analysis
IEEE	Institute for Electrical and Electronics Engineers
IEF	Integrated Evaluation Framework
IMS	Integrated Master Schedule
IOC	Initial Operational Capability
IOT&E	Initial Operational Test and Evaluation
IPT	Integrated Product Team
IT	Information Technology
IT&E	Integrated Test and Evaluation
IT&E-PP	Integrated Test and Evaluation Preparation Process
IV&V	Independent Verification & Valuation
JHU/APL	Johns Hopkins University Applied Physics Lab
KCG	Knowledge Consulting Group Mantech
KPP	Key Performance Parameters
LOA	Letter of Assessment
LOOs	Letters Of Observations
LPR	Limited Production Review
LSE	Lead System Engineer
M&S	modeling and simulation
MCC	Millennium Challenge Corporation
MNS	Mission Needs Statement
MOA	Memorandum of Agreement
MOC	Measure of Cybersecurity
MOE	Measures of Effectiveness
MOP	Measure of Performance
MOS	Measure of Suitability
MSPB	U.S. Merit Systems Protection Board
MTBF	Mean Time Between Failure
MTBOMF	Mean Time Between Operational Mission Failure

ACRONYM	DESCRIPTION
MTTR	Mean Time to Repair
MTV	Metrica Team Venture
NARA	National Archives and Records Administration
NASA	National Aeronautics and Space Administration
NCCIC	National Cybersecurity and Communication Integration Center
NCPC	National Capital Planning Commission
NEA	National Endowment for the Arts
NEH	National Endowment for the Humanities
NGC	Northrup Grumman Corporation
NIST	National Institute for Standards and Technology
NLRB	National Labor Relations Board
NPPD	National Protection and Programs Directorate
NRC	Nuclear Regulatory Commission
NSD	National Security Deployment
NSF	National Science Foundation
NTSB	National Transportation Safety Board
O&M	Operations and Maintenance
OA	Operational Assessment
OAP	Operational Assessment Plan
OAR	Operational Assessment Report
OE	Operational Effectiveness
OGE	Office of Government Ethics
OMB	Office of Management and Budget
OPIC	Overseas Private Investment Corporation
OPM	Office of Personnel Management
ORD	Operational Requirements Document
ORR	Operational Readiness Review
OS	Operational Suitability
OSHRC	Occupational Safety & Health Review Commission
OSC	U.S. Office of Special Council
OT	Operational Test
OT&E	Operational Test and Evaluation
OTA	Operational Test Agent/Authority
OTP	Operational Test Plans
OTR	Operational Test Report
OTRRs	Operational Test Readiness Reviews
PBGC	Pension Benefit Guaranty Corporation

ACRONYM	DESCRIPTION
PCLOB	Privacy and Civil Liberties Oversight Board
PIR	Post Implementation Review
PM	Program Manager
PMO	Program Management Office
PRC	Postal Regulatory Commission
PRR	Production Readiness Review
RAM	Reliability, Availability, and Maintainability
RFQ	Request for Quote
RMF	Risk Management Framework
RRB	U.S. Railroad Retirement Board
RTM	Requirements Traceability Matrix
SBA	Small Business Administration
SDR	System Design Review
SEC	U.S. Securities and Exchange Commission
SELC	Systems Engineering Life Cycle
SEMP	Systems Engineering Management Plan
SEP	System Evaluation Plan
SOW	Statement of Work
SRR	System Readiness Review
SSA	Social Security Administration
SSS	Selective Service System
ST&E	Security Test and Evaluation
SUT	System Under Test
SWAM	Software Asset Management
T&E	Test and Evaluation
TAM	Test Area Manager
TEMP	Test and Evaluation Master Plan
TO	Task Order
TPOC	Technical Point of Contact
TRR	Test Readiness Review
TVA	Tennessee Valley Authority
UAT	User Acceptance Testing
USADF	U.S. Africa Development Foundation
USAID	United States Agency for International Development
USDA	United Stated Department of Agriculture
USDOT	United States Department of Transportation
USITC	U.S. International Trade Commission

ACRONYM	DESCRIPTION
USPS	`United States Postal Service
USPSOIG	United States Postal Service Office of the Inspector General
VA	Veterans Affairs
VUL	Vulnerability Management
V&V	Verification and Validation
VV&A	Verification, Validation, and Accreditation
WIPT	Working Integrated Product Team

ANNEX 12: References

CDM Agency Dashboard Performance Benchmark Analysis, Version 1.0, Metrica Team Venture, February 2017.

CDM Architecture Principles Document Version 0.5 DRAFT August 31, 2016.

CDM Data Model Document Version 1.0 DRAFT September 13, 2016.

CDM ORD version 2.0 signed 2015-04-24 (Section 1.3 Table 1 p. 12).

CMaaS TO, Section 2.5.1.4, 2.5.3, 2.5.9, and 2.5.11.1; Component testing the Agency Dashboard and the Federal Dashboard are the responsibility of the dashboard integrator.

Committee on National Security Systems (CNSS) Instruction No. 4009, National Information Assurance (IA) Glossary, 26 April 2010.

Cyber Security Metrics and Measures, NIST Manuscript Publication, 2 March 2009.

Department of Defense Handbook: Reliability Growth Management, MIL-HDBK-189C, U.S. Department of Defense, Washington DC, 2011.

DHS 4300A Sensitive Systems Handbook, Version 11.0, January 14, 2015.

DHS Acquisition Instruction Guidebook #102-01-001: Interim Appendix L Test and Evaluation Master Plan (TEMP) v2.0, May 07, 2015.

DHS DOT&E only has authority within DHS. Legal concern that would have to be resolved through DHS OGC includes legislation contained in Title 31 U.S.C. and Title 44 U.S.C.

DHS Guidebook, 102-01-103-01, Systems Engineering Life Cycle Guidebook, DHS, April 2016.

DHS Information Technology (IT) Major Acquisition Guidelines for Operational Test Agent

DHS Instruction Guide 026-06-001-01, Test and Evaluation Master Plan (TEMP), Department of Homeland Security, Science and Technology Directorate, February 2017.

DHS Management Directive, Test and Evaluation, 22 May 2009.

DHS Security Authorization Process Guide, Office of the Chief Information Security Officer (CISO), Version 11.1, March 16, 2015.

Reliability Availability Maintainability Rationale – Performance Plan, DHS Office of Cybersecurity & Communications, NSD, January 2016

DoD Guide for Achieving Reliability, Availability, and Maintainability, U.S. Department of Defense, Washington DC, 2005.

E-Government Act of 2002.

FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems, NIST, 2004.

FIPS PUB 200, Minimum Security Requirements for Federal Information and Information Systems, 2006.

Fiscal Years 2014-2018 Strategic Plan, Department of Homeland Security, 2014.

Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements, Office of Management and Budget Memorandum M-16-03.

IEEE Std. 12207.2, p. 94.

Integrated Logistics Support Plan (ILSP) for Continuous Diagnostics and Mitigation (CDM), Version 1.2, 30 September 2014.

"Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," E.M. Hutchins, M,J. Cloppert, R.M. Amin, Presented at the 6th Annual International Conference on Information Warfare and Security, Washington, DC, 2011.

Memorandum of Agreement on Operational Suitability Terminology and Definitions to be used in Operational Test and Evaluation, Service Operational Test Agencies, October 2005.

NIST Special Publications that specify key requirements and artifacts include (not exhaustively): NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems, 2010; NIST Special Publication 800-37, Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems, 2010; NIST Special Publication 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, 2014; NIST Special Publication 800-53A, Revision 4, Assessing Security and Privacy Controls in Federal Information Systems and Organizations, 2014.

NIST Special Publication 800-18, Revision 1, Guide for Developing Security Plans for Federal Information Systems, 2006.

NIST SP 800-37, Revision 1.

Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems, 1985 – as analyzed in Appendix IV: Analysis of Key Sections, with supplemental information in Appendix III, Security of Federal Automated Information Resources.

Office of Management and Budget Memorandum 10-28, Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security, July 6, 2010.

Operational Test Agent's System Evaluation Plan for the Continuous Diagnostics and Mitigation (CDM) Program, IDA, February 2015 this document was not authorized to be provided by OTA and has not been reviewed or approved by the PMO.

Operational Test Agent's System Evaluation Plan for the Continuous Diagnostics and Mitigation (CDM) Program, Institute for Defense Analyses, Document D-5199, February 2015.

ORD 3.0 for Continuous Diagnostics and Mitigation (CDM) October 31, 2016.

Procedures for Operational Test and Evaluation of Cybersecurity, DHS DOT&E Memorandum, 15 October 2015.

Procedures for Operational Test and Evaluation of Cybersecurity, Memorandum, Director, Operational Test and Evaluation (now Director, Office of Test and Evaluation), 15 October 2015.

Procedures for Operational Test and Evaluation of Information Assurance in Acquisition Programs, Director of Operational Test and Evaluation (DOT&E), 21 January 2009.

Reliability Growth: Enhancing Defense System Reliability, National Research Council, Panel on Reliability Growth Methods for Defense Systems, Committee on National Statistics, Division of Behavioral and Social Sciences and Education, The National Academies Press, Washington DC, 2015.

Technical Review Guide, Version 2.0, DHS, Systems Engineering Center of Excellence, December 2015.

TO2A White Paper: Lifecycle (SELC) User Acceptance Test (UAT) and Operational Readiness Review (ORR) for DHS Components, DHS PMO, January 2017.

U.S. Department of Homeland Security Annual Performance Report Fiscal Years 2013 – 2015, Appendix B: Program Evaluations, Department of Homeland Security, June 2014.

RFS #	RIP #	Receiving Agency	Receving Agency Component / Division	Product Manufacturer	Manufacturer Part Number	Product Description	Unit of Issue
RFS-DHS-000X	*1*	*123-Agency*	*123-Agency*	*ABC*	*12345XYZLIC*	*Software License*	*each*
RFS-DHS-000X	*2*	*123-Agency*	*123-Agency*	*ABC*	*12345XYZ-MNT*	*Software License Maintenance, First Year*	*each*

IT70 CDM SIN Price	Proposed Unit Price	Actual Unit Price	Quantity	Extended Price	CLIN	Cost Savings (Discount)	Product Date or Order	Product Date of Receipt by Government	Date of Expiration / Renewal (if applicable)	Renewal Manufacturer Part Number
$10,000	*$7,654*	*$7,654*	*6*	*$ 45,924.00*		*$ 14,076.00*	*1/15/2018*	*2/6/2018*	*NA*	*NA*
$32	*$21*	*$21*	*6*	*$ 126.00*		*$ 66.00*	*1/15/2018*	*2/6/2018*	*2/1/2019*	*12345XYZ-RWL*

Renewal Product Description
NA
Software License Annual Maintenance

REQUEST TO INITIATE PURCHASE (RIP) FOR EQUIPMENT, MATERIALS, OTHER DIRECT COSTS (ODCs), AND/OR SERVICES

Contractor:		**RIP Number:**	
Client:	DHS	**Date:**	
Agency/Division Supported:		**Project Name:**	DHS CDM DEFEND Group D
RFS Number:		**Task Order Number:**	

			Last Invoice submitted:	
TO:	*(Insert First and Last Name)* , FEDSIM Contracting Officer's Representative (COR)	**CLIN X00X VALUE:**	**$**	**-**
		CUMULATIVE AMOUNT BILLED:	**$**	**-**
FROM:	*(Insert First and Last Name of requestor)*	**CURRENT CLIN X00X BALANCE:**	**$**	**-**
THROUGH:	*(Insert client organization and First and Last Name)* , Technical Point of Contact (TPOC)	**RIP ESTIMATE:**	**$**	**-**
		NEW CLIN X00X BALANCE:	**$**	**-**
SUBJECT:	Request to Initiate Purchase # *(insert number)*			
DATE:	*(Insert Month Date, Year)*			

PURPOSE/JUSTIFICATION OF REQUEST:

All equipment, materials, and ODCs shall be purchased in accordance with client requirements. All equipment, materials, and ODCs shall become the property of the Government and shall be regarded as Government Furnished Property (GFP), and unless previously approved by the Contracting Officer, shall be used only in performance of this Task Order. All materials shall be purchased in accordance with applicable Federal Acquisition Regulation (FAR) clauses and approved purchasing procedures. All equipment, materials, and ODCs shall be purchased in accordance with Task Order requirements and shall not exceed the funded amount on this Task Order. The contractor shall ensure that the prices quoted are fair and reasonable at the time of submission and are in the best interest of the Government.

Please contact me at (area code) 000-0000 *(insert requestor's phone number)* if you have any concerns or questions.

FEDSIM COR Approval:	
Signature	Dat
X	

DHS TPOC Concurrence:	
Signature	Dat
X	

Agency POC Concurrence (If needed):	
Signature	Dat
X	

CONSENT TO PURCHASE PARTS/TOOLS/ODCs AND/OR SERVICES (CTP)

Industry Partner:
Client: DHS
Agency/Division Supported:
RFS Number:

CTP#:
Date:
Project Name: DHS CDM DEFEND Group D
Contract/Task Order:

If the prime contractor does not have an approved purchasing system, the contractor will prepare and submit a Consent to Purchase (CTP), to be reviewed by the COR and signed by the CO.

Last Inv submitted:

TO: FEDSIM Contracting Officer Representative

FROM: Requestor

THROUGH: Client POC

CLIN # VALUE:	**$0.00**
CUM AMT BILLED:	**$0.00**
BALANCE:	**$0.00**
CTP ESTIMATE:	**$0.00**
BALANCE:	**$0.00**

SUBJECT: Consent to purchase #

Client Point of Contact:

PURPOSE/JUSTIFICATION OF REQUEST:
The purpose of this request is to

Description of supplies or sevices (FAR 52.244-2(e)(1)(i)):

Type of subcontract (FAR 52.244-2(e)(1)(ii)):

Propose subcontractor (FAR 52.244-2(e)(1)(iii)):

Below is the estimated cost of purchase (FAR 52.244-2(e)(1)(iv)):

ITEM **Tool (CLIN #):**	
Cost to Government: @#	**$ -**
Fee	**$ -**
General & Administrative (G&A) Cost	**$ -**
Total Cost NTE:	**$ -**

All material purchases shall be made in accordance with customer requirements. All materials shall become the property of the Government and shall be regarded as Government Furnished Property (GFP), and unless previously approved by the Contracting Officer, shall be used only in performance of this Task Order. All materials will be purchased in accordance with regulations contained in FAR 52.244-2 approved purchasing procedures. All Tools and ODCs shall be procured in accordance with contract requirements and shall not exceed the funded amount on this contract.

It is the responsibility of the Industry Partner to ensure that the prices quoted are fair and reasonable at the time of submission and are in the best interest of the client. The Industry Partner is to furnish price quotes for hardware and software purchases.

The following documents are attached (as necessary):

1) Subcontractor's certified cost or pricing data as required in FAR 52.244-2(e)(1)(v)
2) Subcontractor's Disclosure Statement or Certification relating to Cost Accounting Standards as required in FAR 52.244-2(e)(1)(vi)
3) Negotiation memo as required in FAR 52.244-2(e)(1)(vii)

Please contact me at (202) 768-2212 if you have any concerns or questions.

FEDSIM CO Approval:

X _____ _____

Date

MATERIAL INSPECTION AND RECEIVING REPORT

Form Approved
OMB No. 0704-0248

The public reporting burden for this collection of information is estimated to average 30 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to the Department of Defense, Executive Services and Communications Directorate (0704-0248). Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

PLEASE DO NOT RETURN YOUR COMPLETED FORM TO THE ABOVE ORGANIZATION.
SEND THIS FORM IN ACCORDANCE WITH THE INSTRUCTIONS CONTAINED IN THE DFARS, APPENDIX F-401.

1. PROCUREMENT INSTRUMENT IDENTIFICATION (CONTRACT) NO.	ORDER NO.	6. INVOICE NO./DATE	7. PAGE	OF	8. ACCEPTANCE POINT

2. SHIPMENT NO.	3. DATE SHIPPED	4. B/L	5. DISCOUNT TERMS
		TCN	

9. PRIME CONTRACTOR	CODE	10. ADMINISTERED BY	CODE

11. SHIPPED FROM *(If other than 9)*	CODE	FOB:	12. PAYMENT WILL BE MADE BY	CODE

13. SHIPPED TO	CODE	14. MARKED FOR	CODE

15. ITEM NO.	16. STOCK/PART NO. DESCRIPTION *(Indicate number of shipping containers - type of container - container number.)*	17. QUANTITY SHIP/REC'D*	18. UNIT	19. UNIT PRICE	20. AMOUNT

21. CONTRACT QUALITY ASSURANCE

a. ORIGIN

☐ CQA ☐ ACCEPTANCE of listed items has been made by me or under my supervision and they conform to contract, except as noted herein or on supporting documents.

DATE | SIGNATURE OF AUTHORIZED GOVERNMENT REPRESENTATIVE

TYPED NAME:

TITLE:

MAILING ADDRESS:

COMMERCIAL TELEPHONE NUMBER:

b. DESTINATION

☐ CQA ☐ ACCEPTANCE of listed items has been made by me or under my supervision and they conform to contract, except as noted herein or on supporting documents.

DATE | SIGNATURE OF AUTHORIZED GOVERNMENT REPRESENTATIVE

TYPED NAME:

TITLE:

MAILING ADDRESS:

COMMERCIAL TELEPHONE NUMBER:

22. RECEIVER'S USE

Quantities shown in column 17 were received in apparent good condition except as noted.

DATE RECEIVED | SIGNATURE OF AUTHORIZED GOVERNMENT REPRESENTATIVE

TYPED NAME:

TITLE:

MAILING ADDRESS:

COMMERCIAL TELEPHONE NUMBER:

** If quantity received by the Government is the same as quantity shipped, indicate by (X) mark; if different, enter actual quantity received below quantity shipped and encircle.*

23. CONTRACTOR USE ONLY

TRAVEL AUTHORIZATION REQUEST (TAR)

Contractor:
Client:

TAR Number:
Date:
Project Name:
Project/Interagency Agreement (IA) Number:
Associated Line of Accounting:
Task Order Number:

TO: *(Insert First and Last Name)* , FEDSIM Contracting Officer Representative (COR)

FROM: *(Insert First and Last Name of requestor)*
THROUGH: *(Insert client organization and First and Last Name)* Technical Point of Contact (TPOC)

SUBJECT: Travel Authorization Request # *(insert number)*

DATE: *(Insert date)*

	Last Invoice submitted:	
CLIN X00X VALUE:	**$**	**-**
CUMULATIVE AMOUNT BILLED:	**$**	**-**
CURRENT CLIN X00X BALANCE:	**$**	**-**
TAR ESTIMATE:	**$**	**-**
NEW CLIN X00X BALANCE:	**$**	**-**

PURPOSE/JUSTIFICATION OF REQUEST:

Traveler:

Name	Company

Travel Itinerary:

Departure:	Date	Origin/Destination		Return:	Date	Origin/Destination
Leave				Leave		
Arrive				Arrive		
Leave				Leave		
Arrive				Arrive		

	Estimated Cost

FEDSIM is a Client Support Center housed within GSA, FAS, AAS.
Version 05-10-17

TRAVEL AUTHORIZATION REQUEST (TAR)

Travel (CLIN X00X)	**$ -**
Airfare: @	$ -
Per Diem: @	$ -
Hotel: @	$ -
Other: *(insert as appropriate; i.e. car rental)*	$ -
Other Direct Costs (CLIN X00X)	
(Insert as appropriate)	$ -
Subtotal Amount	**$ -**
Indirect Handling Cost	$ -
General & Administrative (G&A) Cost	$ -
Total Travel Cost (CLIN X00X)	$ -
Total ODC Cost (CLIN X00X)	$ -
Total Trip Cost NTE	**$ -**

Remarks:

The estimated cost of travel must represent the contractor's best estimate. The amount obligated for this line item may be increased unilaterally by the Government if such action is deemed advantageous. Travel costs shall be reimbursed in accordance with Federal Travel Regulations (FTR) and the Joint Travel Regulations (JTR). Please note that a separate TAR should be submitted for each individual traveler.

Please contact me at (area code) 000-0000 *(insert requestor's phone number)* if you have any concerns or questions.

Contractor Requestor:	FEDSIM COR Approval:	DHS TPOC Acceptance:
Signature Date	Signature Date	Signature Date
X	X	X

ATTACHMENT P
TRIP REPORT TEMPLATE

Trip Report Date:	[Trip Report shall be completed within 5 workdays following completion of each trip (unless specified otherwise in Section F).]	
Project Name:		
Task Order Number:	GSC-QF0B-33118	
Name of Traveler	[Provide First and Last name of Traveler]	
Location of Travel	**From:** [Origin]	**To:** [Destination]
Duration of Trip	**From:** [insert Month Day, Year]	**To:** [insert Month Day, Year]
Point of Contact (POC) at Travel Location	[Provide First and Last name of POC]	
Government Approval Authority Received	[Provide Travel Authorization Request (TAR) Number]	
Total Cost of the Trip	$	

Purpose of the Trip
[Provide a detailed description of the purpose of the trip. Attach additional pages, if necessary.]
Knowledge Gained
[Provide a detailed description of any knowledge gained. Attach additional pages, if necessary.]
Comments, Conclusions, Action Items:
[Provide any additional comments, conclusions, or action items. Attach additional pages, if necessary.]

ATTACHMENT Q
PROBLEM NOTIFICATION REPORT (PNR)

Task Order Number:	GSC-QF0B-18-3318
FEDSIM COR was verbally notified on:	[Notify the FEDSIM COR as soon as it becomes apparent that a scheduled delivery will be late.]
Date PNR Submitted:	[insert Month Day, Year]

Nature and Source of Problem:
[Provide a detailed description of the nature and source of the problem. Attach additional pages, if necessary.]
Is action required by the Government?
Yes/No [If Yes, describe Government action required and date required.]
Will the problem impact delivery schedule?
Yes/No [If Yes, identify which deliverables will be affected and extent of the delay, the rationale for late delivery, and overall project impact.]
Can required delivery be brought back on schedule?
Yes/No [Explain]
Describe corrective action needed to resolve problems:
[Provide a detailed description of corrective action needed to resolve the problem. Attach additional pages, if necessary.]
When will corrective action be completed?
[Provide the new delivery schedule and anticipated completion date.]
Are increased costs anticipated?
Yes/No [If Yes, identify the amount and nature of the increased costs anticipated and define Government responsibility for problems and costs.]

INSTRUCTIONS -- Fill in only the columns/colors per instructions below. DO NOT delete or sort any rows in this spreadsheet.
1. Each tab (for each period) must list all proposed staff, whether they are used in a particular performance period or not. If proposing staff in one or more, but not all periods (e.g., only for surge periods), zero out the hours for staff during the performance period in which staff is not proposed to work. DO NOT delete or sort any rows in this spreadsheet.
2. In the functional roles column, include not only the Functional Role title, but also a description of the duties and/or tasks performed by the individual in that role. This is regardless of whether there is a named individual proposed for the Functional Role or if it is To Be Determined (TBD).
3. In the qualifications column, include the qualifications, expertise and certfication(s) of the proposed individual, or, if an individual has not yet been identified, include the qualifications, expertise, and certifications to fill the requirements of the position.
4. Each row should represent one proposed personnel regardless of whether a name is provided or TBD. For example, for ten TBD Data Analysts, use ten rows; specify in each row the hours, functional role description, clearance level at time of proposal submission, qualifications, expertise, certifications, etc. of the proposed individual/position. DO NOT combine the hours for ten TBD Data Analysts into one row.

Desirable Skills & Qualifications

It is desirable for an Offeror to propose Key Personnel that possess the following skills/qualifications.

Task 1

a. Experience implementing IT security projects in complex and heterogeneous environments
b. Experience leading integration planning activities of multiple U.S. Government Agencies on a scale similar to this Task Order (TO)
c. Experience leading multi-organizational and matrixed technical resources and teams in accordance with approved integration plans and TO terms and conditions
d. Experience managing complex, heterogeneous enterprise security integration projects across multiple disciplines for U.S. Government Agencies
e. Knowledge of system architectures, networks, and operations
f. Technical leadership in Enterprise Architecture (EA), Service Oriented Architecture (SOA), and IT Service Delivery to multiple U.S. Government Agencies

Task 2

a. Current Certified Information Systems Security Professional (CISSP) certification
b. Experience implementing IT security projects in complex and heterogeneous environments
c. Experience developing, configuring, and delivering commercial off-the-shelf (COTS) software in support of enterprise security solutions
d. Experience managing technical integration and solution delivery issues
e. IT security operational experience, including assessment of information assurance and interoperability

Task 3 and Task 4

a. Current CISSP certification
b. Experience implementing IT security projects in complex and heterogeneous environments
c. Experience developing, configuring, and delivering COTS software in support of enterprise security solutions
d. Experience managing technical integration and solution delivery issues
e. IT security operational experience, including assessment of information assurance and interoperability
f. Experience developing and integrating continuous monitoring capabilities
g. Experience developing cyber security solutions across a diverse and heterogeneous IT environment
h. Expertise in security policy and implementation
i. Experience working with security authorization requirements, developing and enhancing the security risk posture, and analysis and reporting of IT security metrics
j. Experience in security policy and emerging cyber security technologies
k. Demonstrated experience in security solution design using existing and emerging technologies to achieve enterprise solutions

Task 5

a. Experience with risk management, issue resolution, problem solving, and customer service

ATTACHMENT T
DELIVERABLE ACCEPTANCE/REJECTION FORM

Dear [insert FEDSIM Contracting Officer's Representative (COR) Name]:

Please review the deliverable identified below, provide any comments in the space provided or on an attached form, and sign and date. Comments are due by [insert Month Day, Year].

DELIVERABLE NAME:	
AGENCY NAME:	
PROJECT NAME:	DHS CDM DEFEND Group D
FEDSIM TASK ORDER/ CONTRACT NUMBER:	
FEDSIM PROJECT NUMBER:	
DELIVERABLE DUE DATE:	

I have reviewed the aforementioned document and have:

- ☐ Accepted without comments
- ☐ Accepted with comments
- ☐ Rejected with comments

COMMENTS:

_____ _____
Signature Date

General Information

Company Name: Click here to enter text.

Corporation Type (check one): ☐**Public** ☐**Private** ☐**Other** ☐**Unknown**

Major Product: Click here to enter text.

DUNS Number: Click here to enter text. **Stock Exchange:** Click here to enter text.

Stock Symbol: Click here to enter text. **Established Date**: Click here to enter text.

Incorporated Date: Click here to enter text. **Web Address:** Click here to enter text.

Central Contractor Registration (check one): ☐**Active** ☐**Inactive** ☐**None**

Central Contractor Registration Date: Click here to enter text.

Is Foreign? ☐**Yes** ☐**No** **Has National Security Agreement?** ☐**Yes** ☐**No**

Products and Services:

SIC: Click here to enter text. **PSC:** Click here to enter text.

Cage/NCage Code: Click here to enter text. **NAICS:** Click here to enter text.

Contract Information:

Company Phone: Click here to enter text.

Company Point of Contact (POC): Click here to enter text.

Company POC Phone: Click here to enter text.

Street Address Type (check one): ☐**Headquarters** ☐**Satellite Location** ☐**Sales Office** ☐ **Manufacturing Plant** ☐**Distribution** ☐**Other**

Address: Click here to enter text.

City: Click here to enter text. **State:** Click here to enter text.

Zip/Postal: Click here to enter text. **Country:** Click here to enter text.

Foreign Ownership, Control or Influence

1a. (For entities which issue stock): Do any foreign person(s), directly or indirectly, own or have beneficial ownership of 5% or more of the outstanding shares of any class of your organization's equity securities? ☐Yes ☐No If yes, please list all parents, both foreign and domestic, by name and address, through to the ultimate parent, to include percentage of ownership. This should include any and all foreign investments in the entity. Include country of origin. Include any special rights or privileges involved in the ownership. Foreign person is defined as any foreign interest and any U.S. person effectively owned or controlled by a foreign interest. Foreign interest is defined as any foreign government, to include any agency or representatives of that government; or any form of business or legally organized entity chartered or incorporated under the laws of any country other than the U.S. or its possessions; and any person who is not a citizen of the U.S. **Click here to enter text.**

1b. (For entities which do not issue stock): Has any foreign person directly or indirectly subscribed 5% or more of your organization's total capital commitment? ☐Yes ☐No If yes, please list all parents, both foreign and domestic, by name and address, through to the ultimate parent, to include percentage of ownership. This should include any and all foreign investments in the entity. Include country of origin. Include any special right or privileges involved in the ownership. Foreign person is defined as any foreign interest and any U.S. person effectively owned or controlled by a foreign interest. Foreign interest is defined as any foreign government, to include any agency or representatives of that government; or any form of business or legally organized entity chartered or incorporated under the laws of any country other than the U.S. or its possessions; and any person who is not a citizen of the U.S. **Click here to enter text.**

2. Does your organization directly, or indirectly through your subsidiaries and/or affiliates, own 10% or more of a foreign interest? ☐Yes ☐No If yes, please list all involved by name, address, and country, with percentages of ownership. Include the names of the personnel running the facilities. **Click here to enter text.**

3. Do any non-U.S. citizens serve as members of your organization's board of directors (or similar governing body), officers, executive personnel, general partners, regents, trustees or senior management officials? ☐Yes ☐No If yes, please list ALL corporate officers (Chairman of the Board, President, Chief Executive Officer, Vice-Presidents, Secretary, Treasurer, Chief Information Officer, Chief Financial Officer, and General Counsel), executive personnel (Facility Security Officer) and all other Board of Director members by full legal name, title, date and place of birth, social security number (SSN), and citizenship. **Click here to enter text.**

4. Does any foreign person(s) have power, direct or indirect, to control the election, appointment, or tenure of members of your organization's board of directors (or similar governing body) or other management positions of your organization, or have the power to control or cause the direction of other decisions activities of your organization? ☐Yes ☐ No If yes, identify the individuals by full legal name, title, and citizenship. Provide a full explanation of the individual's control or influence. **Click here to enter text.**

5. Does the organization have any contracts, agreements, understandings, or arrangements with a foreign person(s)? ☐Yes ☐No If yes, this would include licenses, distributorships,

contracts, purchase orders, sales agreements, etc. For each instance, provide the name of the foreign entity, its country, the percentage of gross income derived, and the nature of the involvement including what type of technology or product is involved, whether the product or service is either defense or nuclear related, whether classified or export controlled information is involved, and whether there is compliance with all U.S. export laws. If not defense or nuclear related, the listing of contracts can be done by listing similar equipment by country and percentage. **Click here to enter text.**

6. Does the organization, whether as borrower, surety, guarantor or otherwise have any indebtedness, liabilities, or obligations, to a foreign person(s)? ☐Yes ☐No If yes, give details concerning with whom the debt or guarantee is, where they are located, the conditions or covenants regarding the debt, and what collateral, if any, was pledged. If stock or assets are pledged, provide copies of the pertinent documents. Provide details on procedures for default of the loans. This answer must be answered affirmatively even if the entity holding the loan is a U.S. entity of a foreign institution. **Click here to enter text.**

7a. During your last fiscal year, did your organization derive 5% or more of its total revenues or net income from any single foreign person? ☐Yes ☐No If yes, please identify the sources from which the income is derived, to include name of entity, country, and percentage. Identify, whether classified or export controlled information or technology is involved. If so, attach copies of licenses. **Click here to enter text.**

7b. During your last fiscal year, did your organization derive in the aggregate 30% or more of its revenues or net income from foreign persons? ☐Yes ☐No If yes, please identify the sources from which the income is derived, to include name of entity, country, and percentage. Identify, whether classified or export controlled information or technology is involved. If so, attach copies of licenses. **Click here to enter text.**

8. Is 10% or more of any class of your organization's voting securities held in "nominee" share, in "street names" or in some other method which does not identify the beneficial owner? ☐Yes ☐No If yes, identify the foreign institutional investors by name, address, and percentage of securities owned. Indicate whether there have been any attempts to exert control or influence over management or policies of the organization. If available, include SEC Schedules 13D or 13H. **Click here to enter text.**

9. Do any members of your organization's board of directors (or similar governing body), officers, executive personnel, general partners, regents, trustees or senior management official hold any positions with, or serve as consultants for any foreign person(s)? ☐**Yes** ☐**No** If yes, identify by name, title, citizenship or immigration status, whether the individual holds a personnel security clearance or is excluded from access, each individual meeting this criteria. Also, identify the name and address of each organization with which the individual holds a position, and in what capacity. **Click here to enter text.**

10. Are there any other factor(s) that indicate or demonstrates a capability on the part of foreign person(s) to control or influence the operations or management of your organization? ☐Yes ☐No If yes, please describe in detail the involvement of the foreign entity, as well as why it is not reportable in accordance with the previous questions. **Click here to enter text.**

Key Management and Personnel List (KMPL)

*Only required if the procurement is classified and requires a security clearance.

Name: Click here to enter text.

Position Title: Click here to enter text.

SSN: Click here to enter text.

Citizenship: Click here to enter text.

Born: Click here to enter text.

Clearance: Click here to enter text.

Submitted: Click here to enter text.

Comments: Click here to enter text.

Company Relationships

Company: Click here to enter text.

Relationship Type (check one): ☐**Former Name** ☐**DBA** ☐**Nickname**
☐**Other (e.g.,, partnership, parent, subsidiaries, suppliers, etc.)**

Related To: Click here to enter text.

Action: Click here to enter text.

Department of Homeland Security

Continuous Diagnostics and Mitigation (CDM) Program

CDM Test Team Strategy for Solution Independent Verification and Validation (V&V)

Version 1.2

March 16, 2017

Independent Verification and Validation (IV&V) Strategy

For

Federal Network Resilience

Continuous Diagnostics and Mitigation (CDM) Program

This document is under formal change control. Modifications to this document must be documented and reviewed by the appropriate change control board prior to usage or distribution.

Submitted by:

CDM Test Team — Date

Endorsed by:

Garfield Jones CDM Test and Evaluation Manager — Date

Approved by:

Kevin Cox CDM Program Manager — Date

Table of Contents

Table of Contents 2

Revision Summary 4

Executive Summary 5

Section A: Overview 6

A.1. Background 6

A.1.1. CDM Test Team 6

A.1.2. Solution Provider T&E Responsibilities 7

A.1.3. Defining IV&V 8

A.1.4. Purpose of IV&V 9

A.2. CDM TEMP References 9

A.2.1. DT&E Overview 9

A.3. CDM Systems Engineering Life Cycle Reference 9

A.3.1. CDM Systems Engineering Life Cycle Process 9

A.3.2. CDM Systems Engineering Life Cycle Test Milestones 10

A.3.3. CDM Test Risk Reduction Strategy 12

Section B: CDM Test Team IV&V Strategy 14

B.1. Technical Documentation Review 14

B.1.1. Design Documentation 14

B.1.2. Requirements Decomposition and Traceability Matrices 14

B.1.3. T&E Strategy, Test Design, and Test Plans 15

B.2. CDM Test Event Coordination 17

B.2.1. Task Order Working-level Integration Product Team 17

B.2.2. Test Readiness Review 17

B.2.3. Test Readiness Review Checklist 17

B.3. Test Event Observation 18

B.4. Data Analysis and Reporting 18

Section C: Examples and References 19

C.1. Requirements Decomposition, Testability, and Traceability 19

C.2. Test Plans 19

C.3. Test Reports 19

C.4. Test Readiness Review Checklist 20

C.5. Test Plan Categorization Guidelines 22

1.0 Overview 22

2.0 Identify Testable Requirements 23

3.0 Categories of Limitations 23

4.0 Impact on Test Documentation 25

5.0 Impact on Test Execution 25
6.0 Impact on Event Scoring 25

Revision Summary

The Table of Changes below describes specific changes, including references to changed sections/paragraphs.

Version	Document Date	Affected Pages	Revised By	Description of Change
1.0	7 May 2015	N/A		Original Copy
1.1	22 May 2015	Multiple		Incorporated comments from CDM PMO, DHS DOT&E, and the OTA
1.2	XX March 2017	All		Incorporated comments from CDM PMO, DHS DOT&E, and the OTA

Executive Summary

The Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) Test Team has the role of identifying risks and assessing readiness of the capabilities delivered by the solution providers to enter operational use and operational test and evaluation (OT&E). To accomplish this, the CDM Test Team follows the Developmental Test and Evaluation (DT&E) strategy outlined in the CDM Test and Evaluation Master Plan (TEMP)[1] and CDM Systems Engineering Life Cycle (SELC)[2]. The foundation of that strategy includes the independent verification and validation (IV&V) of the solution providers' delivered solution, DT&E-related activities, documentation including review of technical documentation (solution design documentation, test plans, test cases, requirements traceability matrices (RTMs), and other required test documents as required), test data and analysis, and other relevant information. This document provides additional detail so that the solution providers understand this IV&V process, understand what information the CDM Test Team expects to receive, and can more effectively communicate with the CDM Test Team during the V&V process. This document also contains reference test plans, RTMs, and requirements engineering guidance and includes both the CDM solutions awarded to the Continuous Monitoring as a Service (CMaaS) holders as well as the Agency and federal level dashboard activities.

[1] (April 2017) Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) Test and Evaluation Master Plan (TEMP) v2.1
[2] (18 April 2016) DHS Guidebook, 102-01-103-01, Systems Engineering Life Cycle Guidebook (SELC)

Section A: Overview

A.1. Background

A.1.1. CDM Test Team

The CDM Test Team is comprised of government and contract personnel that are Subject Matter Experts (SME) in Test and Evaluation (T&E). The CDM Program Management Office (PMO) appoints the CDM government Test Lead to oversee all the testing activities, documentation reviews, and content submissions to the PMO for approval. The Developmental Test and Evaluation (DT&E) is observed and verified by John's Hopkins University (JHU) Applied Physics Lab (APL), industry T&E SMEs, and the CDM Test Team Test Lead. The Operational Test and Evaluation (OT&E) is observed and validated by the Federally Funded Research and Development Center (FFRDC), the Institute for Defense Analysis (IDA) who are the Operational Test Agent (OTA) and report to the Director of Operational Test and Evaluation (DOT&E). DOT&E is the final approval authority on the OT&E and provides recommendations to the PMO on the success of the OT&E event, potential deployment and viability of each solution.

The objectives of the CDM Test Team include the determination regarding the CDM Federal and Agency Dashboards and Continuous Monitoring-as-a-Service (CMaaS) Solutions meet the following requirements as defined in the CDM Operational Requirements Document (ORD)[3]. In addition, the CDM Test Team will identify issues and risks while assessing the readiness for the Operational Test and Evaluation (OT&E) and deployment.

- Program Requirements
- Functional Requirements
- Operational Requirements
- Performance Requirements
- Security Requirements

The CDM Test Team government Test Lead will Chair the Test and Evaluation (T&E) Working-level Integrated Product Team (WIPT) which is comprised of the CDM Test Team, CDM Program Manager (PM) and the CDM Solution Provider PMs, systems engineering personnel, requirements personnel, and any required Subject Matter Experts (SMEs) that conduct CDM Program Technical Analysis to support all levels of DT&E.

The CDM Test Team has the following responsibilities as detailed in the program's Test and Evaluation Master Plan (TEMP) produced by the CDM WIPT for the following:

- Provide oversight of the DT&E activities on behalf of the CDM Program Management Office (PMO)

[3] (March 2017) Continuous Diagnostics and Mitigation (CDM) Operational Requirements Document (ORD) v 3.0

- Conduct Independent Verification & Validation (IV&V) of the Solution Providers delivered capabilities, specifically on Level-1 and Level-3 DT&E; this will be executed under CDM PMO oversight, to include the review of technical documentation such as:
    - Solution Design documents
    - Solution Provider TEMP
    - Requirements Traceability Matrix (RTM)
    - Solution Provider Test Plans
    - Solution Provider Test Cases / Test Steps
    - Test Data
    - Analysis and Assessments
- Conduct Level-2 DT&E, this is optional though can be required at the CDM PMO's discretion or the request of the Solution Provider. Level-2 will be conducted by the CDM Test Team on behalf of the CDM PMO to verify technical and functional specifications, confirm issue resolution, reduce program risks, gather additional data, and ensure readiness to proceed to Level-3 DT&E in the Agency environment
- Conduct IV&V on Level-3 DT&E testing activity which will be conducted in the Agency environment with formal approval from the Agency prior to the test event
- Document any of the Solution Providers deficiencies, defects, and limitations throughout the acquisition process based on the DT&E analysis and assessments
- Track the Solution Providers testing status, highlight issues or concerns to the PMO and the Solution Provider to ensure they are aware and able to take corrective action immediately
- Provide any clarifications to the CMaaS Solution Provider as it relates to the test documentation

A.1.2. Solution Provider T&E Responsibilities

The CDM Test Team requires each CMaaS and Dashboard Solution Provider, subject to official task order (TO) direction, to be responsible for the following T&E-related activities:

- Define their own DT&E strategy; present their strategy to the CDM Test Team along with the design documentation to the CDM PMO for review and acceptance at the Critical Design Review (CDR) or an equivalent design review such as a Solution Design Review (SDR) to support their solutions technical analysis along with their DT&E development plan
- Perform Level-1 DT&E in the Solution Provider development environment, support Level-2 DT&E (if requested or required) in a Government designated environment, and support Level-3 DT&E in the Agency environment including but not limited to component testing, modeling and simulation (M&S), integration testing, systems testing, cybersecurity testing and user acceptance testing (UAT)

- Conduct requirements analysis to include decomposition of the government provided requirements. The Solution Provider will develop derived requirements, as applicable, and develop an RTM which describes requirements relationships and how the solution provider intends to verify these requirements
- Conduct a Test Readiness Review (TRR) prior to each test event which must address all items on the TRR checklist and present the information to the CDM Test Team for concurrence that all items have been met to proceed to the designated Test Milestone as identified in the CDM Systems Engineering Lifecycle (SELC) or the CMaaS Tailored SELC set forth by the PMO
- Provide test plans, test procedures, test reports, and access to testing activities to the CDM Test Team and the OTA within a designated agreed upon timeframe by the Solution Provider and the CDM Test Team to ensure adequate time has been provided for a thorough review of the Solution Provider content
- The CMaaS Solution Provider will verify the tools and sensors that comprise their solution and satisfy program requirements
- The CMaaS Solution Provider and Agency, based on Agency specific policy, will ensure interoperability with the Federal and Agency dashboard

A.1.3. Defining IV&V

The CDM program method for Independent Verification and Validation (IV&V) is made up of DT&E and OT&E. Both types of evaluation are required for each Solution Provider to demonstrate their Agency Solution (s) which should adhere to the specific Task Order (TO).

DT&E focuses on the verification of the functional requirements for the Agency Solution. The primary audiences for the DT&E are the following participants: the CDM Test Team, the designated Solution Provider, CDM PMO, GSA contracting team and to a limited extent, the specific Agency involved. The DT&E activity addresses the solution through Level-1 and Level-3.

OT&E focuses on the validation of the operational requirements and how those requirements achieve the KPP's and meets the required operational thresholds as stated in the Operational Requirements Document (ORD) inside the Agency environment. The use of these methods will demonstrate that their Solution(s) meet the CDM program operational, functional, performance, and security requirements. The primary audience for the OT&E is the Director of Operational Test and Evaluation (DOT&E). For further explanation, reference on DT&E and OT&E, reference the DHS CDM TEMP.

The results are used to inform the CDM PMO as to the status of the delivered capabilities. The CDM Test Team defines IV&V as follows:

- Verification: The process of comparing system attributes to predefined systems and functional requirements (i.e., did you build the system right?)
- Validation: The process of assessing whether a system will satisfy mission needs (i.e., did you build the right system?)

- Independent: This indicates the CDM Test Team independence from the Solution Provider. This separation exists for the purposes of providing the CDM PMO with unbiased analysis of solution provider activities. However, the CDM Test Team verification observation is not independent from the PMO, the Operational Test Agent (OTA) provides an independent validation and is considered independent from the PMO.

A.1.4. Purpose of IV&V

The CDM Test Team performs IV&V in order to:

- Ensure that the acquired solutions meet CDM program requirements
- Ensure readiness for operational use and minimize the risk of operational or technical issues that may arise in OT&E
- Identify gaps between CDM program requirements and mission needs through requirements and solution capabilities validation
- Identify risks and provide recommendations for potential mitigation activities (as applicable), and report to the program as early as possible so that the CDM PM can make informed decisions

A.2. CDM TEMP References

The following section contains summarized excerpts from the DHS CDM TEMP for reference. For additional information, see Section C of the DHS CDM TEMP.

A.2.1. DT&E Overview

The goal of the DT&E activities for the CDM Program is to verify functional and technical specifications, including those related to interoperability and cybersecurity, minimize program risk, and ensure readiness for operational implementation. This section summarizes the CDM Program's DT&E strategy. The CDM DT&E scope includes CMaaS solution integration, the D/A dashboard, and the federal dashboard; however, this does not include DHS DT&E of the tools and sensors incorporated into the CMaaS provider's solution since the criteria used for including tools and sensors on the CDM Blanket Purchasing Agreement (BPA) require only that these tools be available for sale and on Schedule 70. For more information, see the DHS CDM TEMP v2.1 section A.1.

A.3. CDM Systems Engineering Life Cycle Reference

A.3.1. CDM Systems Engineering Life Cycle Process

The following section contains summarized excerpts from the DHS CDM SELC for reference.

The major SELC activities represent the specific activities that all programs need to consider, regardless of the program's development methodology. Each major SELC activity has associated artifacts to record or document the results of the activities performed. SELC technical reviews

are conducted to assess a program's progress towards planned activities. Programs are required to document their specific approach for complying with the intent of the SELC activities, artifacts, and technical reviews. To note per the diagram below, the ALF Conditional Acquisition Decision Event (Event 0 and 2C) have been tailored out of the CDM language.

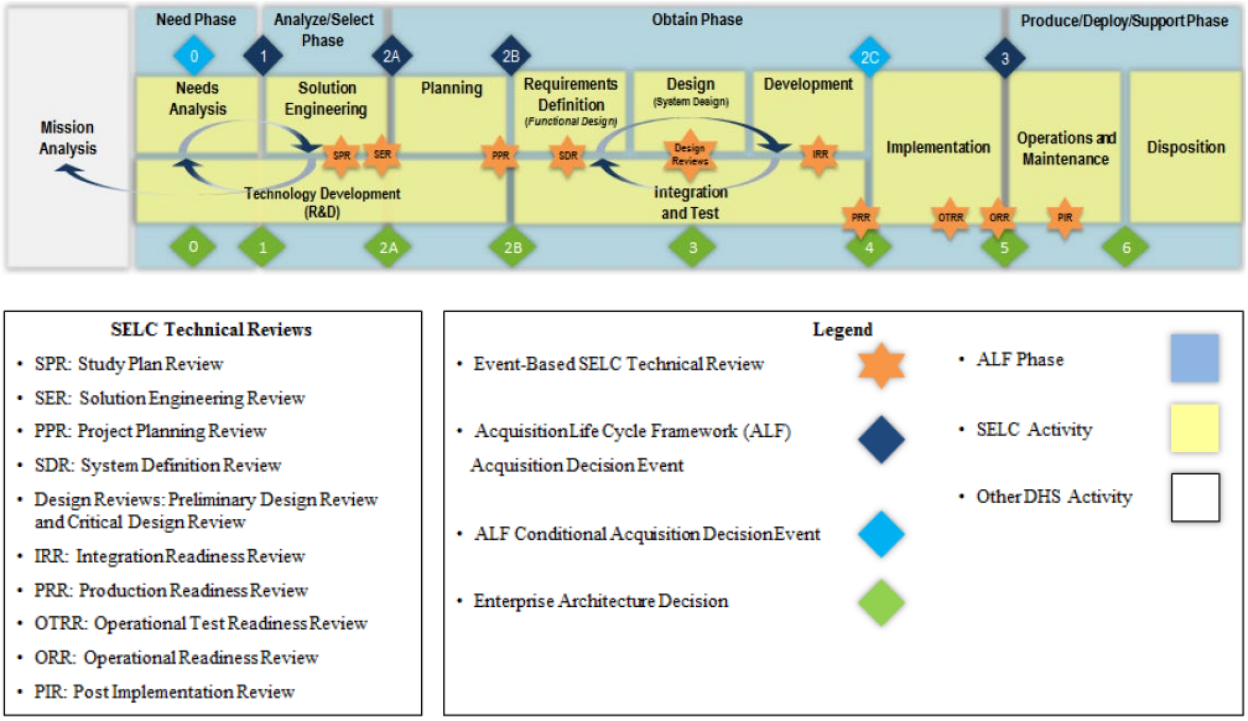


Figure 1-1: SELC Framework (with Acquisition Lifecycle Framework and Enterprise Architecture Decisions)

A.3.2. CDM Systems Engineering Life Cycle Test Milestones

SELC activities may be conducted concurrently, in parallel, or sequentially, with multiple feedback loops and iterations, as appropriate. The scope, content, and schedule of SELC technical reviews may vary based on a program's chosen development methodology. The CDM SELC milestones support the different phases of the acquisition process (Analyze/Select Phase, Obtain Phase, and the Produce/Deploy/Support Phase). The previous milestones are critical to the overall process however the milestone highlighted below are specifically focused on addressing the needs for the DT&E and OT&E.

Milestone: Stages into which a program or project is divided for monitoring and measurement of work performance; scheduled event that indicates the completion of a major deliverable event (or a set thereof) of a project. Milestones are measurable and observable and serve as progress markers.

Test Assessment: the process of documenting knowledge, skills, attitudes and beliefs, usually in measurable terms. The goal of assessment is to make improvements, as opposed to simply being

judged. In an educational context, assessment is the process of describing, collecting, recording, scoring, and interpreting information.

System Definition Review (SDR) Milestone: Focuses on the value, priority, traceability, and continuity of the functional and non-functional requirements. At this review the technical description of the system and top-level architecture is approved to establish the functional baseline for the system.

Production Readiness Review (PRR) Milestone: Conducted to review the results of Integration and Test to validate that the developed system meets defined requirements, and assesses system and manufacturing readiness for the move to limited production. This review supports an ALF ADE-2C decision.

Early Operational Assessment (EOA) – Test Assessment: EOA, typically an analysis, is conducted in accordance with an approved test plan, of the program's progress in identifying operational design constraints, developing system capabilities, and mitigating program risks. The PM can request the OTA conduct an EOA of prototype items of equipment. The EOA's purpose is to help the PM identify and reduce program risk before program initiation and prior to the Critical Design Review. EOA also assists in determining any system-unique test assets for future developmental and operational tests. The PM should request an Operational Assessment (OA) of weapons system components and/or system level Engineering Development Models (EDM) during the Engineering and Manufacturing Development phase to meet exit/entrance criteria and to help evaluate system performance and assess technical risk before Milestone C (production decision).

Operational Test Readiness Review (OTRR) – Test Assessment: Conducted to ensure the system is ready to enter OT&E. The ORR examines the actual system characteristics and the procedures used in the system or end product's operations and ensure that all system and support hardware, software, personnel, procedures, and user documentation accurately reflect the deployed state of the system.

The following are typical objectives of an ORR:

- Establish that the system is ready to transition into an operational mode through examination of analyses, and operational demonstrations
- Confirm that the system is operationally and logistically supported in a satisfactory manner considering all modes of operation and support (normal, contingency, and unplanned)
- Establish that operational documentation is complete and represents the system configuration and its planned modes of operation
- Establish that the training function is in place and has demonstrated capability to support all aspects of system maintenance, preparation, operation, and recovery.

Operational Readiness Review (ORR) Milestone: Assesses the system's operational effectiveness and suitability. The ORR also ensures that the system possesses the required manufacturing and logistics support capabilities and capacities, and is therefore ready to be moved into production, fielding, and operation. The ORR supports an ALF ADE-3 decision.

Post Implementation Review (PIR) Milestone: Documents deployment/implementation and coordination issues, how they were resolved, and how they could be prevented in the future.

A.3.3. CDM Test Risk Reduction Strategy

The CDM Program DT&E risk reduction strategy is designed to provide the flexibility required by the CDM Program's acquisition model, which has multiple mechanisms for solution implementation. The strategy streamlines efforts within the CDM PMO's available resources by leveraging the Solution Providers' testing, deployment, and support capabilities to the greatest extent possible through emphasis on Level-1 DT&E for requirements verification and identifying risks, and Level-3 DT&E for assessing readiness for operational implementation. This strategy also ensures that the CDM PMO has the leverage, if necessary, to perform additional risk reduction through Level-2 DT&E. Level-2 DT&E is optional and executed at the CDM PMO's discretion if resources, authority, and agreement with the D/A are available (Figure 2).

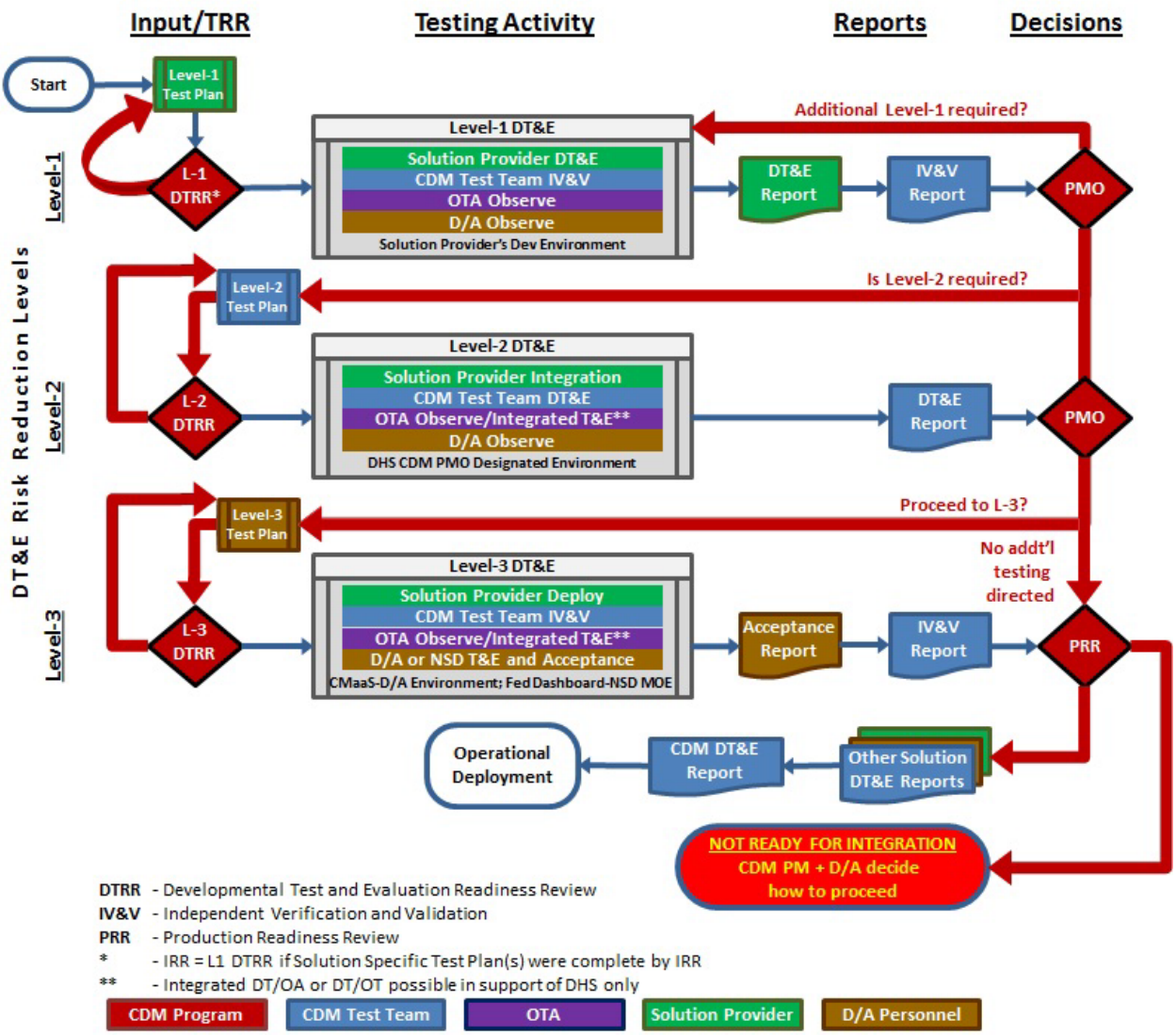


Figure 1 – CDM DT&E Integration Testing Risk Reduction Levels

Upon completion of DT&E activities directed for each solution, the CDM Test Team will provide an assessment of requirements satisfaction, risk, and readiness for operational implementation to the CDM PMO in preparation for a PRR. At the PRR, the CDM PMO will determine whether or not DT&E is complete for the evaluated solution based on CDM Test Team input, Agency acceptance of the solution, and other information sources as necessary. In addition, the CDM Test Team will provide a cumulative program wide DT&E assessment through analysis of all sources of available DT&E results and data which will be periodically provided to the CDM PMO at their request.

Section B: CDM Test Team IV&V Strategy

This section describes how the CDM Test Team conducts IV&V of the delivered solutions and solution provider DT&E activities. This section also provides specific guidelines to the solution provider for what documents they shall provide and what to expect during observed DT&E events.

B.1. Technical Documentation Review

B.1.1. Design Documentation

The CDM Test Team will review technical design documentation delivered by the Solution Provider for the purposes of understanding the approach to the specific solution and understating how CDM operational and functional requirements are being implemented. This documentation should clearly identify how individual solution components or integration of components will satisfy program requirements. This design documentation is evaluated for technical and integration strategy, comprehensiveness of solution, potential gaps in capability coverage, deployment/integration, and ability to meet program requirements.

Change and Configuration Management

The CDM Test Team will track, on behalf of the CDM PMO, any changes made to the original CDM program requirements as part of the Solution Provider's requirements analysis and decomposition. The repository of information will be used by the CDM PMO to review and approve any proposed requirements changes. The CDM Test Team will also track additional information for change and configuration management purposes including technical system baseline information, TO information, target Agency, test events, and other information is applicable. This activity enables the test team to analyze and track each CDM solution throughout its development, test, and deployment lifecycle and inform the PMO accordingly. In addition, each Solution Provider is responsible for change management tasking, as directed in their respective TO. The CDM Test Team's Change and Configuration Management will leverage input from the Solution Provider's change management process as appropriate.

B.1.2. Requirements Decomposition and Traceability Matrices

The CDM program is designed to give the solution provider flexibility in designing and defining the desired capabilities. The CDM operational requirements (as documented in the CDM ORD version 3.0, (March 2017) and the agency-specific technical requirements identified in the awarded TO, provide a high level framework that the solution provider must decompose and refine and/or derive to make specific to its solution. These refined requirements and any derived requirements must be clearly stated and testable. The government will provide an example RTM template (Section C.1) and guidelines on how to write acceptable derived functional

requirements (Requirements Engineering Plan (REP)) (Section C.1) as Government Furnished Information (GFI) to the solution provider as a guideline to help the solution provider develop their own RTM.

B.1.3. T&E Strategy, Test Design, and Test Plans

The Solution Provider shall provide the CDM Test Team a comprehensive Test Plan for each solution (there may be multiple solutions provided under an awarded TO) that includes their T&E strategy, test design, test cases, and test procedures. The strategy shall present a high level overview for the approach to testing the solution, whereas the test design shall detail specific methodologies to minimize redundancy in testing yet provide comprehensive assessment of all requirements. The government will provide as GFI a template test plan (Section C.2) describing the minimum expectations for the solution provider's test plan.

Test Cases and Test Procedures

The Solution Provider test plan shall include detailed test cases and test procedures that will collectively verify all requirements. The execution of a single test case may provide the necessary verification for multiple requirements. Designing efficient test cases to minimize the number of tests required to provide full coverage is the responsibility of the Solution Provider. Effective test cases should not contain compound requirements, if possible. This is to ensure each requirement can be demonstrated independent of one another for the greatest opportunity of success.

In addition, if multiple requirements are contained in one test step, the success rate to fully demonstrate that step reduces significantly if one requirement cannot be demonstrated. For efficiency, those dependent requirements or similar functionality to accomplish a step should be conjoined into one step.

Test Cases and Requirement Disposition

The CDM Test Team and Solution Provider document the requirement disposition after the observation of each test case. The CDM Test Team's disposition criteria are different from the Solution Provider disposition criteria. The rational is the Solution Provider has the authority to "Pass" or "Fail" a requirement within their test lab or Agency environment if the functionality is not or cannot be met at that time. The CDM Test Team does not have the authority to "Pass" or "Fail" a Solution Provider requirement only provide the disposition of the requirement at the time of testing through observation and verification of each requirement.

CDM Test Team disposition criteria are comprised of three disposition categories specific to the CDM Test Team. These criteria will be used in the IV&V Report assessment provided to the Solution Provider 10-15 days after the test event.

1. Requirement Successfully Demonstrated: The requirement fully met the language and criteria as stated in the PMO approved Requirements document and/or Acceptance Criteria.

2. Requirement Partially Demonstrated: The requirement partially met the language and criteria as stated in the PMO approved Requirements document and/or Acceptance Criteria.

3. Requirement Not Demonstrated: The requirement has not met the language and criteria as stated in the PMO approved Requirements document and/or Acceptance Criteria.

Given the requirement fails based on the Solution Provider's criteria or the CDM Test Teams categories of "Partially Demonstrated" or "Not Demonstrated" then that requirement should be categorized in one of five types which are defined in the Test Plan Categorization Guidelines.

Test Plan Categorization Guideline

To enable the ability to verify the requirements a Test Plan Categorization Guideline document has been provided to the Solution Providers. The purpose of this Test Plan Guidance is to provide the PMO with early and actionable information of any known reasons that requirements will not be demonstrable at the time the Test Plan is executed. Five categories of external limitations have blocked requirement demonstrations in the past, and have been standardized by the CDM Test Team.

- (A) Access (privilege or authorization to execute at the Agency)
- (T) Technology (structure, versioning, or technology under development)
- (R) Regression (Additional testing of current requirements for successful demonstration)
- (L) Lab Limitations/Environment (limitations of scale)
- (O) Other (limitations external to the performer. Explain is required.)

Test cases containing requirements which are blocked by external conditions should not be scheduled for execution, as it is already known that those requirements cannot be demonstrated. However, Solution Providers should still include the blocked and unblocked requirements in the same test case so that an accurate categorization of those requirements can be assessed at that current SELC milestone. This enables the categorization of metrics for the success rate of the test and overall Solution.

Quality Management

The CDM Test Team will review and analyze Solution Provider T&E products, data and manage that information for the entire CDM program as part of the CDM Test Team's quality management activity. This will allow for the analysis and archival of T&E material and tracing of the appropriate test artifacts to system baselines. This is tracked as part of our change and configuration management activity and the requirements are tracked as part of the CDM Test Team's requirements management activity. The quality management activity will also track the status of system issues or other discrepancies. The CDM Test Team will maintain this quality management activity in conjunction with requirements management and change and configuration management activities using IBM Rational® Quality Manager and/or equivalent

tool functionality. Access to this information is provided to the CDM PMO and made available to other stakeholders as approved by the PMO.

The prioritization of issues discovered during DT&E will be made using a discrepancy reporting priority scale defined in the Institute of Electrical and Electronics Engineers Standard 12207.2, p. 94.

B.2. CDM Test Event Coordination

B.2.1. Task Order Working-level Integration Product Team

The CDM Test Team and the Solution Provider will hold bi-weekly Working-level Integration Product Team (WIPTs) meetings to enable the collaboration between the CDM Test Team and the Solution Provider's Test Team. These meetings are a venue to address the status of the each Agency's testing process, required test artifacts, test results, concerns, issues or questions. The WIPT allows for the testing community to address the technical complexities that hinder may the success of a test event and plan for any remediation as necessary. This forum discusses test events for planned engineering iterations, technical implementation, expected solution results and ensures the testing is in compliance with DOT&E.

B.2.2. Test Readiness Review

The CDM Test Team participates in test readiness reviews (TRRs) prior to any DT&E or OT&E event as directed by the CDM PMO. The CDM PMO chairs the TRR, except for Level-1 DT&E where the Solution Provider presents their readiness level, including any risks to the CDM PMO. The CDM PM or their designated representative approves the Solution Provider to proceed with the planned testing activities given the criteria has been met. If the TRR criteria have not been met, the Solution Proved will not be permitted to proceed until the TRR criteria has reviewed and deemed acceptable to proceed.

B.2.3. Test Readiness Review Checklist

Prior to any DT&E or OT&E testing events stated in the CDM SELC or the Tailored Solution Provider SELC, each Solution Provider is strongly advised to complete a TRR checklist prior to the start of any test event. The TRR checklist ensures that the minimum essential entrance and exit criteria are met prior to testing to avoid any undue delays or the inability to complete the schedule test cases to verify the requirements. All test related items detailed in the TRR checklist should be turned in at least 7-10 calendar days before the scheduled test event to ensure proper review of the documentation by the CDM Test Team. The TRR checklist can be found in Section C.4.

B.3. Test Event Observation

Consistent with the Request for Proposals for the Task Orders (section 2.6.11 in the TO2 RFQs), the contractor is required to provide the project management, engineering, data and documentation necessary to conduct testing, support IV&V and support system authorization as required by the Task Order. ***The CDM Test Team must be invited to all solution provider DT events and will attend at the discretion of the CDM PMO***. At the discretion of the CDM PMO, all test event activity may not be observed; regardless, all data, analysis, and results must be provided to the CDM Test Team for all DT events. The CDM Test Team will observe DT events with an approved test plan to be executed and all tests are conducted and data is collected as defined in the test plan, any exceptions must be preapproved.

B.4. Data Analysis and Reporting

The solution provider shall provide copies of all data analysis and reporting of DT activities to the CDM Test Team for independent verification per section 2.6.11 in the TO2 RFQs.

Section C: Examples and References

C.1. Requirements Decomposition, Testability, and Traceability

Attached is GFI that provides a template that the solution provider shall follow to submit their requirements decomposition and traceability to the CDM PMO. Also included is guidance on writing verifiable requirements.

REQUIREMENTS TRACEABILITY MATRIX

Project Name:	<required>	**Primary POC Name:**	<required>
Task Order Number:	<required>	**Primary POC**	<required>
Solution Provider:	<required>	**Primary POC**	<required>
RTM Version Number:	<required>		

Source Document	Govt ID	Govt Requirement	Vendor ID	Vendor Requirement	Measureable Threshold	Vendor State	Rqmt Rationale	Additional Comments	Test Case Number(s)	Test Date(s)	Test Location
CRD Alt. I	101	The system shall be configurable to log all changes to the data by date, time, and account making the change.	As defined by the vendor (e.g., MTV-302.1)	The DIA dashboard shall be configurable to log all changes to the data (definition?) by date within 1 hour of the time that the change was made.	<Behavior> = Yes/No or Pass/Fail	Modified		See definition of data in Kim Watson's philosophy document	<As defined by the vendor>		Vendor Lab
CRD Alt. I	101	The system shall be configurable to log all changes to the data by date, time, and account making the change.	As defined by the vendor (e.g., MTV-302.2)	The DIA dashboard shall be configurable to log all changes to the data (definition?) by time within 1 hour of the time that the change was made.	<Behavior> = Yes/No or Pass/Fail	Modified		See definition of data in Kim Watson's philosophy document	<As defined by the vendor>		Vendor Lab
CRD Alt. I	101	The system shall be configurable to log all changes to the data by date, time, and account making the change.	As defined by the vendor (e.g., MTV-302.3)	The DIA dashboard shall be configurable to log all changes to the data (definition?) that are attributable to the person making the change within 1 hour of the time that the change was made.	<Behavior> = Yes/No or Pass/Fail	Modified		See definition of data in Kim Watson's philosophy document	<As defined by the vendor>		Vendor Lab

Figure 2 – Sample Requirements Traceability Matrix

RTM Template.xlsx

Requirements Engineering Plan.doc

C.2. Test Plans

Attached is GFI that provides a template that contains the minimum information the solution provider shall include in their test plans they submit to the CDM PMO.

Sample Test Plan.docx

C.3. Test Reports

Attached is GFI that provides a template that contains the minimum information the solution provider shall include in their test reports they submit to the CDM PMO.

Test Report Template_7-May-201

C.4. Test Readiness Review Checklist

Below is the Test Readiness Review (TRR) Checklist that contains the minimum information from the solution provider to move forward to their designated test event and shall include in their test plans submit to the CDM PMO.

CDM Test Readiness Review (TRR)

Purpose – The purpose of the CDM TRR is an informal review to address a set of entrance and exit criteria prior to each test milestone as set forth in the Systems Engineering Life Cycle (SELC) Guidebook. The TRR has been established to determine the readiness for formal testing by moving toward government concurrence with their solution provider. The TRR has a set of entrance and exit criteria as guidelines that must be addressed with the CDM Test Team, solution providers, government personnel, and all relevant parties to ensure the following conditions are met:

- Ensure the interpretation of requirements to be verified
- Identifying the environment that will be used for testing (lab and/or Agency)
- Plan and identify the verification method of the requirements, to include the combination of test methods (test, demonstration, analysis, and inspection) to be used
- Test case and detailed test procedures, with regard to the traceability of planned tests to program requirements as identified in the RTM
- Ensuring the test personnel of the systems have access and are familiar with the test cases and test steps
- Ensuring the user needs are met
- Ensuring the level of detail and sufficiency has been accounted for in the test cases and test steps
- The TRR can review any past test and defect mitigation results to ensure their resolution prior to initiation of future testing.

Entry Criteria:

The solution provider has provided all the information necessary for the conduct of the TRR to the government sufficiently in advance of the TRR for an effective review. The solution provider is prepared to participate in the TRR to verify the items indicated below. Upon request, the solution provider must be able to show specific information for each itemized criteria listed below to ensure the items have been successfully achieved prior to the test event.

TRR Verifies that:

1. All test cases and detailed test procedures have been placed under configuration management

2. A defined and agreed upon test configuration system has been shown to the CDM test team to include physical and/or virtual
3. The requirements associated with each test case and test step (as applicable) has been clearly identified
4. The planned set of test methods (test, demonstration, analysis, and inspection) to be used to verify traceability is documented for each specific requirement identified in the test
5. An explicit rationale is provided for how the planned collection of test steps across test cases will verify the requirement for each requirement identified in the test event
6. Before the PRR milestone, Level 1 functional testing must be successfully conducted and witnessed by the CDM test team
7. All the test scenarios have been identified and provided to the CDM test team
8. All user accounts have been established
9. The testers have access rights to the systems to verify the respective requirement
10. The facility access has been granted to perform the test
11. All required resources (people, facilities, test articles, test instrumentation) been identified and coordinated to support the planned tests
12. Adequate Government and contractor staffing (expertise and quantity) is available to execute the planned test
13. The Test Manager or other designated persons from the Agency is ready to accept the solution into the environment
14. The length/timeframe for the Pilot has been established
15. There a Risk Management Plan for the test event; including:
    - Test related risks have been determined to be of an acceptable level to enter testing
    - Conditions for continuing/terminating testing have been explicitly identified
16. The completed RTM and has been provided to the CDM Test Team to include:
    - Identification of what requirements are being tested
    - All the requirements for the specific test event have been decomposed/derived and clarified so that they are testable
    - All compound requirement are addressed in the test steps
17. A defect or discrepancy plan has been identified to include:
    - Identify if a repair/regression testing plan will be needed
    - Identify a fallback plan should a technical issue/potential showstopper arise during testing
18. All applicable test plans, test cases, test procedures, and test results have been made available for participants to review
19. The roles and responsibilities of all test participants have been defined, and accepted prior to the test event to include:
    - Training for all test personnel and related data collectors have been completed

20. The relationship of the planned test event to the overall test program has been documented
21. All required interfaces have been defined, documented, and will be tested
22. The Agency designated approval authority has reviewed the ST&E results and approved the System Under Test (SUT) for testing in the Agency environment

Exit Criteria:

The government concurs that the solution provider has achieved the items to be verified by the TRR and can address items indicated below:

1. All known anomalies have been documented, are understood, and deemed to not affect the ability to successfully complete the test event
2. Adequate test plans have been completed and approved for the SUT
3. All required resources been identified and coordinated prior to the SUT
4. All changes to architecture products have been reviewed and approved
5. All Test procedures comply with test plans
6. The Test scenarios are representative of anticipated operational environment
7. Test plans completed and approved for the System Under Test (SUT)
8. The latest version of the TEMP been reviewed and approved (if required)
9. The Test program is executable within the cost, schedule, and performance risks
10. Risk level identified and accepted by Program leadership, as required

C.5. Test Plan Categorization Guidelines

Below is the Test Plan Guidance that supports the identification and conditions that limit the test scope to enable the solution provider to accurately depict the requirement categorization. Each requirement must be verified and validated and this categorization enables each requirement to be articulated whereby metrics can be obtained for qualification and quantification.

Test Plans: Guidance on Identifying and Documenting Conditions that Limit Test Scope

1.0 Overview

The purpose of this Test Plan Guidance is to provide the Continuous Diagnostics and Mitigation (CDM) Program Management Office (PMO) with early and actionable information of any known reasons that requirements will not be demonstrable at the time the Test Plan is executed.

The “Limitations” section of each Test Plan should identify any resources external to the Continuous Monitoring as a Service (CMaaS) contractor that block successful demonstration of requirements. The information provided will set expectations for the results of the test

execution, focus effort on achievable goals, provide focus on critical paths, and enhance understanding of when it will become possible to demonstrate the blocked requirements.

2.0 Identify Testable Requirements

1. Please provide a table showing the total number of requirements in the Requirements Traceability Matrix (RTM). If any requirement in the RTM is not discussed in the test plan, explain why. If any requirements were demonstrated and accepted by the PMO during previous Test Events, provide a reference. This table and explanatory text should account for every requirement in the RTM.

Table 1. Disposition of RTM requirements to Test Cases, Limitations Preventing Demonstration, Previously Demonstrated, and Not Addressed. (Note: All requirements should be categorized in one or more of the five Limitations identified in Section 3.0.)

	A	B	C	D
Functional Area	# Requirements in **RTM**	# Requirements in RTM addressed in **Test Cases**	# Requirements in RTM addressed in **Limitations**	# Requirements demonstrated in **previous** Test Events
HWAM	100	70	20	0
SWAM	100	90	10	0
CSM	100	90	5	0
VUL	100	80	15	0
System	100	90	10	0
Total	500	420	60	0

2. External limitations on the demonstration of requirements are caused when one or more externally provided resources are not available (or not planned to be available) at the time of test execution. Identify both the resource and the resource provider. Provide the anticipated data of resource availability (and source of the information.) Identify the category or categories to which each limitation applies.

3.0 Categories of Limitations

The following categories of external limitations have blocked requirement demonstrations in the past, and have been standardized by the CDM Test Team in five categories.

(A) Access (privilege or authorization to execute at the Agency)

(T) Technology (structure, versioning, or technology under development)

(R) Regression (Additional testing of current requirements to enable successful demonstration)

(L) Lab Limitations/Environment (limitations of scale)

(O) Other (limitations external to the performer)

Examples of the types of external limitation are provided below.

(A) **Access**: High level privileges are required to demonstrate {functionality} in the pilot environment, but have not been granted by the Agency. Requirements impacted include {list}.

(T) **Technology**: Agency Dashboard v2.1 is required to demonstrate {functionality}, but has not yet been released. Requirements impacted include {list}.

(R) **Regression**: Verify the requirements which unable to be successfully demonstrated previously are retested to verify the successful demonstration of those requirements.

(L) **Lab Limitation/Environment:** (Insufficient network nodes are available to demonstrate requirement to support 100,000 nodes)

(O) **Other**: explain the external limitation and list the affected requirements an example: The risk scoring algorithm has not been defined by the PMO, therefore the risk scoring requirements {list} cannot be demonstrated.

Note that descriptions of external blocking conditions will be reviewed by the PMO in case the CMaaS contractor or the Agency can mitigate.

Table 2. Example table of test limitations and number of requirements affected. Indicate the type of limitation using the letter codes above. The POC is the name of the authoritative source consulted for the expected resolution date (e.g., delivery date) of the limitation. If needed, replace Phase 1 functional areas with the functional areas addressed in the Test Plan. The total number of requirements addressed should match the number in Column C of Table 1.

Limitation	Category(s)	Owner	Expected Date	POC	# HWAM Reqs	# SWAM Reqs	# CSM Reqs	# VUL Reqs	# System Reqs	Total Reqs Affected
Scoring	O	DHS	TBD		0	8	0	6	1	**15**
ADB R2.1	T	MTV	11/2016		4	0	0	3	2	**9**
Sys privs	A	D/A	IOC	CIO	16	2	5	6	7	**36**
Total	**-**	**-**	**-**	**-**	**20**	**10**	**5**	**15**	**10**	**60**

4.0 Impact on Test Documentation

Test cases for blocked requirements do not need to be included in the pre-test documentation, if the PMO concurs with the limitations. The CMaaS contractor may submit test case procedures for blocked requirements at the same time, but in a separate review package. With PMO approval, providers may choose to defer writing and submitting test cases for blocked requirements until the external condition resolves.

5.0 Impact on Test Execution

Test cases containing requirements which are blocked by external conditions should not be scheduled for execution, as it is already known that those requirements cannot be demonstrated. Providers should avoid mixing blocked and unblocked requirements in the same test case.

6.0 Impact on Event Scoring

Objectives of this guidance are to provide clearer measure of integration accomplishments during test events. In addition, provide a standardized categorization of disposition regarding requirements verification through demonstration across the CDM Test Team to enable the external community reviewing the results to have a common approach and standard terminology.

Past practice has been for integrators to not identify external blocking conditions in their test plans and to write test cases that could not succeed given the limitations. By not acknowledging the limitations, overly high expectations of achievement were fostered and then dashed.

By limiting the testing to the possible, the successes of the test event are highlighted and limitations that affect all of CDM are documented.

In Table 1 above, the legacy calculation would lead to the expectation of demonstrating 480 of 500 requirements, when only 420 can possibly be demonstrated. In this case, the old maximum success rate would be 420 out of 500 (84%). By omitting the blocked test cases

from the exercise, the integrator can show a maximum success of 420 out of 440 (95%) while providing the PMO with information on limitations that will impact future testing.

The DHS SELC provides a review process for the design and development of IT solutions, including a structured, formal handoff from developers/designers (engineering) to operations and maintenance staff. CDM efforts shall follow the DHS SELC process unless otherwise specified by the Agency, in which case the contractor shall follow the Agency SELC process in coordination with the DHS CDM PMO.

There are six key gates in the SELC:

a. Solution Design Review (SDR)

b. Service Readiness Review (SRR)

c. Production Readiness Review (PRR)

d. User Acceptance Test (UAT)/Operational Test Readiness Review (OTRR)

e. Operational Readiness Review (ORR)

f. Post Implementation Review (PIR)

For these gates, the contractor shall coordinate with Government stakeholders, including DHS CDM PMO, GSA FEDSIM, and participating Agencies, to ensure agreement on solution implementation, schedule, and deliverables necessary approval to proceed to the next phase for each Agency's respective CDM Solution. It is expected Agency stakeholders will review deliverables to ensure, at minimum, operational effectiveness and Agency polices are addressed.

The SELC process is governed through reviews that provide the opportunity to assess project progress against a minimal defined set of exit criteria tailored for the program. These reviews provide a knowledge point or mechanism for Government to determine if a project has completed the necessary activities.

The application of the SELC process is varied based upon timing and source (Agency vs. DHS CDM PMO) for the execution of the CDM capability. The Government anticipates three different scenarios as part of the SELC process.

The first scenario, as depicted in **Diagram 5: Tailored DHS SELC Process**, applies to CDM capabilities being executed at the Time of Award (TOA). This process identifies the initial Solution Design occurring at the TOA as part of the evaluation process.

The second scenario, also depicted in **Diagram 5**, applies to CDM capabilities being executed during the project period of performance through the use of the Request For Service (RFS) process (reference **Section C.5**). In this process, the initial Solution Design occurs with the Government review of the RFS response. The remainder of the process is consistent with **Diagram 5**.

The third scenario occurs when an Agency executes a CDM capability during the project period of performance and elects to remove DHS SELC review gates. The removal of any SELC gates would be identified in the corresponding RFS form, in accordance with Section C.4 - Request for Service.

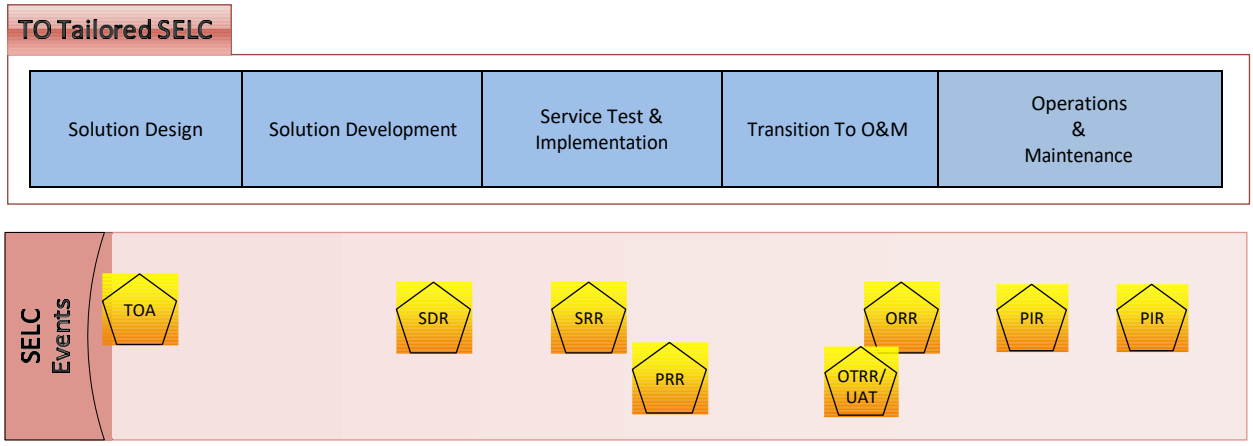


Diagram 5: Tailored DHS SELC Process

SELC Event Legend:
SDR - Solution Design Review
SRR- Solution Readiness Review
PRR - Product Readiness Review
ORR - Operational Readiness Review
UAT – User Acceptance Test Review
OTRR - Operational Test Readiness Review
PIR - Post Implementation Review

Factors critical to successful reviews are:

a. All stage activities and exit criteria, as tailored, for each review must be satisfactorily fulfilled, including required documents, in order to proceed.

b. At each SELC review, the contractor must provide evidence that clearly substantiates the fulfillment of the exit criteria. For example, in testing requirements, test cases designed to validate requirements compliance must successfully produce the required results to be used as evidence of successfully meeting exit criteria. The act of testing in itself is not sufficient evidence if tests fail to produce required results.

c. The Government expects that the prerequisite documents are submitted and Government reviewed before the actual gate review, ensuring that the Government has adequate time to prepare for a gate review.

d. The Government expects that the contractor reuse documentation where acceptable to limit the recreation and review of previously accepted documentation. In instances where only portions of a previously accepted SELC document requires updating, the contractor shall clearly denote the changes in the document allowing the Government to only have to review the changed content.

The Government's review time is not anticipated to exceed ten business days after receipt by the DHS CDM Program Office of documentation for each SELC review detailed below. The contractor shall coordinate directly with the DHS TPOC to manage the SELC review process.

1. SOLUTION DESIGN/DEVELOPMENT PHASE

The contractor shall complete the Solution Design/Development phase at the SDR, where key Government stakeholders will verify that all SDR deliverables are completed and acceptable and that the project baseline scope and schedule are still accurate or need to be adjusted.

The intent of this review is to provide all stakeholders with a common understanding of the solution design that was used as the basis of award [Baseline 0] or execution of a contractual modification from an RFS.

The prerequisite documents to enter the SDR are:

a. Overview of CDM Solution selection

b. Concept of Operations (CONOPS)

c. System Design to include Data Model/Architecture

d. Proposed deployment

e. Test and Evaluation Master Plan (TEMP)

f. Project Management Plan (PMP)

The specific deliverables are:

a. Documents noted above

b. Presentation materials

c. Baseline schedule (IMS) and Technical Bill of Materials (TBOM)

d. Identification of Next Steps

   1. Plan for resolution of SDR outstanding items
   2. Identification of items needs to SRR
   3. Timeline for SRR

2. SOLUTION TEST & IMPLEMENTATION PHASE

During this phase, the project transitions from designers to the operations staff. The Government will review the contractor's CDM Solution implemented in an evaluation environment and provide or withhold approval at the SRR. Later, the Government will review the contractor's CDM Solution against requirements of each Agency during the PRR.

The intent of this review is to provide all stakeholders with a common understanding of the design and implementation implications based on revalidation/discovery.

The prerequisite documents to enter the SRR are:

a. Demonstration of CDM Solution implementation

b. Initial Security Documentation (e.g., System Security Plan)

c. Initial core solution documentation (e.g., User Manuals)

d. Initial Governance Support Plan

The specific deliverables are:

a. Documents noted above
b. Presentation materials
c. Demonstration of solution
d. Baseline schedule (IMS) and TBOM
e. Identification of Next Steps
    1. Plan for resolution of SRR outstanding items
    2. Identification of items needs to PRR
    3. Timeline for PRR

The intent of PRR is to ensure that implementation is ready for deployments into an operational environment. The prerequisites to enter the PRR are:

a. Documentation and requirements for Agencies to move the CDM Solution to their environments
b. Demonstration of integration to the Agency environment (e.g., pilot).

The specific deliverables are:

a. Documents noted above
b. Presentation materials
c. Requirements Traceability Matrix
    1. Decomposed or Derived requirements from the source requirements (CDM Requirements Document **(Section J, Attachment Y)**, TO, and ORD)
d. TEMP update
e. Test Plan for each test event supporting the PRR
    1. Test cases for all functional requirements or reasons detailing requirements not test
    2. Defect Plan
f. Demonstration of solution
g. Baseline schedule (IMS) and TBOM
h. Identification of Next Steps
    1. Plan for resolution of PRR outstanding items
    2. Identification of items needs to UAT/OTRR
    3. Timeline for UAT/OTRR

3. TRANSITION TO OPERATIONS AND MAINTENANCE (O&M) PHASE

The Government will review the contractor's test and evaluation plan execution against the CDM Solution based on the requirements of the Agencies and the scope of the TO during the

Operational/User Acceptance RR. The contractor shall complete the Transition to O&M phase at the ORR. Government stakeholders will verify that all deliverables are completed and acceptable, and that operations staff are ready to deploy the CDM Solution into production and maintain and support it going forward.

The intent of ORR is to provide all stakeholders with the specific understanding of the ability to transition the solutions to operational status for each of the participating Agency environments.

The requirements to complete the UAT are:

a. Documentation and requirements to move the CDM Solution to the operational environments.

b. Documentation of Testing and Results.

The prerequisite to enter the ORR are:

a. Documentation and requirements for Agencies to move the CDM Solution to the operational environments

b. Results of Operational Testing, Security Risk Assessment

c. Finalized Deployment and Back-out Plan

d. Finalized CONOPS

e. Finalized CDM Solution documentation

f. Finalized Plan for Transition to Production Operations

g. Finalized Security Model and Accreditation Package

h. Plan for Production Operations

The specific deliverables are:

a. Documents noted above

b. Presentation materials

c. Demonstration of solution

d. Baseline schedule (IMS) and TBOM

e. Identification of Next Steps

    1. Plan for resolution of UAT/OTRR outstanding items
    2. Identification of items needs to Transition to O&M
    3. Timeline for Transition to O&M

4. OPERATIONS AND MAINTENANCE PHASE

After some period of operational maturity the Government may require PIR be held. For the PIR, the Government will review the contractor's CDM Solution in production for successful implementation and subsequently determine if expected benefits have been realized, including review of operational data measuring the CDM Solution’s effectiveness and confirming that it is delivering the desired service and support level. The Government may require PIRs periodically throughout the O&M phase and evaluate ongoing operation of the contractor’s CDM Solution.

The prerequisites to complete the PIR are:

a. Performance Reports
b. Operational Analysis
c. Ongoing Security Assessments (to include Plans of Action and Milestones (POA&M) tracking)
d. As-built documentation
e. Finalized Plan for Production Operations

The specific deliverables are:

a. Documents noted above
b. Presentation materials
c. Demonstration of solution
d. Baseline schedule (IMS) and TBOM

Continuous Diagnostics and Mitigation (CDM)

Technical Capabilities

Volume One

Defining Actual and Desired States

Version 1.1

July 18, 2017

Table of Contents

Introduction **4**
Security Frameworks Supported by CDM **6**
I - 1 CDM Architecture 6
I - 1.1 CDM ABCD Architecture 6
I - 1.2 CDM Requirements Core Design Concepts 8
I - 2 CDM and the Cybersecurity Framework Core 15
I - 3 CDM and NIST Risk Management Framework 19
I - 3.1 Ongoing Assessment and CDM 21
I - 3.2 Ongoing Authorization and CDM 21
I - 3.3 Leveraging NIST SP 800-53 Controls 22
I - 4 Defining CDM from Attachment N Requirement's Documents 27
I - 5 Conclusion 30
References **31**
III - Appendix A: Acronyms, Terms and Definitions **33**
III - Appendix B: Cybersecurity Framework Categories **40**

Table 1: Cybersecurity Framework Core Element mapping 16
Table 2: CDM Phased Attachment-N Requirements and Associated CDM BPA Capabilities 27
Table 3: Acronyms, Terms and Definitions 39

Figure 1-Phases of CDM 4
Figure 2-ABCD Notional Architecture (Phases 1 through 3) 7
Figure 3-CDM Data Model Legend 10
Figure 4-CDM Desired State Objects Relationship 14
Figure 5-CDM mapping to Cybersecurity Framework Core Functions and Categories 18
Figure 6-RMF OU Tiers 19
Figure 7-RMF Process Steps (Cyclical) 20

REVISION SUMMARY

Table of Changes

Version Number	Date	Revised by	Section
1.0	4/25/2017	CDM PMO	All
1.1	7/14/2017	CDM PMO	Reflecting edits from USDA, DOI and NIST

Introduction

Strengthening the security posture of Federal networks, systems, and data is one of the most important challenges we face as a nation. Therefore, the Department of Homeland Security (DHS) seeks to provide agencies with the Continuous Diagnostics and Mitigation (CDM) Program to safeguard, secure, and strengthen cyberspace and the security posture of Federal networks in an environment where cyber attacks are continuously growing and evolving.

The CDM Architecture Principles document defines defect checks as "automated tests that compare an object's actual state (as derived from sensors) with the desired security state (as established by policy)."

This document discusses how agencies can define the desired state within the CDM program, leveraging three frameworks: that of the CDM architecture (ABCD diagram), the Cybersecurity Framework, and the security controls framework outlined by the National Institute of Standards and Technology (NIST).

Since the cybersecurity space is inherently complex, the CDM approach is to address the problem space in phases, as shown in Figure *1*:

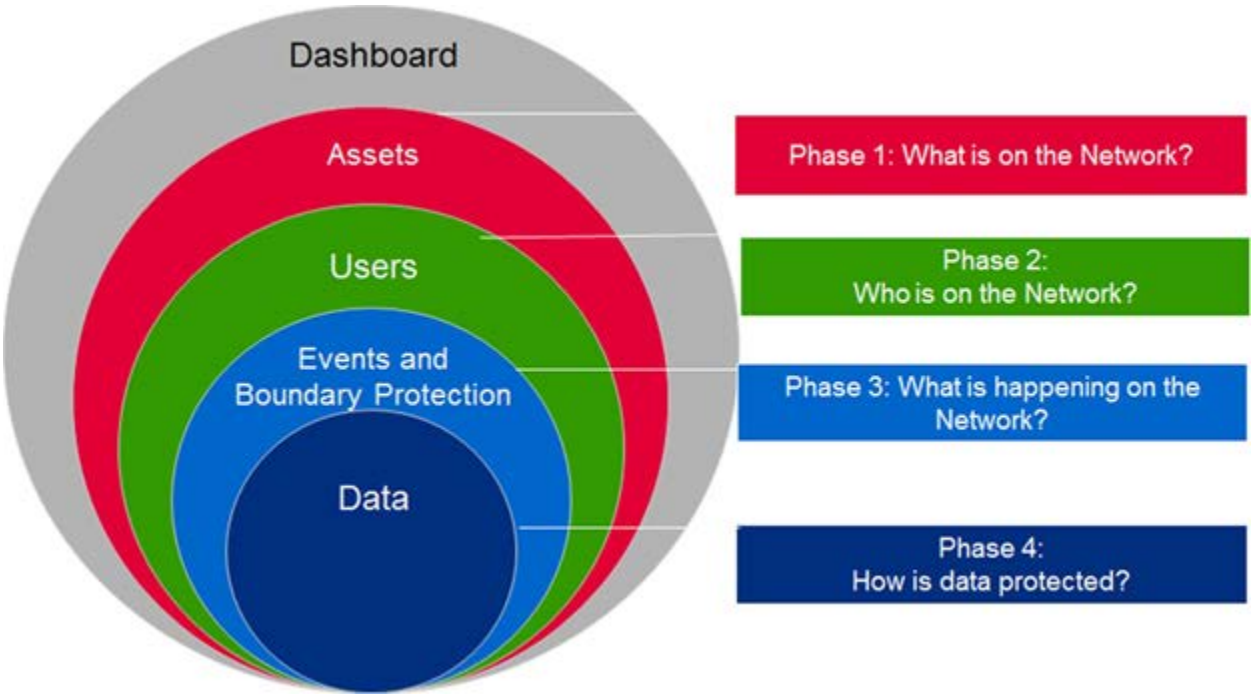


Figure 1-Phases of CDM

NOTE: While Phase 4 is recognized as part of the CDM overall program, this document will focus on Phases 1, 2 and 3, for which there are defined requirements. It is expected that there will be an update to this document as the Phase 4 requirements are defined.

The guiding principle of the CDM approach is to observe the "actual state" of the components that form the network, have a targeted "desired state" match to the Agency's abilities, and provide the mechanism to implement the improvement, usually through the removal of security

"defects," with accompanying performance metrics to demonstrate the "value" of the improvement—often risk reduction.

It is important to note that while the scope of this document is the portion of the CDM program that is deployed within Agency environments, limitations of funding and other considerations will determine the prioritization and scoping of the breadth and depth of solutions deployed.

From the viewpoint of requirements, the CDM solution is composed of two distinct elements. The first is the CDM Dashboard (both Federal and Agency specific); the second is the collection of elements that are not in the scope of the Dashboard. The latter are labeled the Continuous Monitoring as a Service (CMaaS) elements and are the basis for the requirements captured in the companion volume (Volume Two), "CDM Technical Capabilities – Requirements Catalog." The Dashboard follows its own requirements process in alignment with the use of the agile methodology.

This document addresses the security frameworks supported by CDM and presents the major approaches applied to the definition of security posture and how each identifies the desired state. The Agency-defined "desired state" can take on different values depending on the security framework selected. Under this approach, the following are addressed:

1. The CDM-centric solution architecture and related constructs
2. CDM and the NIST Cybersecurity Framework
3. CDM and NIST Risk Management Framework, focused on the relationship of the NIST Special Publication (SP) 800-53 controls
4. CDM as defined through the compendium of capability requirements known as "Attachment Ns"

Security Frameworks Supported by CDM

The ability of an Agency to identify and implement correct security safeguards depends on its processes and procedures to assess, manage, and improve its security posture. Different approaches are often used to implement, assess, and evaluate the current state of security posture against Agency security goals, and to provide measurable guidelines for selecting appropriate security improvements. The lens by which Agencies select the desired state provides different contextual boundaries against which a given object as may be represented through these security frameworks.

This section outlines how leveraging the CDM architecture (including CDM design concepts), the NIST Cybersecurity Framework, and the NIST Risk Management Framework (with emphasis on the NIST SP 800-53 controls) can provide a measurable CDM approach to assess and improve an Agency's information system security posture.

I - 1 CDM Architecture

This approach looks for conformance to the CDM architecture as a reference framework. The approach includes both the conceptual CDM architecture and the associated core design concepts.

I - 1.1 CDM ABCD Architecture

The CDM architecture uses a four-layer A-B-C-D design, as shown in Figure 2-ABCD Notional Architecture. Since the requirements for Phase 4 are in process, only Phases 1, 2, and 3 are shown.

- Layer A is the lowest and most diverse layer, containing tools and sensors that are deployed and interact with the low-level hardware and software components in an Agency's information system infrastructure. Almost by definition, Layer A is highly distributed and rarely centralized.
- Layer B serves as the contractor integration point specific to the Agency-provided solution. It is dual purposed, supporting the data integration and normalization function as well as orchestrating the operational control points for the CMaaS solution. The subsystems that form Layer B may be centralized but should be able to accommodate horizontal or vertical implementation either for scaling or geopolitical reasons. The general recommendation (at minimum) is that the instances of Layer B should align to the topology employed for Layer C.
- Layer C is the Agency Dashboard provided as government-furnished equipment by the CDM program to the contractor to customize as appropriate for the Agency environment. It is the Agency's exclusive (authoritative) connection to the Federal Dashboard and receives its Agency feeds from Level B. The inherent structure of the agency Dashboard supports a hierarchical implementation to accommodate horizontal or vertical implementation either for scaling or geopolitical reasons.
- Layer D provides dashboards and repositories at the Federal Enterprise level. The Federal level holds the Agency summary material and provides the standards and policies feed to the Agency Dashboards. As such, this area has no CMaaS contractor responsibilities and is being provided by a separate CDM Dashboard Task Order.

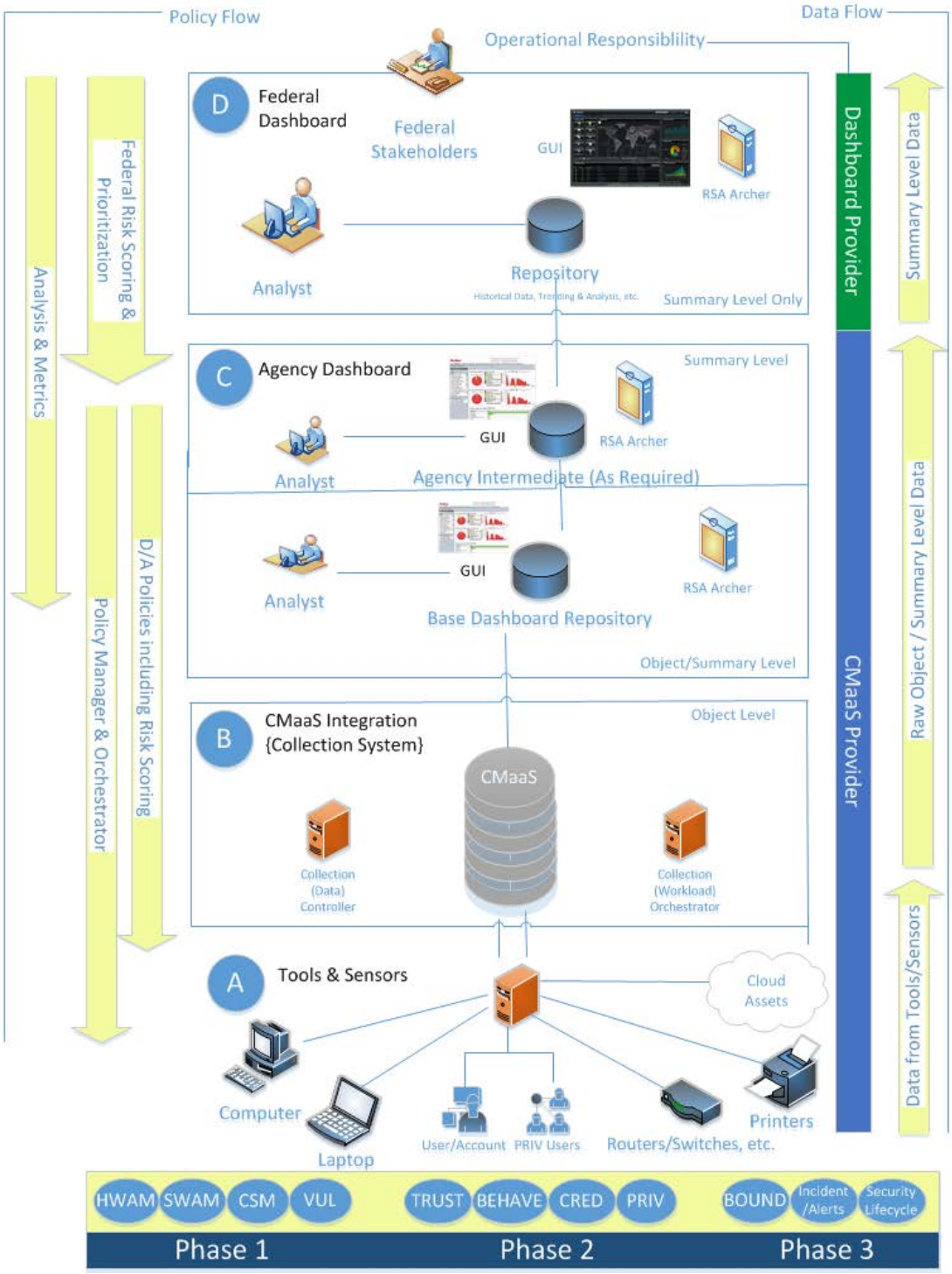


Figure 2-ABCD Notional Architecture (Phases 1 through 3)

To compute an Agency security risk, CDM monitors and collects hardware and software component actual state data values in Layer A. These values represent the actual state of an Agency's information system security posture. Layer B aggregates and correlates the actual state data values for evaluation against the desired state policy data, and through the Layer B

orchestration desired state parameters (such as Organizational Unit [OU] or Federal Information Security Modernization Act 2014 [FISMA] structures) can be passed to and executed by Layer A.

While data collection is an upward flow, CDM Federal and Agency desired state policies flow from Layer D and Layer C, respectively. These policies are used to establish the desired state of an Agency information security posture based on the threats facing the Agency.

The risk scores, security risk, and gaps between the desired and actual states are reported to the Federal and Agency Dashboards for further analysis and actions. To address a security risk or lower a risk score, additional Federal or Agency desired state policies may be sent to augment existing security controls to mitigate the security risk.

I - 1.2 CDM Requirements Core Design Concepts

The core design concepts in this section are applicable to implementing CDM requirements in terms of desired and actual state processing:

- CDM Actual State (section I - 1.2.1) represents the “as-is” state of an Agency’s current security posture.
- CDM Desired State (section I - 1.2.2) represents the “to-be” state for an Agency’s projected security posture.
- CDM Policy Decision Point Machine-Readable Policies (section I - 1.2.3) is the technique used to translate and maintain security policies that are used for ongoing assessment.
- CDM Containers and Objects (section I - 1.2.4) represent the categorization of security related data types and information to manage, control and maintain desired and actual state data values.

All the previously mentioned CDM design concepts must adhere to the following set of CDM architectural principles:

- *Data Interrogation Actions: The CDM system provides methods for users to interact with CDM data to support higher level security activities.*
- *Common Schema: The CDM system uses a common schema to ensure that all data made available for diagnostics in CDM is consistent across all participating agencies.*
- *Machine-Readable Policy: Federal and Agency policy is captured such that the CDM system can automatically compare that policy information to sensor information to determine defects.*
- *Risk Scores: The CDM system uses risk scores to prioritize defects.*
- *Result Data Types: The CDM system provides different result data types to support various reporting needs within the CDM architecture layers.*
- *Grouping Object Data: The CDM system provides the ability to group object data to provide context to results and support security and authorization decisions.*

I - 1.2.1 CDM Actual State

The CDM actual state is the discoverable, observable, and measurable state of the security attributes associated with the relevant containers and objects that are generated from sensor hardware and software components. The relevant security information to be measured for containers, objects, and attributes is determined based on the needs of the NIST SP 800-53 controls (or additional organizationally defined security controls) and other security oversight sources, such as FISMA, and others as may be identified by the Office of Management and Budget (OMB) Circulars such as A-130. The actual state includes the states and behaviors (reflected in attribute values) that may indicate the presence of a change in security posture that may introduce additional risk to the information system.

In relationship to the CDM architecture, CDM actual state values are collected and generated in Layers A and B, respectively.

I - 1.2.2 CDM Desired State

The CDM desired state defines data values that represent the targeted best status of an Agency security posture. These data values may be in the form of an attribute with a specific value, a list of acceptable values, or a rule specification that includes desired values of other attributes. Rules for desired state attribute values may include attributes from containers and/or other objects. These rules can be used to build simple to complex relationships between different desired status attributes.

In relationship to the CDM architecture, CDM desired state policies are pushed down from Layers C and D and are very closely related to the Policy Decision Point operations defined below.

“Desired State” is continuously evolving, as a mature information technology (IT) governance process at the Federal level will contribute to identifying and approving the desired state attributes to protect the Agency information system.

I - 1.2.3 CDM Policy Decision Point Machine-Readable Policies

The CDM Policy Decision Point (PDP) is a logical mechanism used to measure the actual state against the desired state criteria.

The CDM PDP provides assurance that each information system component is configured with the correct policy (i.e., the desired state). The CDM PDP compares desired state attribute values with actual state attribute values using the policy and rules associated with that desired state. A discrepancy between a desired state attribute value and an actual attribute value (also known as a defect) represents a change in security posture for the information system. The change in security posture may be acceptable if the change in information system risk is acceptable. At this point, a policy decision is made to accept or mitigate the defect.

The CDM PDP supports the continuous monitoring of policies and attributes, and identifies and reports on policy discrepancies for an information system. To ensure that the ongoing assessment is automated, policies should be implemented in a machine-readable format that can be loaded into the CDM PDP.

To be machine readable, the CDM desired state policies must be expressed in a format that can be read and processed by the CDM PDP. That is, CDM attributes should be defined as values

and lists that, when combined with rules, can be used to compute and measure the CDM ongoing assessment of the information systems to determine the ongoing authorization (see section I - 3.2) of the information system.

I - 1.2.4 CDM Containers and Objects

This section describes CDM containers and objects, graphically represented in the Figure 3, with the three key constructs being container, record, and requirement source.

The overall purpose of the CDM containers and objects is to store the results from the monitoring for state and behavior changes that impact the ongoing security risk level of information systems. This ongoing risk assessment and corresponding ongoing authorization will allow the determination whether information systems will be allowed to continue operations.

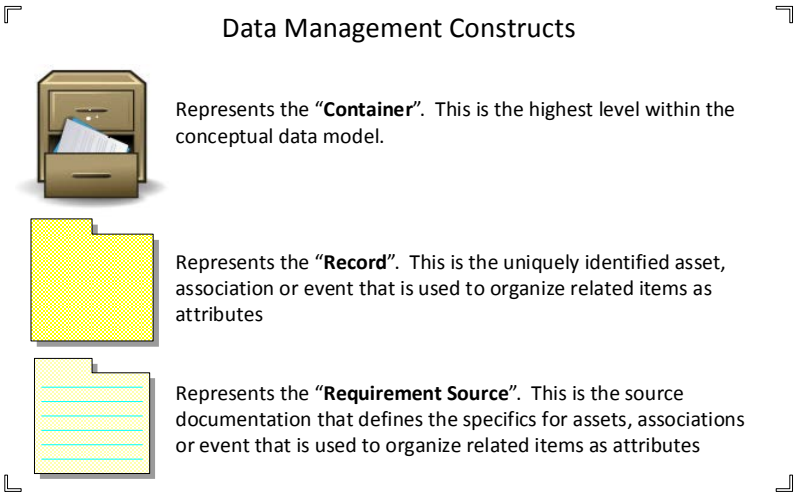


Figure 3-CDM Data Model Legend

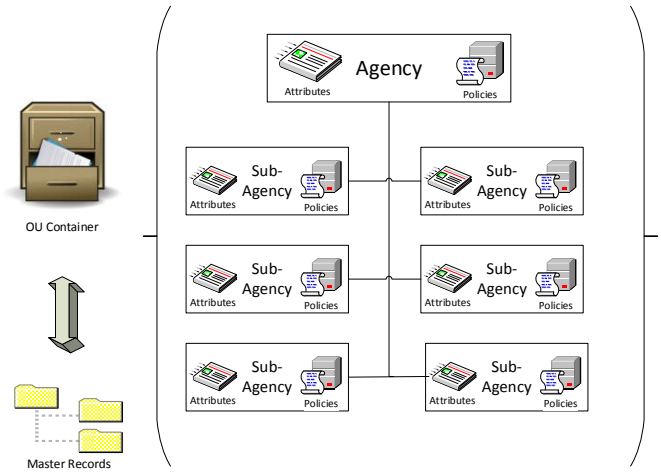
I - 1.2.4.1 Containers

CDM containers are the highest level of logical abstraction. CDM containers define the CDM policies and attributes for a given organization and system. There are two types of CDM containers: the OU Container (for example, under DHS, OUs might include components such as Immigration and Customs Enforcement, Customs and Border Protection, etc.) is used for organization-specific policies and attributes, while the FISMA Container is used for security policies and attributes that are required for compliance with FISMA.

The policies in a container specify values for attributes, relationships between object attributes (of potentially more than one object type), relationships between container attributes and object attributes, and/or a combination of these, for the CDM actual state and the CDM desired state. For example, the container may specify policies and attribute values for users of a device linked to the container.

I - 1.2.4.1.1 Organizational Unit Container

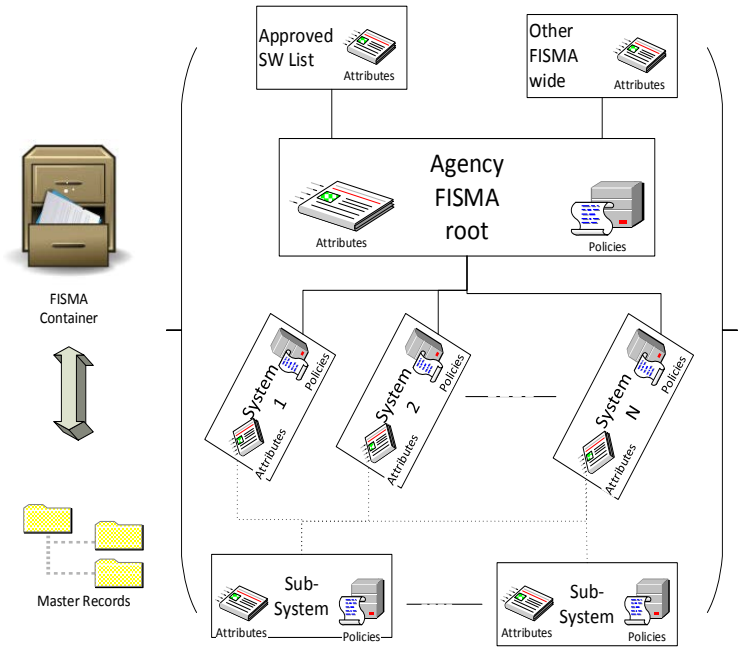
The OU Container is a set of policies and attributes that are applicable to information systems and users within the organization (e.g., an Agency). OU Containers represent the official organizational hierarchy. Attributes in the OU Container represent the organizational and functional roles (e.g., department heads, managers, etc.) and chain of command for the organization. The OU Container contains attributes for both the desired state and corresponding actual state for NIST SP 800-53 controls (or additional organizationally defined security controls) implemented at the organizational level, as well as other items required for reporting purposes.



The OU Container is composed of desired state policies and attribute values for attributes contained within various Master Records, which are compilations of attributes for the specified object (e.g., the Master User Record [MUR] for users and accounts, Master Device Record [MDR] for devices, Master System Record [MSR] for network interfaces, and/or Master Incident Record [MIR] for incidents and events) linked to the OU Container. These Master Records are described below.

I - 1.2.4.1.2 FISMA Container

The FISMA Container represents the authorization boundary for an information system, which defines the network, devices, and users that are part of the information system. The FISMA Container defines the security/mission assurance environment (e.g., data sensitivity, impact level, etc.) of the information system. Attributes in the FISMA Container represent the FISMA security roles (e.g., Risk Executive, Authorizing Official, Security Control Assessor, etc.), as well as security access roles (e.g., privileged and non-privileged users) for the information system. The FISMA Container contains attributes for both the desired state and corresponding actual state for NIST SP 800-53 controls (or additional organizationally defined security controls) implemented at the information system level, as well as other items required for reporting purposes.



The FISMA Container is composed of desired state policies and attribute values for attributes contained within the MUR, MDR, MSR, and/or MIR linked to the FISMA Container.

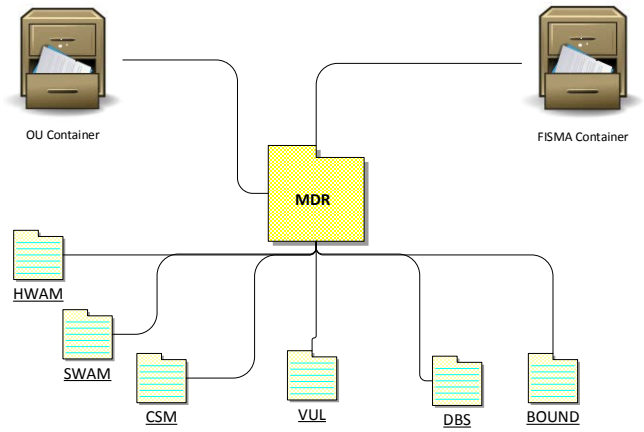
Controls implemented at the FISMA system level are linked to all systems and system components of the FISMA system associated with the FISMA Container. Further, the FISMA container can be used to hold enterprise control items such as the Approved Software List.

I - 1.2.4.2 Objects

Policies and attributes are derived and represented in CDM objects to capture instantiated actual attribute values during deployed runtime processing of information system components. CDM objects include the MDR, MUR, MSR, and MIR. These objects are associated with one or more OU Containers (based on the organizational hierarchy) and one or more FISMA Containers.

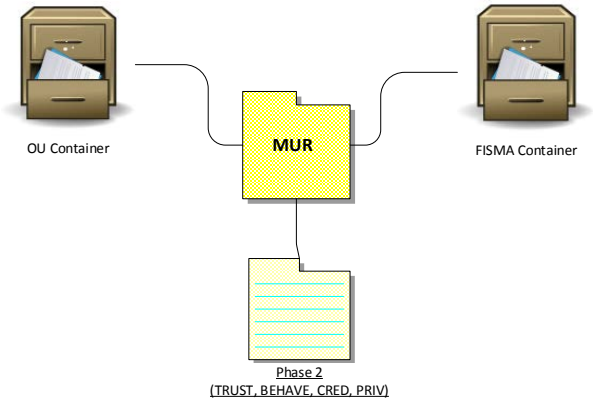
I - 1.2.4.2.1 Master Device Record

The MDR represents a physical or logical network device and deals with "What is on the network?" The MDR represents Internet Protocol addressable devices (e.g., router, switch, computers, mobile devices, etc.) and can include information about hardware, operating systems, installed applications, software services, connected devices (e.g., printers, universal serial bus [USB] devices, etc.), and hardware/software component configuration settings. The MDR contains attributes that need to be collected for comparison against a desired state for those attributes. The MDR desired state is based on desired state policies and attribute values associated with the organization (OU Container) and/or FISMA system (FISMA Container) to which the device belongs (i.e., is linked to). An MDR is linked to a single FISMA Container and may be linked to multiple OU Containers.



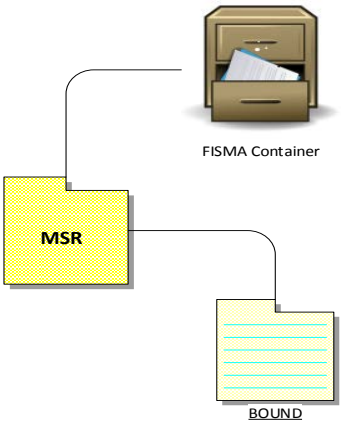
I - 1.2.4.2.2 Master User Record

The MUR represents an entity (person or non-person) that requests access to information, information systems, and facilities and deals with "Who is on the network?" The MUR includes information about credentials (i.e., elements of who) for identification, authorization (i.e., elements of trust) for access rights and permissions for granted access, accounts associated with information systems, and appropriate training for specific roles and responsibilities. The MUR contains attributes that need to be collected for comparison against a desired state for those attributes. The MUR desired state is based on desired state policies and attribute values associated with the organization (OU Container) and/or FISMA system (FISMA Container) linked to the item the entity is attempting to access. A MUR may be linked to multiple OU and FISMA Containers.



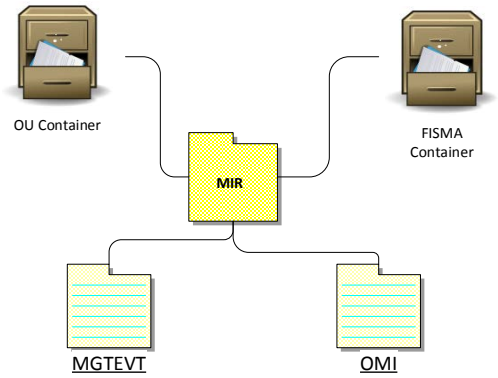
I - 1.2.4.2.3 Master System Record

The MSR represents the communication interface between information systems and deals with "How is the boundary protected?" The communication interface could be between information systems internal to the organization or with an information system external to the organization. The MSR contains attributes that need to be collected for comparison against a desired state for those attributes. The attributes are associated with one or more devices (MDRs) that mediate network traffic flow across the boundary (e.g., router, firewall, etc.) of the information system to implement the appropriate filtering policy. The MSR desired state is based on desired state policies and attribute values associated with the organization (OU Container) and/or FISMA system (FISMA Container) to which the information system belongs (i.e., is linked to). An MSR can be linked to multiple MDRs within the FISMA Container.



I - 1.2.4.2.4 Master Incident Record

The MIR represents activities associated with security controls that require an action when an event occurs and deals with "What is happening on the network?" The MIR includes information about the incident and the activities (e.g., Standard Operating Procedures, response/mitigation actions, reporting, etc.) associated with the incident. The MIR contains attributes that need to be collected for comparison against a desired state for those attributes. The MIR desired state is based on desired state policies and attribute values associated with the organization (OU Container) and/or FISMA system (FISMA Container) linked to the MSR, MDR, and/or MUR involved in the incident. An MIR may be linked to multiple OU and FISMA Containers, depending on the objects involved in the incident.



I - 1.2.4.3 Recap of Container/Objects

Figure 4 presents the container(s) and object(s) in a unified view of the entire conceptual data model.

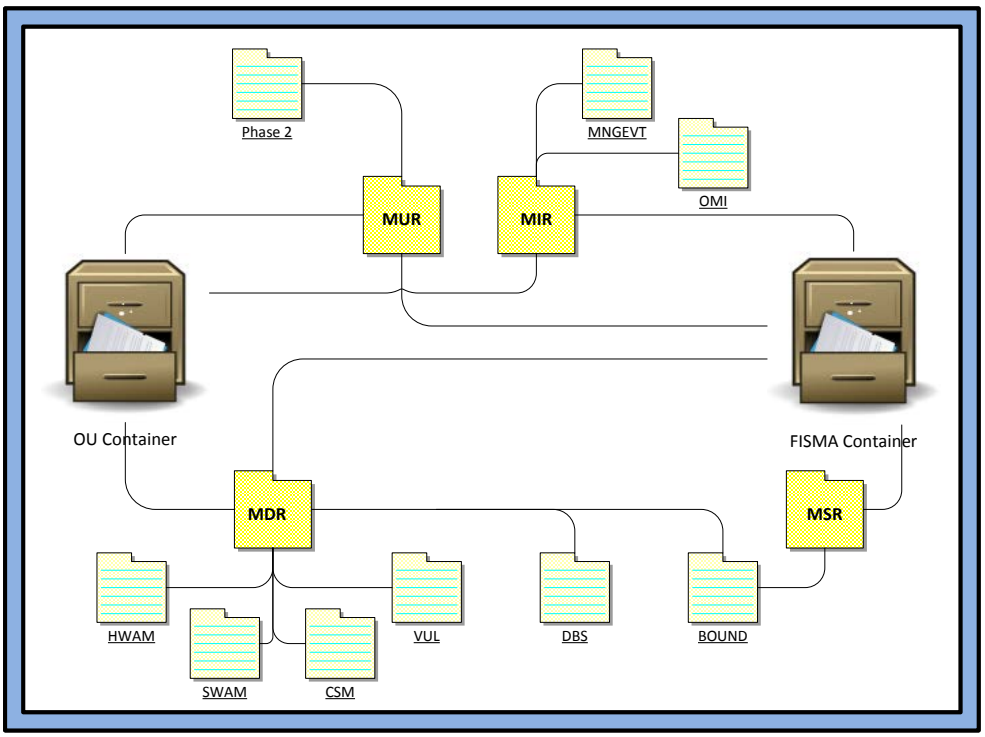


Figure 4-CDM Desired State Objects Relationship

I - 2 CDM and the Cybersecurity Framework Core

OMB Memorandum 16-03, "Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements," calls out the Federal adoption of the NIST Cybersecurity Framework (CSF) for improving critical infrastructure cybersecurity.

The ability of an Agency to identify and implement correct security controls depends on its processes and procedures to assess, manage, and improve its security posture. To support that effort, security models are often used to continuously assess and evaluate the actual state of an Agency security posture against its desired state, and to provide measurable guidelines for selecting appropriate security improvements.

The NIST CSF Core comprises four elements: Functions, Categories, Subcategories, and Informative References. Currently, there are five Functions, 23 Categories (with IDs), and 98 Subcategories. This document covers only the CSF Core Functions and Categories with the Category ID in the third column (see Table 1) and shows how CDM tools, sensors, dashboards, and policies support the outcomes. The complete list of Categories to Subcategories mapping, and Subcategories mapping to Informative References, can be found in the NIST document *Framework for Improving Critical Infrastructure Cybersecurity*.

While the CDM program provides tools that meet the CDM goals and objectives to strengthen cybersecurity posture by continuous mitigation and diagnostics of security settings, it is not funded to procure cyber tools per se, but rather to provide tools that help agencies ensure that the cyber tools they do possess are appropriately configured.

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
Protect	Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Table 1: Cybersecurity Framework Core Element mapping

CSF defines Functions and Categories as follows:

- *Functions organize basic cybersecurity activities at their highest level. These Functions are Identify, Protect, Detect, Respond, and Recover. They aid an organization in expressing its management of cybersecurity risk by organizing information, enabling risk management decisions, addressing threats, and improving by learning from previous activities. The Functions also align with existing methodologies for incident management and help show the impact of investments in cybersecurity. For example, investments in planning and exercises support timely response and recovery actions, resulting in reduced impact to the delivery of services.*
- *Categories are the subdivisions of a Function into groups of cybersecurity outcomes closely tied to programmatic needs and particular activities. Examples of Categories include "Asset Management," "Access Control," and "Detection Processes."*

Within the CDM program, the five CSF Functions are defined as follows:

Identify – What processes and assets need protection? Examples include identifying hardware assets, software assets, and vulnerabilities.

Protect – What safeguards are available? Examples include controls to protect and prevent compromise.

Detect – What techniques can identify incidents? Examples include monitoring to detect events and incidents related to vulnerabilities and weaknesses.

Respond – What techniques can contain impacts of incidents? Examples include identifying appropriate actions regarding detected cybersecurity events and incidents.

Recover – What techniques can restore capabilities? Examples include identifying plans for resiliency and to restore operational functions.

Descriptions of the 23 CSF Categories are shown in Section ***III - Appendix B: Cybersecurity Framework Categories.***

The set of tables in Figure 5 show the relationship of the Cybersecurity Framework categories to the CDM Phases.

Manage "What is on the Network?"	
IDENTIFY	Asset Management
	Governance
	Risk Assessment
PROTECT	Data Security
	Information Protection
	Maintenance
DETECT	Anomalies & Events
	Continuous Monitoring
RESPOND	
RECOVER	

Manage "Who is on the network?"	
IDENTIFY	Asset Management
	Governance
	Risk Assessment
PROTECT	Access Control
	Awareness & Training
	Data Security
DETECT	Anomalies & Events
	Continuous Monitoring
RESPOND	Communications
RECOVER	

Manage "What is happening on the network" through BOUND	
IDENTIFY	Asset Management
	Governance
	Risk Assessment
PROTECT	Access Control
	Data Security
	Infrastructure Protection
	Protection Technology
DETECT	Anomalies & Events
	Continuous Monitoring
	Detection Process
RESPOND	
RECOVER	

Manage "What is happening on the network" through DBS	
IDENTIFY	Business Environment
	Governance
	Risk Assessment
	Risk Management
PROTECT	Information Protection
DETECT	Anomalies & Events
	Continuous Monitoring
	Detection Process
RESPOND	Analysis
RECOVER	

Manage "What is happening on the network" through MGTEVT	
IDENTIFY	Asset Management
	Governance
	Business Environment
PROTECT	Infrastructure Protection
	Data Security
DETECT	Anomalies & Events
	Continuous Monitoring
	Detection Process
RESPOND	Analysis
RECOVER	

Manage "What is happening on the network" through OMI	
IDENTIFY	Governance
	Risk Assessment
	Risk Management
PROTECT	Information Protection
	Protection Technology
	Maintenance
DETECT	Anomalies & Events
	Continuous Monitoring
	Detection Process
RESPOND	Analysis
	Communications
	Improvement
	Mitigation
	Response Plan
RECOVER	Recovery Plan
	Improvement

Figure 5-CDM mapping to Cybersecurity Framework Core Functions and Categories

I - 3 CDM and NIST Risk Management Framework

The CDM desired state attribute values represent a security posture for an information system as delineated within NIST SP 800-37 (Risk Management Framework [RMF]). Two key representations of the RMF are of direct concern to CDM. The first is shown in the RMF Organization Tiers as shown in the Figure 6, and the second is the process steps for the RMF as shown in Figure 7.

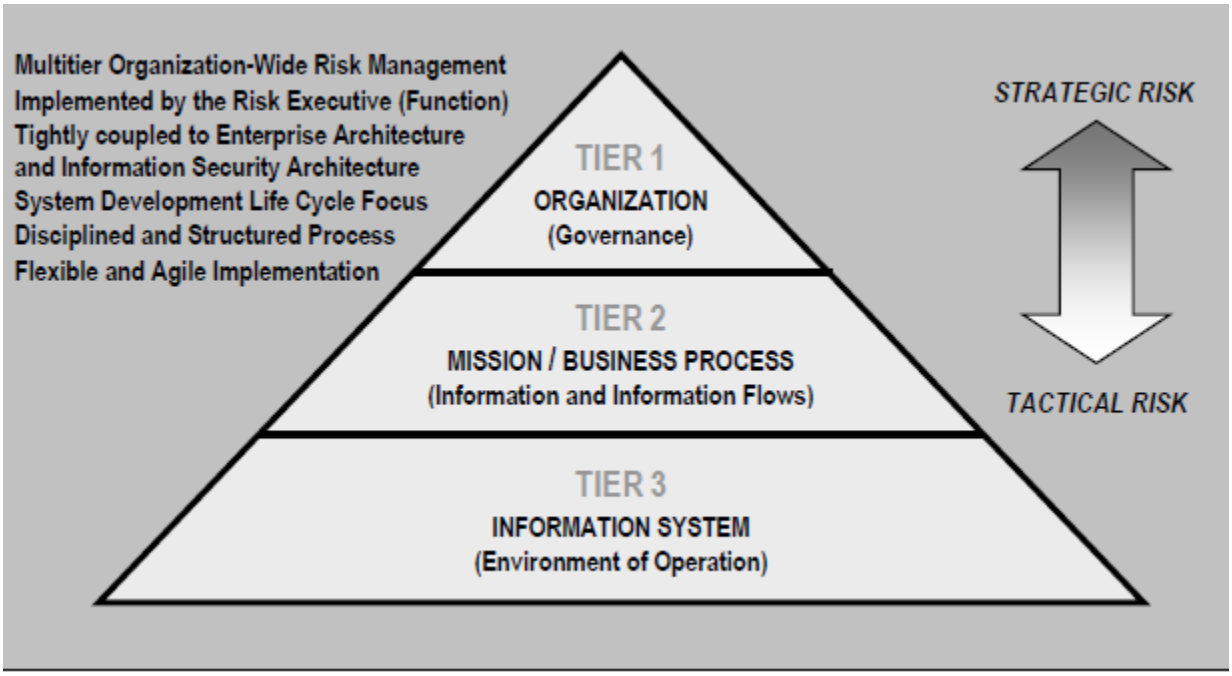


Figure 6-RMF OU Tiers

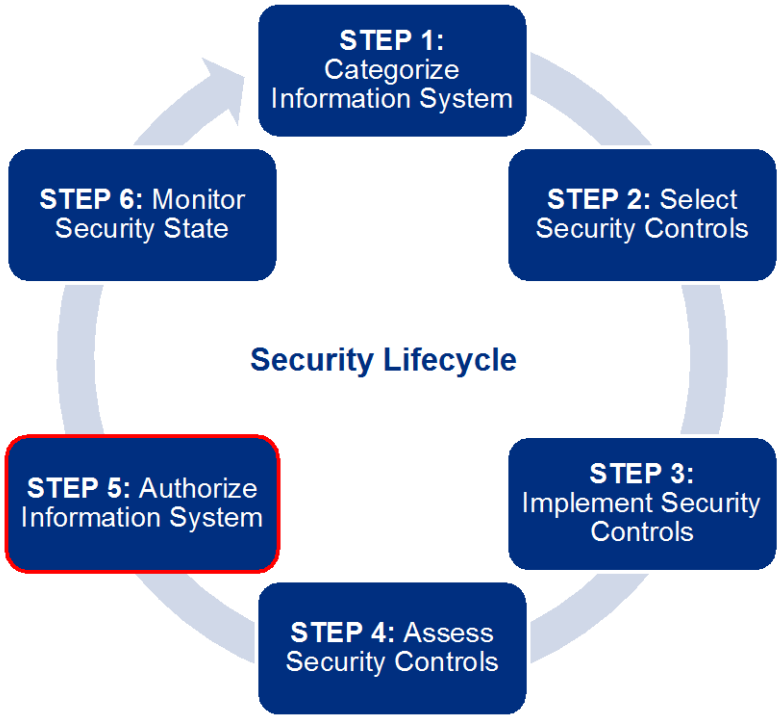


Figure 7-RMF Process Steps (Cyclical)

Thus, CDM actual state data attributes can be associated with the implementation of NIST SP 800-53 controls[1] for an information system, specifically as referenced in the RMF process cycle. Additional attributes may be organizationally defined based on other security standards and guidelines, especially in support of the RMF Organization and Mission/Business Process Tiers.

Under this topic, there are three distinct areas of discussion:

1. Role of CDM with Ongoing Assessment
2. Role of CDM with Ongoing Authorization
3. The role of specific NIST SP 800-53 controls to CDM

The relationship of these CDM areas to the overall RMF Process Steps is shown in the following table:

RMF Step	Definition	CDM Defined Activity
1	CATEGORIZE Information System	Establish each Agency information system within its own FISMA container to include its relationship to assets and policies within the CDM Agency Dashboard.

[1] While this document uses NIST SP 800-53 controls to describe CDM desired states, controls are not limited to NIST SP 800-53 but include any security control (safeguard or countermeasure) that can support CDM desired state measurement of the security posture of an information system.

2	SELECT Security Controls	For each FISMA system based on FIPS 199 rating and Agency policies, tailor NIST SP 800-53 controls and align to operationalized CDM capabilities.
3	IMPLEMENT Security Controls	Utilize CDM-provided capabilities for those controls for which the assessment of their effectiveness can be automated.
4	ASSESS Security Controls	Performed on an ongoing basis by leveraging the CDM integration system ability to aggregate and correlate actual state data against desired state specific to each affected NIST SP 800-53 control.
5	AUTHORIZE Information System	Provides standardized measurements and visibility into deviations that might change risk assessment and authorization determinations.
6	MONITOR Security Controls	Provides authorizing officials and other parties of interest with automated and ongoing situational awareness of system status through risk scoring.

I - 3.1 Ongoing Assessment and CDM

Agencies are expected to perform information and information system risk assessments to support the authorization of systems to operate. Based on the risk assessment process for Agency information and information systems and to be consistent with the RMF step 2, appropriate NIST SP 800-53 controls must be implemented (RMF Step 3) to prevent system compromise and protect sensitive information.

Based on the activities of a threat actor, security events could immediately indicate a compromise and/or failure of one or more NIST SP 800-53 controls. In other cases, such as Advanced Persistent Threat and Zero Day threats, additional assessment and investigation may be needed to determine the underlying cause of the event and appropriate countermeasure response. These events may indicate a state change for the implementation of a NIST SP 800-53 control on a system. Continuously monitoring events for these state changes enables ongoing assessment of NIST SP 800-53 controls (RMF Step 4). State changes related to these security controls may or may not increase system risk, and need to be passed to the ongoing authorization risk management process to determine changes in the risk level of the system, which is the interaction of ongoing assessment with ongoing authorization.

I - 3.2 Ongoing Authorization and CDM

The output of ongoing assessment identifies events that represent state changes in the implementation of NIST SP 800-53 controls (RMF Step 5). Ongoing authorization identifies events that represent potential increases in security risks as incidents. The primary policy that is associated with the requirement for agencies to perform Ongoing Authorization (and by

inference ongoing assessment) is OMB A-130, "Managing Information as a Strategic Resource," and its associated guidance.

Incidents may indicate an unacceptable state change for the implementation of a NIST SP 800-53 control on a system. Based on state changes related to these security controls and the responses to incidents, CDM performs the Ongoing Authorization risk management process to determine changes in the security risk level of the system and whether the security risk level remains acceptable to support continued authorization and operation.

Failure to respond to mismatches between the desired and actual state, respond and recover from a security incident, or use shared information to protect the system from known threats increases risk to the system and organization and could result in suspension of the authorization to operate by the authorizing official.

I - 3.3 Leveraging NIST SP 800-53 Controls

The standard practice for the documentation of an information system's security posture characteristics is used by following the process defined in NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, {Reference 10} which provides a significant amount of the practical context for working within the RMF as established in NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach.*" {Reference 13} This is specifically identified as Step 6 in the RMF Process Cycle.

The full details for all CDM desired state policies, attributes, and examples for the following 17 NIST SP 800-53 control families will be available as government-furnished information from the CDM Program Management Office:

- Security Controls in the Access Control (AC) family address the ability to allow authorized subjects to gain access to system resources and data, and to prevent all other accesses. Most of the AC controls are linked to attributes of the FISMA Container to express desired state for system access. Organization-level controls (e.g., AC-1) are associated with the OU Container, while specific controls related to users and permissions are related to attributes in the MUR. AC controls used to derive the CDM desired states are: AC-1, AC-2 (1) (2) (3) (4) (5) (11) (12) (13), AC-3, AC-4, AC-5, AC-6 (1) (2) (3) (5) (9) (10), AC-7, AC-8, AC-10, AC-11 (1), AC-12, AC-14, AC-17 (1) (2) (3) (4), AC-18 (1) (4) (5), AC-19 (5), AC-20 (1) (2), AC-21, AC-22.
- Security Controls in the Awareness and Training (AT) family address that system designers, administrators, operators, and users have the appropriate training to securely perform their roles. The controls ensure that users understand cybersecurity threats and concerns, and that they are cognizant of the threats the organization faces and their responsibilities in defending against them. Most of the AT controls are linked to the attributes of the OU Container to express desired state for training. Organization-level controls (e.g., AT-1) are associated with the OU Container, while specific controls related to the implementation of training users are related to attributes in the MUR. AT controls used to derive the CDM desired states are: AT-1, AT-2 (2), AT-3, AT-4.
- Security Controls in the Audit and Accountability (AU) family address the ability to record actions that occur in the system, to analyze those records, and to correctly attribute

each action to the entity that caused it to happen. Most of the AU controls are linked to attributes of the FISMA Container to express desired state for auditing. Organization-level controls (e.g., AU-1) are associated with the OU Container, while specific controls related to the implementation of auditing on system components are related to Configuration Settings Management (CSM) attributes in the MDR. AU controls used to derive the CDM desired states are: AU-1, AU-2 (3), AU-3 (1) (2), AU-4, AU-5 (1) (2), AU-6 (1) (3) (5) (6), AU-7 (1), AU-8 (1), AU-9 (2) (3) (4), AU-10, AU-11, AU-12 (1) (3).

- Security Controls in the Security Assessment and Authorization (CA) family address the steps involved in authorizing a system to operate under specific conditions in a specific environment with a defined and acceptable level of risk. Security Assessment is the process of determining what a system's characteristics and risk level are; Authorization is the process of granting (or denying) approval to operate under a defined set of conditions. Most of the CA controls are linked to attributes of the FISMA Container to express desired state for assessment and authorization. Organization-level controls (e.g., CA-1) are associated with the OU Container, while specific controls related to the personnel performing assessments and authorizations are related to attributes of the MUR. Controls addressing connections between systems are related to attributes in the MSR with a corresponding linkage to CSM attributes in the MDR. CA controls used to derive the CDM desired states are: CA-1, CA-2 (1) (2), CA-3 (5), CA-5, CA-6, CA-7 (1), CA-8, CA-9.
- Security Controls in the Configuration Management (CM) family address the steps involved in understanding and controlling the components of a system and how those components are configured. The goal is to ensure that all components of the system operate as expected, that there is no component that is unexamined or not understood, and that all changes have been carefully considered and their impacts are understood before they are made. Most of the CM controls are linked to attributes of the FISMA Container to express desired state for configuration management. Organization-level controls (e.g., CM-1) are associated with the OU Container, while specific controls related to the personnel performing configuration management functions are related to attributes of the MUR. The specific implementation of system configurations is related to CSM attributes of the MDR. CM controls used to derive the CDM desired states are: CM-1, CM-2 (1) (2) (3) (7), CM-3 (1) (2), CM-4 (1), CM-5 (1) (2) (3), CM-6 (1) (2), CM-7 (1) (2) (5), CM-8 (1) (2) (3) (4) (5), CM-9, CM-10, CM-11.
- Security Controls in the Contingency Planning (CP) family address whether the system can operate and carry out its mission despite any defined set of events that may occur. Those events may be natural disasters (e.g., hurricanes, floods), unintentional (e.g., a power failure) or intentional (e.g., an attack by an adversary). The controls ensure that the organization has considered events that may occur; believes that it understands how likely each event is and what its impact may be; and can respond should the event occur. Most of the CP controls are linked to attributes of the FISMA Container to express desired state for contingency planning. Organization-level controls (e.g., CP-1) are associated with the OU Container, while specific controls related to personnel performing contingency planning functions are related to attributes of the MUR. The specific implementation of controls related to backup operations on system components is related

to CSM attributes of the MDR. CP controls used to derive the CDM desired states are: CP-1, CP-2 (1) (2) (3) (4) (5) (8), CP-3 (1), CP-4 (1) (2), CP-6 (1) (2) (3), CP-7 (1) (2) (3) (4), CP-8 (1) (2) (3) (4), CP-9 (1) (2) (3) (5), CP-10 (2) (4).

- Security Controls in the Identification and Authentication (IA) family address knowing who or what each entity in the system is and on whose behalf it is operating. Identification means being able to associate a unique name with each entity—individual user, group of users, device, program, network component—in the system. Authentication means providing proof that the user of an identifier is authorized to use that identifier (e.g., that this user is the correct human user). Most of the IA controls are linked to attributes of the FISMA Container to express desired state for identification and authentication. Organization-level controls (e.g., IA-1) are associated with the OU Container, while specific controls related to personnel performing identification and authentication management are related to attributes of the MUR. The specific implementation of controls related to authentication of users is related to CSM attributes of the MDR. IA controls used to derive the CDM desired states are: IA-1, IA-2 (1) (2) (3) (4) (8) (9) (11) (12), IA-3, IA-4, IA-5 (1) (2) (3) (11), IA-6, IA-7, IA-8 (1) (2) (3) (4).
- Security Controls in the Incident Response (IR) family address how the organization will respond to a security incident that occurs during operation. Security incidents include attempted or successful attacks; failures of security-related system components; and suspected or actual misbehavior by system users. Most of the IR controls are linked to attributes of the FISMA Container to express desired state for incident response. Organization-level controls (e.g., IR-1) are associated with the OU Container, while specific controls related to personnel performing incident response functions are related to attributes of the MUR. Specific activities related to incident response actions are related to attributes of the MIR. IR controls used to derive the CDM desired states are: IR-1, IR-2 (1) (2), IR-3 (2), IR-4 (1) (4), IR-5 (1), IR-6 (1), IR-7 (1), IR-8.
- Security Controls in the Maintenance (MA) family address events that occur in ensuring that the system is operating correctly, is updated when needed, and can be repaired with minimal security impact when a problem does occur. Most of the MA controls are linked to attributes of the FISMA Container to express desired state for maintenance. Organization-level controls (e.g., MA-1) are associated with the OU Container, while specific controls related to personnel associated with maintenance processes are related to attributes of the MUR. MA controls used to derive the CDM desired states are: MA-1, MA-2 (2), MA-3 (1) (2) (3), MA-4 (2) (3), MA-5 (1), MA-6.
- Security Controls in the Media Protection (MP) family address the creation, management, distribution, storage, and disposal of electromagnetic or optical storage media. Media can include DVDs, CDs, USB drives, hard drives, etc. Security controls in this family cover physical and logical access to media; proper electronic and physical marking of media; and use, storage, transport, and disposal of media. Most of the MP controls are linked to attributes of the FISMA Container to express desired state for media protection. Organization-level controls (e.g., MP-1) are associated with the OU Container, while specific controls related to personnel associated with media protection processes are related to attributes of the MUR. The specific implementation of controls related to media protection on system components is related to CSM attributes of the MDR. MP controls

used to derive the CDM desired states are: MP-1, MP-2, MP-3, MP-4, MP-5 (4), MP-6 (1) (2) (3), MP-7 (1).

- Security Controls in the Physical and Environmental Protection (PE) family address controlling the spaces in which system components operate to ensure that components cannot be accessed, modified, replaced, stolen, or removed in a manner that would violate security policy.

  Security controls in this family also address system damage that could be caused by fire, water, electrical failure, or other related issue.

  Most of the PE controls are linked to attributes of the FISMA Container to express desired state for physical and environmental protection. Organization-level controls (e.g., PE-1) are associated with the OU Container, while specific controls related to personnel associated with physical and environmental protection processes are related to attributes of the MUR. Where the specific implementation of controls for physical access protections use a Physical Access Control System (PACS) on the network, those controls are related to CSM attributes of the MDR for the PACS. The specific implementation of environmental protection controls on system components is related to CSM attributes of the MDR. PE controls used to derive the CDM desired states are: PE-1, PE-2, PE-3 (1), PE-4, PE-5, PE-6 (1) (4), PE-8 (1), PE-9, PE-10, PE-11 (1), PE-12, PE-13 (1) (2) (3), PE-14, PE-15 (1), PE-16, PE-17, PE-18.

- Security Controls in the Planning (PL) family address the organization's security plans. Factors include how the plan is developed; contents of the plan; and the plan's impact on security, privacy, and organizational operations. Most of the PL controls are linked to attributes of the FISMA Container to express desired state for planning. Organization-level controls (e.g., PL-1) are associated with the OU Container, while specific controls related to information system users and personnel associated with planning processes are related to attributes of the MUR. PL controls used to derive the CDM desired states are: PL-1, PL-2 (3), PL-4 (1), PL-8.

- Security Controls in the Personnel Security (PS) family address vetting of the authorized organizational users of the system and system components. The goal is to ensure that all people with access to the system have earned the level of trust required of them to access the system and use information system data in a way that conforms to policy. Most of the PS controls are linked to attributes of the OU Container to express desired state for personnel security. Specific controls related to users and personnel associated with personnel security processes are related to attributes of the MUR. PS controls used to derive the CDM desired states are: PS-1, PS-2, PS-3, PS-4 (2), PS-5, PS-6, PS-7, PS-8.

- Security Controls in the Risk Assessment (RA) family address that the development, deployment, and operation of the system is controlled by and is compatible with the organization's overall risk assessment process. That is, the risk incurred by developing, deploying, and operating the system is understood and accepted by the organization. The RA controls are split between links to attributes of the FISMA Container and the OU Container. Specific controls related to personnel associated with risk assessment processes are related to attributes of the MUR. RA controls used to derive the CDM desired states are: RA-1, RA-2, RA-3, RA-5 (1) (2) (4) (5).

- Security Controls in the System and Services Acquisition (SA) family address how the organization acquires and operates the system. The control family covers the entire system life cycle, from initial design to ultimate decommissioning. The controls ensure that proper security engineering principles and practices are used in all phases of the life cycle.

  This control family includes how the organization selects and uses contractors and partners where needed to provide/support an information system.

  Most of the SA controls are linked to attributes of the OU Container to express desired state for system and services acquisition and Supply Chain Risk Management (SCRM). Where the implementation of specific development and acquisition controls is defined for individual information systems, those controls are linked to the FISMA Container. Controls incorporating SCRM activities are related to attributes in the MDR. Specific controls related to personnel associated with system and services acquisition processes are related to attributes of the MUR. SA controls used to derive the CDM desired states are: SA-1, SA-2, SA-3, SA-4 (1) (2) (9) (10), SA-5, SA-8, SA-9 (2), SA-10, SA-11, SA-12, SA-15, SA-16, SA-17.

- Security Controls in the System and Communications Protection (SC) family address how the system is designed and operated to detect and defeat attempted attacks. Controls include architectural principles such as partitioning; the use and protection of boundaries; the use of cryptography (including Public Key Infrastructure); and providing defenses against denial-of-service attacks. Most of the SC controls are linked to attributes of the FISMA Container to express desired state for physical and environmental protection. Organization-level controls (e.g., SC-1) are associated with the OU Container. The specific implementation of controls related to external connections/communications is related to attributes of the MSR. The specific implementation of controls related to system and communications protections internal to the information system is related to CSM attributes of the MDR. SC controls used to derive the CDM desired states are: SC-1, SC-2, SC-3, SC-4, SC-5, SC-7 (3) (4) (5) (7) (8) (18) (21), SC-8 (1), SC-10, SC-12 (1), SC-13, SC-15, SC-17, SC-18, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-28, SC-39.

- Security Controls in the System and Information Integrity (SI) family address protecting the system from attacks using malicious code; monitoring system behavior to detect flaws or attacks; and acting to remediate the situation when a flaw or attack is detected. Most of the SI controls are linked to attributes of the FISMA Container to express desired state for system and information integrity. Organization-level controls (e.g., SI-1) are associated with the OU Container, while specific controls related to personnel associated with information system monitoring processes are related to attributes of the MUR. The specific implementation of controls related system and information integrity and monitoring is related to CSM attributes of the MDR. SI controls used to derive the CDM desired states are: SI-1, SI-2 (1) (2), SI-3 (1) (2), SI-4 (2) (4) (5), SI-5 (1), SI-6, SI-7 (1) (2) (5) (7) (14), SI-8 (1) (2), SI-10, SI-11, SI-12, SI-16.

I - 4 Defining CDM from Attachment N Requirement's Documents

Historically, the definition of what was CDM content was established through discussion of its capabilities. This section provides an overview of how the original Attachment N documents and corresponding tool functional areas (TFAs) for each CDM phase map to the Phased Detailed Requirements (Table *2*) as described below. The material following this table presents a synopsis of each of the Attachment N documents.

DHS CDM Phase Attachments	Phased Detailed Requirements	CDM/CMaaS Blanket Purchase Agreement (BPA) TFAs
Phase 1 Attachment N Requirements	Manage "What is on the network?"	• TFA 1 – Hardware Asset Management • TFA 2 – Software Asset Management • TFA 3 – Configuration Settings Management • TFA 4 – Vulnerability Management
Phase 2 Attachment N-2 Requirements	Manage "Who is on the network?"	• TFA 6 – Manage Trust in People Granted Access • TFA 7 – Manage Security-Related Behavior • TFA 8 – Manage Credential and Authentication • TFA 9 – Manage Account/Access/Manage Privileges
Phase 3 Attachment N-BOUND Requirements	Manage "How is the network protected?"	• TFA 5 – Manage Network Access Controls
Phase 3 Attachment N-3-Manage Events (MNGEVT) Requirements	Manage "What is happening on the network?" for MNGEVT	• TFA 10 – Prepare for Contingencies and Incidents • TFA 11 – Respond to Contingencies and Incidents • Ongoing Assessment
Phase 3 Attachment N-3-Design and Build in Security (DBS) Requirements	Manage "What is happening on the network?" for DBS	• TFA 12 – Design and Build in Requirements Policy and Planning • TFA 13 – Design and Build in Quality • Supply Chain Risk Management
Phase 3 Attachment N-3-Operate, Monitor, and Improve (OMI) Requirements	Manage "What is happening on the network?" for OMI	• TFA 14 – Manage Audit Information • TFA 15 – Manage Operation Security • Ongoing Authorization

Table 2: CDM Phased Attachment-N Requirements and Associated CDM BPA Capabilities

Phase 1 - Manage "What is on the network?"

This phase is based on Phase 1 Attachment-N requirements.

Manage hardware and software baseline system inventory is based on the CDM Hardware Asset Management (HWAM) and Software Asset Management (SWAM) capabilities, which require the collection of device hardware and software components to establish the Agency's information system infrastructure computing environment. These CDM HWAM and SWAM

capabilities cover verification and validation for the existence of hardware infrastructure devices, and the accurate identification of approved software components.

Hardware and software configurations are based on CSM requirements to ensure that hardware and software (specifically the operating system and installed applications) assets are securely configured and hardened.

Vulnerability Management (VUL) requirements extend the focus of SWAM to achieve a level of confidence that software is free from vulnerabilities. This CDM capability covers verification and validation that hardware devices have the correct security configuration settings, and the system platform is hardened to reduce the platform attack surface.

Phase 2 – Manage "Who is on the network?"

Manage users/accounts is based on Phase 2 Attachment-N2 management and control of account/access/managed privileges (PRIV), trust in people granted access (TRUST), credentials and authentication (CRED), and security-related behavior (BEHAVE) requirements that require the management and control of users as an asset to ensure that the right individual has appropriate access to the right resource. This supports "Who is on the network?"

This CDM capability covers the verification and validation of appropriate user privileges, assigned credentials, trustworthiness, appropriate user security behavior training, and appropriately granted resource access rights to users.

Phase 3 – Manage "How is the network protected?"

Network defense and infrastructure abnormal behavior is based on Phase 3 Attachment N-BOUND to defend network boundaries and identify abnormal behavior (of networks and users) that may indicate that a security incident has occurred. This supports "How is the network protected?"

This CDM capability covers verification and validation of logical and physical network interfaces to reduce intrusive, malicious, and disruptive attacks; cryptographic mechanisms ensure confidentiality and integrity of data on the network; and methods to identify security incidents.

Phase 3 – Manage "What is happening on the network?" for MNGEVT

Integrity of process and resultant materials is based on the Phase 3 Attachment-N-3-MNGEVT and Attachment-N-3-OMI requirements to prepare for security incidents/events (through processes, policies, and procedures), gather appropriate audit/log data from appropriate sources, and identify security events/incidents (network and user abnormal behavior) through the analysis of audit/log data. This supports "What is happening on the network?"

In addition, ongoing assessment is the continuous process of comparing security-related container and object attributes between the actual state and the desired state. This comparison is performed by the CDM PDP. The discrepancy between actual state and desired state reflects the level of effectiveness of control implementations and the overall security posture of the system. The results of the ongoing assessment are used to evaluate the changes in risk posture associated with the discrepancy. Ideally, the ongoing assessment process is fully automated, with the desired state being encoded in the CDM PDP and the actual state being collected using CDM sensors. This supports ongoing assessment.

This CDM capability covers verification and validation of processes, policies, and procedures supporting cybersecurity preparation, audit and log data collection, security analysis of audit/log data, and incident reporting to provide forensic evidence of malicious or suspicious behavior.

Phase 3 – Manage "What is happening on the network?" for DBS

Software assurance based on Phase 3 Attachment-N-3-DBS requirements ensures the level of confidence that the software is free from defects, either intentionally designed into the software or accidentally inserted at any time during its life cycle, and that the software functions in the intended manner. This supports the software element of "What is happening on the network?"

The U.S. government and critical infrastructure sectors are increasingly dependent on commercial products and systems, which present significant benefits including low cost, interoperability, rapid innovation, a variety of product features, and choice among competing vendors. However, with some of these benefits there is an increase in the risk of a threat event that can directly or indirectly affect the supply chain, which often goes undetected and may result in risks to the acquirer. Therefore, SCRM seeks to enable the provisioning of the least vulnerable solutions to agencies through a robust assessment of supply chain risks, communication about those risks to the agencies, and appropriate response and monitoring of those risks throughout the entire system life cycle.

This CDM capability covers verification and validation of preventing and detecting software vulnerabilities to measure software assurance for built and acquired software components.

Phase 3 – Manage "What is happening on the network?" for OMI

Responding to and recovering from cyber incidents is based on Phase 3 Attachment-N-3-OMI requirements for incident prioritization and response, and post-incident activities (e.g., information sharing). This supports "What is happening on the network?"

Ongoing Authorization is the continuous evaluation of the change in risk level related to changes in security policies concerning object attributes (i.e., actual state and desired state) for threat behaviors that impact the security posture. This impact to security is measured by capturing changes in existing security safeguards (e.g., NIST SP 800-53 controls and countermeasures) and identifying new component weaknesses and vulnerabilities.

MNGEVT supports the runtime collection of attributes (actual state) and continuous monitoring of the policies related to attributes for ongoing assessment (actual state vs. desired state) to enhance current or apply new security controls and countermeasures. The results of the ongoing assessment will be used as inputs to the OMI Ongoing Authorization risk assessment process to determine if the level of risk remains acceptable for a given information system to support continued authorization and operation.

This CDM capability covers verification and validation of processes/procedures to prioritize incidents and associated response actions, quickly mitigate the impact of an incident, take appropriate remediation actions to eliminate the impact (restore normal operations) of the incident, and support information sharing and collaboration (both internal and external) to minimize or prevent the impact of future incidents.

I - 5 Conclusion

This document defines the multiple frameworks that have been applied to CDM solutions and establishes the different points of view that need to be represented in any discussion of the definition of the "best" security posture for "desired state."

The details of the requirements that are part of the CDM solution definition are provided in the companion volume (Volume Two), "CDM Technical Capabilities – Requirements Catalog."

References

1. Continuous Diagnostics and Mitigation (CDM) System Architecture: Architecture Principles Document, Version 0.5, August 31, 2016
2. Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, February 12, 2014
3. Phase 1: Attachment N Requirements, Section 9
4. Phase 2: Attachment N-2 Requirements, February 12, 2015
5. Phase 3: Attachment N-3-BOUND Requirements, 2nd Issue November 15, 2016
6. Phase 3: Attachment N-3-Manage Events Requirements, June 7, 2016
7. Phase 3: Attachment N-3-Operate, Monitor and Improve, August 5, 2016
8. Phase 3: Attachment N-3-Design and Build in Security, September 16, 2016
9. Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (draft), January 10, 2017
10. NIST SP 800-53, https://nvd.nist.gov/800-53/Rev4/
11. Security Requirements for Cryptographic Modules, FIPS 140-2, May 25, 2001, http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf
12. Standards for Security Categorization of Federal Information and Information Systems, FIPS 199, February 2004, http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf
13. NIST SP 800-37R1, Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf
14. Common Platform Enumeration (CPE) https://nvd.nist.gov/products/cpe
15. Common Configuration Enumeration (CCE) https://nvd.nist.gov/config/cce/index
16. Common Vulnerability Enumeration (CVE) https://nvd.nist.gov/vuln/search
17. NISTIR 7502 The Common Configuration Scoring System (CCSS): Metrics for Software Security Configuration Vulnerabilities, December 2010, http://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7502.pdf
18. National Vulnerability Database (NVD) https://nvd.nist.gov/
19. Common Vulnerability Scoring System CVSS https://nvd.nist.gov/vuln-metrics/cvss
20. Federated Identity, Credential, and Access Management (FICAM) https://www.idmanagement.gov/IDM/s/article_content_old?tag=a0Gt0000000XNYG
21. Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks (X.509 ITU-T) http://www.itu.int/rec/T-REC-X.509/en
22. Personal Identity Verification (PIV) of Federal Employees and Contractors, FIPS 201-2, August 2013, http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf
23. Common Weakness Enumeration (CWE) https://nvd.nist.gov/vuln/categories
24. US-CERT Federal Incident Notification Guidelines
25. HPE Security ArcSight Common Event Format, version 23, May 16, 2016
26. Guide to the Software Engineering Body of Knowledge, version 3.0, 2014

27. Security Content Automation Protocol (SCAP) https://scap.nist.gov/

III - Appendix A: Acronyms, Terms and Definitions

Acronym	Term	Definition
	Attributes	A set of labels, values, and hierarchies that describe a characteristic or dimension of a CDM object.
	Attribute Values	A list of possible value assignments or types for an attribute.
	BOUND	BOUND provides boundary protection for the interior of the network from all interconnections to other external networks.
	Data Element	A piece of information about CDM objects, their attributes, and/or associated policy to support the identification of defects.
	CDM Dashboard	The tool that aggregates and displays CDM information at the Agency or Federal level. The dashboard provides consistent, timely, targeted, and prioritized information to security decision makers from cross-agency and Federal-level managers to systems administrators to identify and support fixing the worst problems first.
AC	Access Control	This family of controls addresses the ability to allow authorized subjects to gain access to system resources and data, and to prevent all other accesses.
AT	Awareness and Training	This family of controls addresses that system designers, administrators, operators, and users have the appropriate awareness and training to securely perform their roles.
AU	Audit and Accountability	This family of controls addresses the ability to record actions that occur in the system, to analyze those records, and to correctly attribute each action to the entity that caused it to happen.
BEHAVE	Manage Security-Related Behavior	The BEHAVE capability ensures that authorized users with or without special security responsibilities exhibit the appropriate behavior for their role.

Acronym	Term	Definition
CA	Security Assessment and Authorization	This family of controls addresses the steps involved in authorizing a system to operate under specific conditions in a specific environment with a defined and acceptable level of risk.
CDM	Continuous Diagnostics and Mitigation	Provides Federal Departments and Agencies with capabilities and tools that identify cybersecurity risks on an ongoing basis, prioritize these risks based upon potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first. Congress established the CDM program to provide adequate, risk-based, and cost-effective cybersecurity and allocate cybersecurity resources more efficiently.
CM	Configuration Management	This family of controls addresses the steps involved in understanding and controlling the components of a system and how those components are configured.
CMaaS	Continuous Monitoring as a Service	The collection of elements that are not in the scope of the Dashboard.
CP	Contingency Planning	This family of controls addresses whether the system can operate and carry out its mission despite any defined set of events that may occur.
CRED	Credentials and Authentication Management	The CRED capability ensures that only proper credentials are authenticated to systems, services, and facilities.
CSF	Cybersecurity Framework	OMB Memorandum 16-03, “Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements,” calls out the federal adoption of the NIST Cybersecurity Framework (CSF) for improving critical infrastructure cybersecurity.
CSM	Configuration Settings Management	CSM ensures that authorized security configuration benchmarks exist and contain acceptable value(s) for each relevant configurable setting for each IT asset type.
CVE	Common Vulnerability Enumeration	A dictionary of common names (i.e., CVE Identifiers) for publicly known cybersecurity vulnerabilities.

Acronym	Term	Definition
CVSS	Common Vulnerability Scoring System	CVSS provides an open framework for communicating the characteristics and impacts of IT vulnerabilities.
CWE	Common Weakness Enumeration	The CWE Specification provides a common language for discussing, finding, and dealing with the causes of software security vulnerabilities found in code, design, or system architecture.
DBS	Design and Build in Security	Describes preventing exploitable vulnerabilities from being effective in the software/system while in development or deployment.
DHS	Department of Homeland Security	Federal Agency whose missions include preventing terrorism and enhancing security; managing our borders; administering immigration laws; securing cyberspace; and ensuring disaster resilience.
FISMA	Federal Information Security Modernization Act 2014	The U.S. legislation that defines a comprehensive framework to protect Government information, operations and assets against natural or man-made threats. FISMA was signed into law part of the Electronic Government Act of 2002. [2014 Act changed Management to Modernization.]
HWAM	Hardware Asset Management	The HWAM Function is to discover unauthorized or unmanaged hardware on a network.
IA	Identification and Authentication	This family of controls addresses knowing who or what each entity in the system is and on whose behalf, it is operating.
IR	Incident Response	This family of controls addresses how the organization will respond to a security incident that occurs during operation.
IT	Information Technology	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency.

Acronym	Term	Definition
MA	Maintenance	This family of controls addresses events that occur in ensuring that the system is operating correctly, is updated when needed, and can be repaired with minimal security impact when a problem does occur.
MDR	Mater Device Record	A set of attributes or assertions about a user, with the device as the primary key.
MIR	Master Incident Record	Represents activities associated with security controls that require an action when an event occurs; deals with “what is happening on the network?”
MNGEVT	Manage Events	Describes preparing for events/incidents, gathering appropriate data from appropriate sources, and identifying incidents through analysis of data.
MP	Media Protection	This family of controls addresses the creation, management, distribution, storage, and disposal of electromagnetic or optical storage media.
MSR	Master System Record	A set of attributes or assertions about a user, with the system as the primary key.
MUR	Master User Record	A set of attributes or assertions about a user, with the user as the primary key.
NIST	National Institute of Standards and Technology	The Federal technology Agency that works with industry to develop and apply technology, measurements, and standards.
OMB	Office of Management and Budget	OMB is the business division of the Executive Office of the President of the United States that administers the United States federal budget and oversees the performance of federal agencies.
OMI	Operate, Monitor and Improve	Describes audit data collection and analysis, incident prioritization and response, and post-incident activities (e.g., information sharing).
OU	Organizational Unit	The Government Department or Agency responsible for the information system.

Acronym	Term	Definition
PACS	Physical Access Control System	An automated system that manages the passage of people or assets through an opening(s) in a secure perimeter(s) based on a set of authorization rules.
PDP	Policy Decision Point	Repository for policies that are distributed to enforcement points; mediates or de-conflicts DPs per MPs in some implementations.
PE	Physical and Environmental Protection	This family of controls addresses the controlling of the spaces in which system components operate, to ensure that components cannot be accessed, modified, replaced, stolen, or removed in a manner that would violate security policy.
PEP	Policy Enforcement Point	A service that resides on and directly interacts with network objects (e.g., servers, asset scanners, firewalls), which exchanges policy-related messages with the Policy Decision Point. The PEP enforces organizational policy via the configuration applied to the object.
PL	Planning	This family of controls addresses the organization's security plans. Factors include how the plan is developed; contents of the plan; and the plan's impact on security, privacy, and organizational operations.
PRIV	Managing Account Access Capability	This CDM capability is to provide an agency the assurance that users and systems have access to, and control of, only the appropriate resources. The capability identifies access beyond what is needed to meet business requirements.
PS	Personnel Security	This family of controls addresses vetting of the authorized organizational users of the system and system components.
RA	Risk Assessment	This family of controls addresses that the development, deployment, and operation of the system is controlled by and is compatible with the organization's overall risk assessment process.
RMF	Risk Management Framework	A structured approach used to oversee and manage risk for an enterprise.
SA	System and Services Acquisition	This family of controls addresses how the organization acquires and operates the system.

Acronym	Term	Definition
SC	System and Communications Protection	This family of controls addresses how the system is designed and operated to detect and defeat attempted attacks.
SCRM	Supply Chain Risk Management	The process of identifying, assessing, and mitigating the risks associated with the distributed and interconnected nature of IT/operational technology (OT) product and service supply chains. It covers the entire life cycle of a system (including design, development, distribution, deployment, acquisition, maintenance, and destruction), as supply chain threats and vulnerabilities may intentionally or unintentionally compromise an IT/OT product or service at any stage.
SDLC	System Development Life Cycle	The process of planning, creating, testing, and deploying an information system. The SDLC concept applies to a range of hardware and software configurations, as a system can be composed of hardware only, software only, or a combination of both.
SI	System and Information Integrity	This family of controls addresses protecting the system from attacks using malicious code; monitoring system behavior to detect flaws or attacks; and acting to remediate the situation when a flaw or attack is detected.
SP	Special Publication	NIST Special Publications that include SP 800 subseries (computer security), SP 1800 subseries (NIST Cybersecurity Practice Guides) and selected SP 500-series (information technology) publications directly relevant to computer/cyber/information security and privacy
SWAM	Software Asset Management	The SWAM Function is to discover unauthorized or unmanaged software on a network.
TFA	Tool Functional Area	DHS is implementing the CDM program, made up of 15 BPA TFAs, that addresses “what is on the network,” “who is on the network,” and “what is happening on the network.”
TRUST	Manage Trust in People Granted Access Capability	This CDM capability assesses the inherent risk to an Agency from insider attacks for the purposes of granting trust to users and authorizing each user for certain attributes.

Acronym	Term	Definition
USB	Universal Serial Bus	An industry standard for connecting devices to computers.
VUL	Vulnerability Management	The VUL Function is to discover and support remediation of vulnerabilities in IT assets on a network as defined in NIST SP 800-53 controls.

Table 3: Acronyms, Terms and Definitions

III - Appendix B: Cybersecurity Framework Categories

Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.

Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.

Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.

Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.

Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.

Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.

Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.

Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.

Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.

Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.

Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.

Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.

Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.

Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.

Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.

Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.

Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.

Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.

Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.

Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.

Continuous Diagnostics and Mitigation (CDM)

Technical Capabilities

Volume Two

Requirements Catalog

Version 1.0

July 18, 2017

Table of Contents

I - Introduction **3**
I - 1 Evolution of CDM Attachment N Requirement's Documents 5
I - 2 Other key cross-references 5
II - CDM Detailed Requirements **6**
II - 1 Requirements Common to All CDM Capabilities 6
II - 1.1 Common Actual State 6
II - 1.2 Common Interoperability 6
II - 1.3 Common Scaling 6
II - 1.4 Common Securing 7
II - 1.5 Common Timeliness and Completeness 7
II - 1.6 Common Grouping 7
II - 1.7 Common Policy Decision Point 7
II - 2 Requirements to manage "What is on the network?" 7
II - 2.1 HWAM Requirements 8
II - 2.2 SWAM Requirements 9
II - 2.3 CSM Requirements 11
II - 2.4 VUL Requirements 12
II - 3 Requirements to manage "Who is on the network?" 13
II - 3.1 TRUST Requirements 14
II - 3.2 BEHAVE Requirements 15
II - 3.3 BEHAVE Operational Requirements 16
II - 3.4 BEHAVE Functional Requirements 16
II - 3.5 BEHAVE Tool Functionalities 17
II - 3.6 CRED Requirements 17
II - 3.7 PRIV Requirements 19
II - 4 Requirements to Manage "What is happening on the network?" 19
II - 4.1 Manage BOUND, or "How is the network protected?" 20
II - 4.2 Manage Events (MNGEVT) Requirements 27
II - 4.3 Operate, Monitor and Improve (OMI) Requirements 31
II - 4.4 Design and Build in Security (DBS) Requirements 35
III - References **40**
IV - Appendix A: Acronyms, Terms and Definitions **41**

Table 1: CDM Phased Attachment-N Requirements and Associated CDM BPA Capabilities 4

Figure 1: Phases of CDM 3

I - Introduction

Strengthening the security posture of Federal networks, systems, and data is one of the most important challenges we face as a nation. Therefore, the Department of Homeland Security (DHS) seeks to provide agencies with the Continuous Diagnostics and Mitigation (CDM) program to safeguard, secure, and strengthen cyberspace and the security posture of Federal networks in an environment where cyber attacks are continuously growing and evolving.

This document describes the requirements for the CDM program that are consistent with the overarching goal of enabling U.S. Government entities to assess and improve the security posture of agencies' information systems. These requirements will be used for the CDM solicitations called DEFEND (Dynamically Evolving Federal Enterprise Network Defense).

The companion volume (Volume One) "CDM Technical Capabilities - Defining Actual and Desired States" should be used in conjunction with this document.

Since the cybersecurity space is inherently complex, the CDM approach is to address the problem space in phases, as shown in Figure *1*:

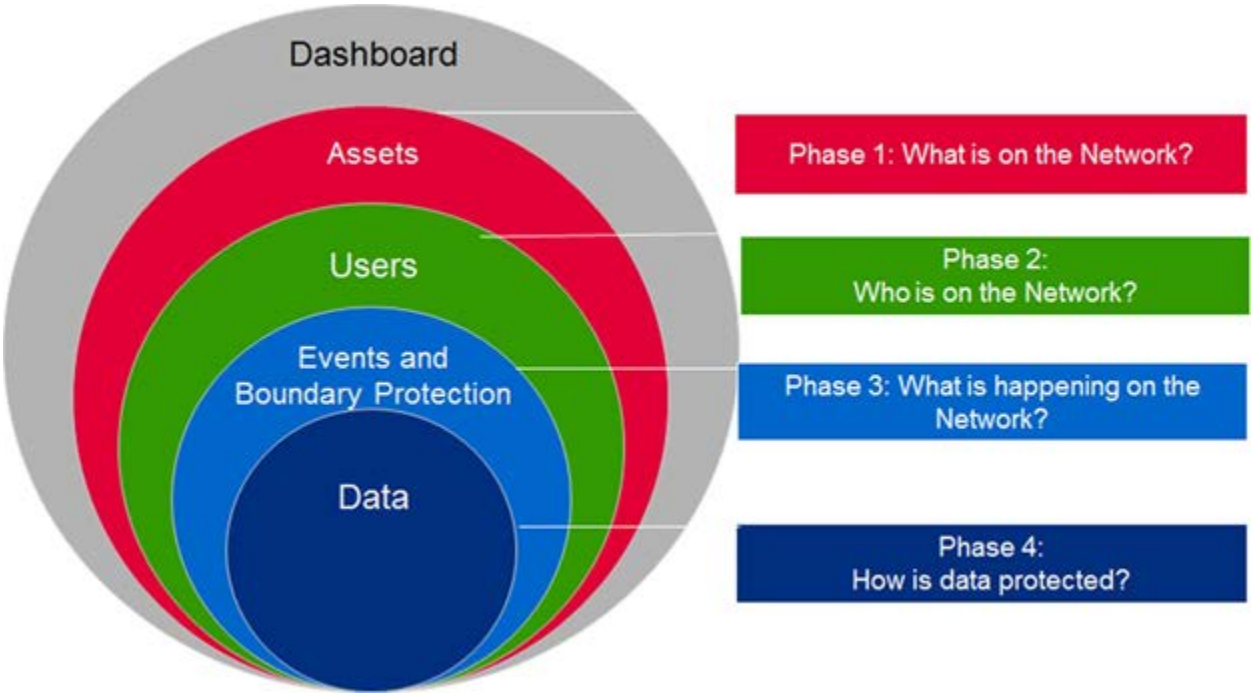


Figure 1: Phases of CDM

The CDM requirements to support these phases are grouped into the following:

1. Requirements to manage "What is on the network?"
2. Requirements to manage "Who is on the network?"
3. Requirements to manage "What is happening on the network?" are decomposed into four sub-areas:
    a. Managing Events (MNGEVT)
    b. Operate, Monitor, and Improve (OMI)

   c. Design and Build in Security (DBS)
   d. Boundary Protection (BOUND) – addressing "How is the network protected?"
4. Requirements to manage "How is data protected?"[1]

Table *1* shows the relationship between the original Attachment N documents, corresponding tool functional areas (TFAs), and detailed requirements for each CDM Phase.

DHS CDM Phase Attachments	Phased Detailed Requirements	CDM/CMaaS Blanket Purchase Agreement (BPA) TFAs
Phase 1 Attachment N	Manage "What is on the network?"	• TFA 1 – Hardware Asset Management • TFA 2 – Software Asset Management • TFA 3 – Configuration Settings Management • TFA 4 – Vulnerability Management
Phase 2 Attachment N-2	Manage "Who is on the network?"	• TFA 6 – Manage Trust in People Granted Access • TFA 7 – Manage Security-Related Behavior • TFA 9 – Manage Credential and Authentication • TFA 9 – Manage Account/Access/Manage Privileges
Phase 3 Attachment N-BOUND	Manage "How is the network protected?"	• TFA 5 – Manage Network Access Controls
Phase 3 Attachment N-3-Manage Events	Manage "What is happening on the network?" for MNGEVT	• TFA 10 – Prepare for Contingencies and Incidents • TFA 11 – Respond to Contingencies and Incidents • Ongoing Assessment
Phase 3 Attachment N-3-Design and Build in Security	Manage "What is happening on the network?" for DBS	• TFA 12 – Design and Build in Requirements Policy and Planning • TFA 13 – Design and Build in Quality • Supply Chain Risk Management
Phase 3 Attachment N-3-Operate, Monitor and Improve	Manage "What is happening on the network?" for OMI	• TFA 14 – Manage Audit Information • TFA 15 – Manage Operation Security • Ongoing Authorization

Table 1: CDM Phased Attachment-N Requirements and Associated CDM BPA Capabilities

[1] This is often referred to as "Phase 4," which is in the early planning and definition stages with requirements yet to be developed.

I - 1 Evolution of CDM Attachment N Requirement's Documents

This document is dependent on companion volume "CDM Defining Actual and Desired State," subsequently referred to as "Companion."

The evolution from the CDM Attachment N requirement documents to the CDM detailed requirements in section II - CDM Detailed Requirements was achieved by updating the requirements to support the following goals:

- Consolidate requirements across all phases.
- Provide a consistent structure and content.
- Capture the same level of breadth and depth of technical information.
- Delete information that is no longer relevant or applicable.
- Describe system-level functional and operational requirements of the CDM program through the desired state values and actual state values.

I - 2 Other key cross-references

Section II of this document will also reference to the following parts of the Companion:

1. CDM Architecture (Companion I-1)
2. CDM and the Cybersecurity Framework (CSF) (Companion I-2)
3. CDM and the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) (Companion I-3)
4. Defining CDM from Attachment N requirement's Documents (Companion I-4)

Users of this document should be familiar with the contents of the Companion volume.

II - CDM Detailed Requirements

Based on the above enhanced CDM phase definitions, this section describes CDM requirements in terms of those requirements that are common to all phases and then describes the detailed requirements for each area of focus.

While these requirements are for the entire scope of the CDM solution ecosystem, the primary area impacted would be Layer A and B in the CDM Architecture.[2] The Dashboard plays an active role in providing visibility to the outcomes of these requirements and providing the policy orchestration if applicable. There are additional specific requirements to the dashboards (both Federal and Agency) that are managed through the Dashboard-specific development process.

II - 1 Requirements Common to All CDM Capabilities

The requirements in this section are common and mandatory, and apply universally across all CDM capabilities. These requirements are in addition to operational and functional requirements covered in sections II - 2 through II - 4 . All CDM capabilities support the Governance CSF Category under the Identify CSF Function and the Continuous Monitoring and Anomalies and Events CSF Categories under the Detect CSF Function.

II - 1.1 Common Actual State

C_AS_FR-1-1: Shall have a date/time associated with each instance of Actual State information and identify the collection source.

II - 1.2 Common Interoperability

C_Interop_OR-1-1: Shall deliver information to the CDM Dashboard using standardized data structures and/or API (application program interfaces).

C_Interop_OR-1-2: Shall support data interchange and sharing between all CDM capabilities using standardized formats.

C_Interop_FR-1-1: Shall receive and collect relevant data via a standard interface and in a standard format to the CDM Dashboard and other solution subsystems using CDM data structure(s), including use of MUR, MDR, MIR, and MSR.[3]

II - 1.3 Common Scaling

C_Scale_FR-1-1: Shall store, process, and provide data for large Federal organizations (using the threshold of up to one million devices) while maintaining adequate timeliness, completeness, and accuracy for applicable capabilities.

C_Scale_FR-1-2: Shall minimize the use of network bandwidth and end point system resources to limit potential impact to mission/business operations.

[2] Found in Companion section I-1.1.

[3] Found in Companion section I-1.2.4

II - 1.4 Common Securing

C_Secure_FR-1-1: Shall support Federal Information Processing Standard (FIPS) 140-2 approved algorithms to encrypt data, both in transit and at rest, consistent with Federal and Agency policies.

C_Secure_FR-1-2: Should provide source integrity verification for all tool components, such as digital fingerprints for each software file used within the system.[4]

II - 1.5 Common Timeliness and Completeness

C_Time-FR-1-1: Shall support the requirement that attribute information associated with an object is within the 72-hour data currency goal coupled with the 90% coverage goal for all objects.

C_Time-FR-1-2: Shall retain assessment results for an Agency-defined period to enable enterprise security posture reporting and trending.

II - 1.6 Common Grouping

C_Group_OR-1-1: Shall include the mechanism to define risk scores for the difference between actual and desired states (including scores that reflect a reduction in risk) dependent on object context (e.g., Organizational Unit [OU] and Federal Information Security Management Modernization Act [FISMA] container linkage) and the scope of the capability's attributes.

C_Group-OR-1-2: Shall include the mechanism to define actual state dependent on object context and the scope of the capability's attributes.

C_Group-OR-1-3: Shall include the mechanism to define the desired state for an object dependent on the object context (e.g., OU and FISMA container linkage) and the scope of the capability's attributes.

II - 1.7 Common Policy Decision Point

C_PDP_FR-1-1: Shall include Policy Decision Point (PDP) capabilities to support the ingestion of machine-readable policies to measure the actual state against the desired state for ongoing assessment of security controls.

C_PDP_FR-1-2: Shall support the MUR, MDR, MIR, and MSR in conjunction with PDP, specific to the determination of actual versus desired state function of the PDP.

II - 2 Requirements to manage "What is on the network?"

Managing "what is on the network?" requires the management and control of devices (HWAM), software (SWAM), security configuration settings (CSM), and software vulnerabilities (VUL).

These four functions are briefly summarized below, and the requirements are separately specified later in the HWAM, SWAM, CSM, and VUL sections.

- HWAM discovers and manages Internet Protocol (IP) addressable devices on the network.

[4] Dependent on the ongoing formulation of Federal policies directing increased activities for Supply Chain Risk Management (SCRM).

- SWAM discovers and manages the software installed on devices on the network.
- CSM identifies and manages the security configuration settings for devices (and the associated installed software) on the network.
- VUL discovers and supports remediation of the vulnerabilities in software installed on devices on the network.

Note that while the scope of HWAM is to capture the entire Agency "attack surface," the scope of SWAM, CSM, and VUL is specific to the subset of HWAM that is under the accountability and therefore control of the Agency. This is determined by the Agency's overall risk management strategy and as articulated in the Agency's Information Security Continuous Monitoring strategy.

II - 2.1 HWAM Requirements

The HWAM capability discovers IP-addressable hardware on a network.

HWAM establishes and maintains a hardware inventory baseline, unique identifiers for hardware, and other properties, such as the manager of the hardware.

HWAM also establishes and maintains the actual inventory of hardware in accordance with data currency requirements, along with information needed to assess the risk to and locate the hardware.

The capability to maintain and update the inventory needs to allow for decentralized administration, using appropriate access and audit controls to ensure that only authorized personnel with appropriate privileges can modify authorized inventories, and only for assets for which they are accountable. Data in the authorized hardware inventory baseline must be validated continuously through automated hardware discovery. Manual processes, such as assigning hardware to the baseline, are expected to integrate with and be supported by automated processes.

II - 2.1.1 HWAM Operational Requirements

HWAM _OR-1-1: Shall identify and track hardware devices (physical and virtual) that are on the network, authorization status and who (by individual, access group, or organization) manages each device.

HWAM_OR-1-2: Shall allow manual or batch creation of Agency approved device data (e.g., through integration with external asset information repositories or through business rules).

II - 2.1.2 HWAM Functional Requirements

This capability requires CDM tools and sensors to collect information about attributes in the OU and FISMA containers and the MDR. This capability is related to CSM to ensure that hardware configuration settings are correctly maintained. If cryptography is used, this capability is related to BOUND-E. This capability supports the Asset Management CSF Category under the Identify CSF Function CSF Category under the Protect CSF Function.

HWAM_FR-1-1: Shall:

a. Provide a unique identifier (which may vary by device type) that supports device persistent of any network location changes for each device on the network.

b. Identify and collect hardware inventory information on all IP addressable devices on the network on a scheduled and ad-hoc basis as specified by authorized users.
c. Collect appropriate data to match actual to authorized Agency approved (i.e., authorized devices) hardware inventory, including when detected and if the device is in desired state.
d. Document and record Agency approved (i.e., authorized devices) hardware inventory information, including device type (e.g., router, workstation, firewall, printer), owner/manager, and operational status.

HWAM_FR-1-2: Should:

a. Collect data to enable staff to physically locate the hardware devices.
b. Collect additional data (e.g., subcomponents, attached peripheral devices, local account information), for managed and properly configured devices and with credentials sufficient to validate actual inventory data.
c. Detect the type of each hardware device based upon its network behavior.

II - 2.1.3 HWAM Tool Functionalities

The following is a non-exclusive list of tool functionalities that support the HWAM capability:

- Passive detection tools
- Tools to interrogate network infrastructure to detect devices
- Active scanning tools
- Tools that provide packet filtering for device identification

II - 2.2 SWAM Requirements

The SWAM capability discovers software installed on managed network hardware devices. Since unauthorized software may be vulnerable and exploited as a pivot to other network assets, there is a need for unauthorized software to be removed or managed. In addition, a complete, accurate, and timely software inventory is essential to support awareness and effective control of software vulnerabilities and security configuration settings. Malware often exploits vulnerabilities to gain unauthorized access to and tamper with software and configuration settings to propagate throughout the enterprise.

SWAM establishes and maintains a software inventory, unique identifiers for software, and other properties such as the manager of the software.

SWAM also establishes and maintains the actual inventory of all software in accordance with data currency requirements, along with information needed to assess the risk to and physically locate the software.

The capability to maintain and update the software inventory needs to enable decentralized administration, using appropriate access and audit controls, to ensure that only authorized personnel with appropriate privileges can modify authorized inventories, and only for software for which they are accountable.

The authorized software inventory baseline is established through some process involving actual inventory data and business rules that determine assignment of default responsibility. Data in the

authorized software inventory baseline should be validated continuously through automated software discovery. Manual processes, such as assigning software to the baseline, are expected to integrate with and be supported by automated processes.

II - 2.2.1 SWAM Operational Requirements

SWAM _OR-1-1: Shall identify and track software products that are on the device for each hardware device (physical and virtual) on the network within Agency system boundaries, authorization status, and who (by individual, access group, or organization) manages each software product.

SWAM_OR-1-2: Shall allow manual or batch creation of authorized software data (e.g., through integration with external asset information repositories or through business rules).

II - 2.2.2 SWAM Functional Requirements

This capability requires CDM tools and sensors to collect information about attributes in the OU and FISMA containers and the MDR. This capability is related to CSM to ensure that software configuration settings are correctly maintained. This capability also is related to DBS to understand the provenance of software and the risk associated with the development and acquisition of software components. If cryptography is used, this capability is related to BOUND-E. This capability supports the Asset Management CSF Category under the Identify CSF Function CSF Category under the Protect CSF Function.

SWAM_FR-1-1: Shall:

a. Provide a unique identifier (e.g., Common Platform Enumeration [CPE], Software Identification Tags) for each software product that is used to identify instances of installed software products and components, including version number, across devices on the network.
b. Identify and collect software inventory information on Agency defined and scoped devices on the network on a scheduled and ad hoc basis as specified by authorized users.
c. Collect additional data (e.g., software components, component digital fingerprints) for managed and properly configured devices, with credentials sufficient to validate actual inventory data.
d. Document and record software inventory information, including product name, owner/manager, and operational status.

SWAM_FR-1-2: Should execute detect/protect for:

a. Malware (including, as configured, all on whitelisted software, and software not behaving as expected) at a rate comparable to existing anti-virus products, and provide a means for removing malware in time to prevent it from executing.
b. Whitelist changes and software installation actions.
c. Unauthorized software execution by blocking based on an authorized software list specific to each hardware device. At a minimum, resident executables must be blocked.

II - 2.2.3 SWAM Tool Functionalities

The following is a non-exclusive list of tool functionalities that support the SWAM capability:

- Blacklisting tools
- Whitelisting tools
- Software version scanning tools
- License management tools

II - 2.3 CSM Requirements

The CSM capability reduces misconfiguration of assets, including misconfigurations of hardware devices (including physical and virtual machines, as well as the associated operating system) and software. Cyber adversaries often use automated scanning attacks to search for and exploit assets with misconfigurations, and then pivot to attack other assets.

CSM establishes and maintains security configuration benchmarks, consisting of the acceptable value(s) for each relevant configurable setting for each asset type.

CSM also establishes and maintains the value of the actual settings for each relevant configurable setting for each asset type.

Differences between desired and actual configuration settings represent a change in risk to the system. CSM needs to assign core (using the Federal benchmark) and alternate (using the Agency benchmark) risk scores to each reported configuration setting difference based on relevant factors. The configuration setting's difference may make the information system more secure (have less risk), which may be accounted for in the risk score determination.

CSM supports managing a change control process that documents Agency extensions or exceptions (an authorized difference with the justification for the difference) to the authorized core Federal benchmarks.

II - 2.3.1 CSM Operational Requirements

CSM _OR-1-1: Shall:

a. Create, update, and maintain the security configuration settings benchmarks for target hardware devices and software products, including the Federal core benchmark as well as Agency-specific variations that implement Agency policies.
b. Store, process, maintain, track changes, and distribute security configuration benchmarks, including Agency exceptions (including the justification and compensating countermeasures), as determined by authorized users (with authorization being granted per benchmark).
c. Permit authorized users to select and compose a set of security configuration benchmarks to establish an authorized security configuration baseline for an asset or group of assets.

II - 2.3.2 CSM Functional Requirements

This capability requires CDM tools and sensors to collect information about attributes in the OU and FISMA containers, the MDR, and the MSR. This capability is related to HWAM and

SWAM to accurately assess hardware and software configuration settings on authorized devices. If cryptography is used, this capability is related to BOUND-E. This capability is also related to MNGEVT to implement auditing on devices. Finally, this capability is related to DBS to ensure implementation of configuration settings baselines provided as part of information system deployment. This capability supports the Risk Assessment CSF Category under the Identify CSF Function and the Data Security, Information Protection, and Maintenance CSF Categories under the Protect CSF Function.

CSM_FR-1-1: Should:

a. Support a unique identifier (CCE) for each configuration setting collection across devices on the network.

b. Identify and collect configuration settings (including the actual values) for specific software and hardware products on Agency defined and scoped devices on the network on a scheduled, event-driven, and ad hoc basis as specified by authorized users.

c. Document authorized security configuration settings that are set and managed by authorized users within benchmarks for specific software and hardware products.

d. Enumerate differences from the security configuration benchmark, including differences that provide greater protection or reduce risk further than the benchmark.

II - 2.3.3 CSM Tool Functionalities

The following is a non-exclusive list of tool functionalities that support CSM capability:

- Security Content Automation Protocol (SCAP) configuration assessment tools
- CCE assessment tools
- Common Configuration Scoring System (CCSS) tools

II - 2.4 VUL Requirements

The VUL capability discovers vulnerabilities in assets on the network. Vulnerability management is the management of risks presented by known software weaknesses that are subject to exploitation. The vulnerability management function ensures that mistakes and deficiencies are identified. (An information security vulnerability is a deficiency in software that a hacker can use to gain access to a system or network.)

VUL discovers, identifies, and locates known security vulnerabilities in network assets.

Most vulnerabilities are defined by the Common Vulnerabilities and Exposures (CVEs®), though other detectable vulnerabilities may exist that are not in the CVEs® and for which patching may also be an available remedy. Vulnerabilities identified will typically be remediated through the software inventory management function, using updates, patches, plug-ins, and new releases.

II - 2.4.1 VUL Operational Requirements

VUL_OR-1-1: Shall:

a. Update tools in a timely manner to be able detect vulnerabilities that have been identified by the Government CVEs.

b. Discover vulnerabilities on the network using unauthenticated or authenticated methods.

VUL_OR-1-2: Should:

a. Provide text for system administrators to explain clearly and simply how to correct the vulnerability.

II - 2.4.2 VUL Functional Requirements

This capability requires CDM tools and sensors to collect information about attributes in the OU and FISMA containers and the MDR. This capability is related to DBS to discover, identify, and locate other known weaknesses in software applications and source code and the use of Supply Chain Risk Management (SCRM) to support the awareness and understanding of potential exposure to risks associated with the provenance of system components. This capability supports the Risk Assessment CSF Category under the Identify CSF Function and the Data Security, Information Protection, and Maintenance CSF Categories under the Protect CSF Function.

VUL_FR-1-1: Shall:

a. Identify and collect vulnerability information, including time first detected and time remediated, on all IP addressable devices on the network on a scheduled, event-driven, and ad hoc basis as specified by authorized users.
b. Collect appropriate data to map actual vulnerabilities to the on-network hardware and software inventories.

VUL_FR-1-2: Should:

a. Provide complete coverage of the CVEs identified by the National Vulnerability Database (NVD) and equivalent vulnerability information from other useful sources.

II - 2.4.3 VUL Tool Functionalities

The following is a non-exclusive list of tool functionalities that support the VUL capability:

- Vulnerability scanners
- Web application scanners
- Database scanners
- Import published vulnerabilities

II - 3 Requirements to manage “Who is on the network?”

Managing “Who is on the network?” requires the management and control of account/access/managed privileges (PRIV), trust determination for people granted access (TRUST), credentials and authentication (CRED), and security-related behavioral training (BEHAVE). These four functions have significant interdependencies. The separation of measurements and execution of the controls related to these areas poses a complex set of problems and requires a coordinated effort to properly assess the actual state.

This capability supports the Asset Management CSF Category under the Identify CSF Function, the Communications CSF Category under the Respond CSF Function, and the Access Control CSF Category under the Protect CSF Function.

These four functions are briefly summarized below, and the requirements are separately specified later in the TRUST, BEHAVE, CRED, and PRIV sections.

- TRUST validates a person's identity and the degree to which he or she has been vetted.
- BEHAVE identifies that the individual has the proper knowledge and training for the roles he or she is assigned and that he or she remains up to date.
- CRED binds a type of credential or authentication mechanism to an identity established in TRUST with a level of assurance and is used to grant access (physical and logical).
- PRIV establishes the privileges associated with the credential and in turn the individual or service.

II - 3.1 TRUST Requirements

The TRUST capability reduces the probability of loss in availability, integrity, and confidentiality of data by ensuring that only properly vetted users are given access to systems and credentials, including user, system, and users with elevated privileges and special security roles. This includes the requirement that the vetted trust level is properly monitored and renewed per Agency policy.

The primary attributes that will be looked at within the trust capability are that the background investigations and any related determinations are "current" (as specified in the Federated Identify, Credential, and Access Management [FICAM] roadmap) according to the "currency" criteria of the Agency:

- Security clearance determination (if applicable)
- Suitability determination
- Fitness determination

Collecting data associated with the level of trust granted to a user, the level of trust required for an attribute, actual attributes for which the user is assigned or authorized, and other locally defined policy for attributes and TRUST levels will provide measurable data for the performance of automated security checks. These security checks will provide the basis for automating the monitoring, reporting, and prioritizing of trust deficiencies in an Agency's cyber environment.

The TRUST capability will help ensure that every user meets the required trust level of any assigned attribute, is periodically rescreened to revalidate trustworthiness, and is not assigned to incompatible attributes that violate an Agency's policies.

II - 3.1.1 TRUST Operational Requirements

TRUST_OR-1-1: Shall:

a. Employ an established screening/indoctrination process before granting access to various levels of sensitive material.
b. Make key trust level authorization attributes available to the systems and processes that monitor/enforce access.

c. Have security checks that provide the basis for automating the monitoring, reporting, and prioritizing of trust deficiencies in an Agency's cyber environment.
d. Provide, to control systems and processes that monitor/enforce access, key TRUST attributes about authorization requirements regarding a user at the time that user is authorized for access to a facility or an account on a system.

II - 3.1.2 TRUST Functional Requirements

This capability requires CDM tools and sensors to collect information about attributes in the OU and FISMA containers and the MUR. This capability is related to BOUND-P and BOUND-F to support physical and logical access control decisions for access to facilities, systems, and information.

TRUST_FR-1-1: Shall:

a. Collect and report TRUST information on all users.
b. Determine the granted trust level for each authorized user.
c. Determine the required operational trust level for each user.
d. Determine when a user issued a credential does not meet trust level requirements and when that user's trust level has expired.

II - 3.1.3 TRUST Tool Functionalities

The following is a non-exclusive list of tool functionalities that support TRUST capability:

- Audit reporting
- Policy management

II - 3.2 BEHAVE Requirements

The BEHAVE capability documents that authorized users exhibit appropriate security-related behaviors. For CDM, appropriate security-related behavior is defined as actions that have been explained and "agreed to" by the user via user agreements, training, job requirements, or similar methods. This capability provides an Agency with insight into risks associated with non-conformance with policies for accessing systems and data by authorized users. Agencies have an increased risk when any user is granted access to facilities, systems, and information without the appropriate security training, demonstrated skill specialty knowledge, or certification. These users may have been granted access to resources or sensitive data without completing proper security-related documentation or training, may have ineffective training, or may not have been assigned the proper training for the access. Poorly trained users can engage in behaviors that compromise systems, expose sensitive data, or subvert security policies meant to mitigate risk. This capability is dependent on the existence of a set of attributes that denote roles or characteristics that require specific security-related behaviors per policy. All authorized users have minimum security-related training requirements. Authorized users with special access may have additional training requirements.

Collecting data associated with completed training, security-related behavior documentation required for an attribute, and actual attributes for which the user is assigned or authorized provides measurable data elements for the creation of automated security checks. These security

checks provide the basis for automating the monitoring, reporting, and prioritizing of security-related behavior deficiencies in an Agency's cyber environment.

Properly implemented and acted upon, the BEHAVE capability helps to ensure that every user has received appropriate and up-to-date training and knowledge/certification for access to facilities, systems, and information

II - 3.3 BEHAVE Operational Requirements

BEHAVE_OR-1-1: Shall:

a. Validate the existence of Agency training policies and report on their enforcement. Agency training policies shall document how long a training/knowledge/certification activity is valid before it expires and the user is required to repeat the training/knowledge/certification.
b. Make reports of successful completion of required training/knowledge/certification available to the systems and processes that can monitor/enforce access.
c. Collect data associated with completed training/knowledge/certification and security-related behavior documentation required for security-related behavior requirements for which the user is assigned or authorized in order to provide measurable data elements for the creation of automated security checks.
d. Provide, to control systems and processes that monitor/enforce access, key BEHAVE attributes about authorization requirements regarding a user at the time that user is authorized for access to a facility or an account on a system.

BEHAVE_OR-1-2: Should:

a. Utilize automated security checks to provide the basis for automating identifying, monitoring, reporting, prioritizing, reviewing, and correcting security-related behavior deficiencies in an Agency's cyber environment.
b. Define appropriate grace periods for training/knowledge/certification associated with each security-related behavior requirement.

II - 3.4 BEHAVE Functional Requirements

This capability requires CDM tools and sensors to collect information about attributes in the OU and FISMA containers and the MUR. This capability is related to BOUND-P and BOUND-F to support physical and logical access control decisions for access to facilities, systems, and information. This capability is also related to MNGEVT and OMI when behavior events related to incidents are recorded in the MIR and may influence attribute values in the MUR. This capability supports the Awareness & Training CSF Category under the Protect CSF Function and the Communications CSF Category under the Respond CSF Function.

BEHAVE_FR-1-1: Shall:

a. Collect and report BEHAVE information for each authorized user in the Agency.
b. Collect and report security-related behavior indicators for each authorized user in the Agency.

c. Include training completed, knowledge demonstrated, and/or certification obtained, depending on Agency policy.
d. Support collection, monitoring, and reporting of general security-related training applicable to all users.
e. Support collection, monitoring, and reporting for security-related training based on the roles authorized/assigned to the user.

BEHAVE_FR-1-2: Should:

a. Provide collection mechanisms and/or processes to detect and record/report information to identify when an authorized user does not meet attribute-based security-related behavior requirements, and when an authorized user's security-related behavior requirements have expired.

II - 3.5 BEHAVE Tool Functionalities

The following is a non-exclusive list of tool functionalities that support BEHAVE capability:

- Audit reporting
- Learning management system
- Security-related behavior management

II - 3.6 CRED Requirements

The CRED capability reduces the probability of loss in availability, integrity, and confidentiality of data by ensuring that only proper credentials are authenticated to systems, services, and facilities. This includes the requirement that credentials are properly monitored and renewed per Agency policy. The capability is intended to ensure that credentials for both physical and logical access are assigned to, and only used by, authorized users or services that require that access to perform their specific job functions.

The CRED capability provides an Agency insight into risks associated with weaknesses in its credential management. The CRED capability collects data associated with the credentials issued to a user, the credential type required for an attribute, actual attributes the user is assigned or authorized, and the locally defined policies for authentication, in order to provide measurable data elements for the creation of automated security checks. These security checks provide the basis for automating the monitoring, reporting, and prioritizing of credential and authentication deficiencies in an Agency's cyber environment.

CRED capability will help ensure that every user can be authenticated appropriately for access to facilities, systems, and information. The capability will also provide insight into whether authentication, reissuance, and revocation policies are incurring more risk than deemed acceptable by the Agency.

II - 3.6.1 CRED Operational Requirements

CRED_OR-1-1: Shall:

a. Employ an approved process for issuing different credential types and defining authentication requirement policies for access to various facilities, systems, and information.

b. Provide, to control systems and processes that monitor/enforce access, key CRED attributes about authorization requirements regarding a user at the time that user is authorized for access to a facility or an account on a system.

c. Continuously monitor key outputs from the credential issuance and authentication definition processes to detect when a credential or authentication action deviates from established standard(s).

d. Verify that all authentication mechanisms deployed on in-scope systems across the Agency implement the appropriate authentication policy.

e. Verify that all credential types have appropriate expiration, reissuance, and revocation policies.

II - 3.6.2 CRED Functional Requirements

This capability requires CDM tools and sensors to collect information about attributes in the OU and FISMA containers and the MUR. This capability is related to BOUND-F and BOUND-P to support physical and logical access control decisions for access to facilities, systems, and information. If cryptography is used, this capability is related to BOUND-E. This capability supports the Anomalies & Events CSF Category and the Continuous Monitoring CSF Category under the Detect CSF Function.

CRED_FR-1-1: Shall collect and report CRED information associated with accounts and users, including:

a. Credentials (e.g., X.509 certificates, user identifiers, public/private key pairs) issued to each user employed by the Agency (including contractors).
b. Credential reissuance, revocation, and suspension enforcement mechanisms and their configuration for all applicable credential types.
c. Password complexity enforcement mechanisms and their configuration for all in-scope accounts at the Agency.

CRED_FR-1-2: Shall verify:

a. The authentication mechanisms implemented for every in-scope account at the Agency.
b. Default accounts/passwords are NOT enabled on in-scope systems.

II - 3.6.3 CRED Tool Functionalities

The following is a non-exclusive list of tool functionalities that support this capability:

- X.509 certificates
- Public Key Infrastructure (PKI)
- Identity and access management
- Access certifications
- Authentication mechanisms

- Audit reporting

II - 3.7 PRIV Requirements

The PRIV capability provides the Agency with insight into risks associated with authorized users being granted excessive privileges to facilities and systems. The intent of the capability is to ensure that privileges for both physical and logical access are assigned to authorized people or accounts that require authorized access for job functions. This capability is dependent on the existence of a set of attributes that denote roles or characteristics that require or restrict specific privileges per policy.

The PRIV capability collects the privilege rights for all privileged accounts as attributes. Privilege policies can be mapped directly to attributes.

The PRIV capability identifies access beyond what is needed to meet business mission by monitoring and measuring account access privileges, identifying excess privileges, and identifying unneeded accounts. The PRIV capability reduces the risk of the loss of confidentiality, integrity, and availability of data due to the provision of excessive access, including physical access, to people who do not need such access to perform their work.

The PRIV capability helps to ensure that authorizations and accounts do not exceed the privileges required by a user's attributes. The capability also provides insight into whether access (re)authorization policies are incurring more risk than deemed acceptable by the Agency.

II - 3.7.1 PRIV Functional Requirements

This capability will require CDM tools and sensors to collect information about attributes in the OU, FISMA, and MUR. This capability may interact with BOUND to manage and control logical and physical access decisions (e.g., in BOUND-P and BOUND-F) for facilities, systems, and information.

PRIV_FR-1-1: Shall collect and report:

a. PRIV information on privileged and non-privileged accounts and users.
b. Physical access authorizations issued to each user employed by the Agency.
c. Account status (restrictions, enablement, revocation, in authorization time window, etc.) implemented for every in-scope account at the Agency.

II - 3.7.2 PRIV Tool Functionalities

The following is a non-exclusive list of tool functionalities that support the PRIV capability:

- Identity and access management
- Privileged account management
- Credential management
- Compliance verification

II - 4 Requirements to Manage "What is happening on the network?"

Managing "What is happening on the network?" builds on the CDM capabilities provided by "What is on the network?" and "Who is on the network?" These CDM capabilities include

network and perimeter components, host and device components, data at rest and in transit, and user behavior and activities. These capabilities move beyond asset management to a more extensive and dynamic monitoring of security controls. This includes preparing for and responding to behavior incidents, ensuring that software/system quality is integrated into the network/infrastructure, detecting internal actions and behaviors to determine who is doing what, and finally, mitigating security incidents to prevent propagation throughout the network/infrastructure.

"What is happening on the network?" is broken into three capabilities. These capabilities are briefly summarized below, and the detailed requirements are separately specified later in the BOUND, MNGEVT, OMI, and DBS sections.

- BOUND (Section III - 4.1) describes that part of "What is happening on the network?" by focusing on "How is the network is protected?"
- MNGEVT (Section II - 4.2) describes ongoing assessment, preparing for events/incidents, audit data collection from appropriate sources, and identifying incidents through the analysis of data.
- OMI (Section II - 4.3) describes ongoing authorization, audit data aggregation/correlation and analysis, incident prioritization and response, and post-incident activities (e.g., information sharing).
- DBS (Section II - 4.4) describes preventing exploitable vulnerabilities from being effective in the software/system while the software/system is in development or deployment.

The iterative and continuous interaction between MNGEVT ongoing assessment and OMI Ongoing Authorization capabilities provides a systematic approach to prepare, detect, respond to, and recover from existing residual security risk and newly discovered security risk in near-real time. This automated approach is an attempt to move away from the traditional, static, multi-year risk assessment and authorization process that is slow to respond to security risks, attacks, and compromises.

II - 4.1 Manage BOUND, or "How is the network protected?"

Managing "How is the network protected?" requires capabilities that limit, prevent, and/or allow the removal of unauthorized network connections/access. Such access would allow attackers to cross internal and external network boundaries and then pivot to gain deeper network access and/or capture network resident data at rest or in transit.

This capability includes the use of devices such as firewalls that sit at a boundary and regulate the flow of network traffic. It also includes the use of encryption to protect traffic that must cross logical boundaries and addresses physical access systems that limit unauthorized user physical access to Federal Government facilities.

BOUND is categorized into three security capabilities:

- BOUND-F to Manage Network Filters and Boundary Controls
- BOUND-E to Monitor and Manage Cryptographic Mechanisms Controls
- BOUND-P to Monitor and Manage Physical Access Controls

II - 4.1.1 BOUND-F Requirements

Manage Network Filters and Boundary Controls (BOUND-F) network filters include devices such as firewalls and gateways that sit at the boundary between enclaves (such as a trusted internal network or subnet and an external or internal, less trusted network). The filters apply sets of rules and heuristics to regulate the flow of traffic between the trusted and less trusted sides of the boundary.

The BOUND-F capability is further divided into the following categories:

- Content Filtering
- Packet Filtering
- Layer 2 Filtering
- Network Access Protection
- Encapsulation Filtering

BOUND-F reduces the probability that unauthorized traffic will pass through a network boundary. This includes the requirement that the boundary filtering policies are monitored, reviewed, and reauthorized per Agency policy. Network boundary security focuses on network weaknesses and vulnerabilities that can affect the network's ability to prevent the disclosure of confidential data, to determine when the integrity of the network is compromised, and to detect when malicious behavior impacts the network's availability. For the purposes of BOUND-F, network encryption points (e.g., virtual private networks) are considered network boundaries. Policies involving network encryption will have attributes associated with both BOUND-F and BOUND-E.

A BOUND-F device must be capable of filtering (actively or passively) network traffic at some level per policy established by the Agency.

The BOUND-F capability provides Agencies visibility into the risk associated with boundary filtering policies, to include the use of network encryption. BOUND-F traffic filtering policies can be applied at one or more layers of the network stack. Policies at layers 4 and above typically filter based on specific applications and application content (e.g., filtering email messages and messages containing spam and/or malware). Those polices would contain content filtering records that describe the content that was filtered based on rules and policies.

Collecting data associated with the boundary filtering policy and the filtering policy required for network flow across a boundary provides measurable data elements for the creation of automated security checks. These security checks provide the basis for automating the monitoring, reporting, and prioritizing of boundary filtering policy deficiencies in an Agency's cyber environment. Through CDM, deficiencies are displayed for review and action.

BOUND-F helps to ensure that the filtering policies for enclaves and systems are properly implemented to secure network traffic crossing boundaries. The capability also provides insight into duplicative and/or conflicting filtering policies.

II - 4.1.1.1 BOUND-F Operational Requirements

BOUND_OR-1-1: Shall enforce one or more filtering policies using one or more PDPs and one or more Policy Enforcement Points (PEPs). These filtering policies control what data can enter or exit the system and may consist of one or more of the following filter types:

a. Content filtering to filter traffic based on the application content of the traffic, including both the syntax and the semantic content. For example, policies at layers 4 and above typically filter based on specific applications and application content (e.g., filtering email messages and messages containing spam and/or malware). Those polices describe the content that is filtered based on rules and policies.

b. Packet filtering to filter traffic based on IP packet header information and optionally on other IP datagram externals such as datagram length or frequency. For example, policies at the IP layer typically filter based on IP packet header information (e.g., filtering based on source and destination IP address). Those policies describe the datagrams and/or sessions that are filtered based on rules and policies.

c. Layer 2 filtering to filter traffic based on layer 2 header information and optionally based on other layer 2 traffic externals, such as length or frequency. For example, policies at the data link layer (layer 2) typically filter based on layer 2 header information (e.g., filtering based on source and destination Ethernet address or virtual local area network number). Those policies describe the packets that are filtered based on rules and policies.

d. Encapsulation filtering to filter traffic based on the encapsulation method and traffic characteristics (e.g., IP header attributes, application, and packet content). For example, encapsulation polices describe how data from one network protocol is translated into another network protocol so that the data can continue to flow across the network (e.g., encrypting traffic between two IP subnets across a wide area network). Those policies describe the network flows that are encapsulated and filtered based on rules and policies.

e. Network Access Protection to ensure that a device can only connect to an enterprise network if the device is explicitly authorized to connect, and is compliant with the stated hardware, software, configuration, and patching policies. Network Access Protection policies permit access to a network only if a device is approved to access that network, and is compliant with policies regarding hardware, software, configuration, and patching. For example, a device attempting to connect to a network can be blocked from connecting if the latest security updates are not installed. Network Access Protection also contains functions that can force the patching or upgrading of a device, and then allow connection. Network Access Protection policies describe the device connection actions that are filtered based on rules and policies.

f. Boundary filtering (a combination of multiple filtering capabilities) based on the policies and traffic characteristics. For example, boundary policies combine multiple filtering policies (e.g., IP layer and content filtering) into the overall policy for filtering traffic across a boundary (and may be implemented on one or more devices).

II - 4.1.1.2 BOUND-F Functional Requirements

This capability requires CDM tools and sensors to collect information about attributes in the OU and FISMA containers, the MDR (e.g., device categorization, filtering policies), the MUR (e.g.,

physical security training), and the MSR (e.g., boundary/interconnection between systems and the associated boundary filtering policies). This capability is related to PRIV, TRUST, CRED, and BEHAVE to support physical and logical access control decisions for access to facilities, systems, and information. This capability supports the Access Control, Data Security, Information Protection, and Protective Technology CSF Categories, all under the Protect CSF Function, the Asset Management CSF Category under the Identify CSF Function, and the Detection Process CSF Category under the Detect CSF Function.

BOUND_FR-1-1: Shall collect and report information related to the implementation of filtering policies at one or more levels in the protocol stack. This information shall support the enforcement of filtering policies. Information collected and reported on may consist of one or more of the following types:

a. Content filtering that directly filters traffic based on the application and application content. For example, the content is based on concepts understood at the application layer. Content filtering is described in terms of the applications (and the application characteristics) on which filtering can occur (e.g., URL filtering for HTTP content) and whether a proxy or translation is performed.

b. IP layer (packet) filtering that filters traffic based on the contents of IP layer protocols. Packet filtering is described in terms of what portions of the IP header are being used for the filtering decision and whether proxying or translation is being performed.

c. Layer 2 filtering that filters traffic at the data link layer, or layer 2, in the protocol stack. Layer 2 filtering is described in terms of which layer 2 protocol and what aspects of the protocol are being used for the filtering decision.

d. Encapsulation filtering that shows how data from one network protocol is translated into another network protocol so that the data can continue to flow across the network. Encapsulation filtering is described in terms of the encapsulation method and the traffic characteristics (e.g., IP header attributes, application, and packet content).

e. Network Access filtering that implements policy for permitting devices to connect to the network. Network Access filtering is described in terms of the types of devices the policy applies to, authentication method, and device characteristics used to make the connection decision.

f. Boundary filtering of policies to determine what traffic can flow, and what traffic is blocked across a boundary. A boundary filtering policy is of the set of filtering policies for a boundary, including metadata about that policy.

II - 4.1.1.3 BOUND-F Tool Functionalities

The following is a non-exclusive list of tool functionalities that support BOUND-F capability:

- Forward Web Proxies (or Secure Web Gateways)
- Reverse Web Proxies
- Web Application Firewalls
- Application Aware Firewalls (or Next Generation Firewalls)
- Email Security Gateways (or Secure Email Gateways)

- Database Firewalls
- Network Access Protection or Control Devices
- Intrusion Detection or Prevention Systems

II - 4.1.2 BOUND-E Requirements

The BOUND-E capability provides visibility into risks associated with the use of cryptographic mechanisms employed on an organization's network. Agencies use cryptography to protect credentials, data at rest, and data in motion.

BOUND-E provides the Agency indications of improper cryptographic behavior and/or of hardware/software misconfiguration. If cryptography is used, cryptography must be properly implemented and configured to provide the desired level of protection. BOUND-E collects policies from hardware devices, software products, and cryptographic implementation configuration settings to ensure that the right implementations are being used and configured properly.

The BOUND-E capability is further sub-divided into the following categories:

- Cryptography
  - Encryption Cryptography Technique
  - Hash Cryptography Technique
- Key Management/Certificate Authority (CA)
  - Key Management Design
  - Digital Signature Design
  - Certificate Authority Service

II - 4.1.2.1 BOUND-E Operational Requirements

BOUND_OR-2-1: Shall afford protection to the confidentiality, integrity, and authenticity of data at rest, in transit, or in process via cryptography.

BOUND_OR-2-2: Shall collect data associated with the boundary encryption policy and the encryption policy required for a network flow across a boundary to provide measurable data elements for the creation of automated security checks.

II - 4.1.2.2 BOUND-E Functional Requirements

This capability requires CDM tools and sensors to collect information when cryptography is used about attributes in the OU and FISMA containers, the MDR, the MUR, and the MSR. This capability is related to CRED if credentials employ cryptography. This capability is also related to HWAM, SWAM, and CSM if system components employ cryptography. This capability supports the Access Control, the Data Security, and the Protective Technology CSF Categories, all under the Protect CSF Function.

BOUND_FR-2-1: If applicable, shall collect and report information related to:

a. The use of U.S. government approved cryptographic algorithms as described in:

– Cryptographic Algorithm Validation Program (CAVP) http://csrc.nist.gov/groups/STM/cavp/standards.html

– NSA's Suite B Cryptographic Program https://www.nsa.gov/ia/programs/suiteb_cryptography/.

b. The use of one-way cryptographic hash techniques to ensure the integrity of data, that is, to detect the alteration of the data at rest or in transit. The hash technique maps an input field of arbitrary size to a unique output field of a fixed size. The hash value of a given data can be used to determine if the original data was modified. Hash can be applied to either plain text data or cipher text data. The hash technique ensures the integrity of data at rest and in transit, and under certain designs can be used to support data confidentiality (e.g., password hash).

c. An approved key management process for generating, distributing, using, and destroying cryptographic key material. Keys are used to support confidentiality, integrity, authenticity, and secure communication between multiple users. The application of keys includes digital certificates, protection against the disclosure of information, identification of when data is altered, and verification of the authenticity of the data source.

d. Digital certification to provide proof of identity and authenticity. A digital certificate associates a public key with an owner. It provides two benefits: proof of origin (i.e., authenticity) and that the information was not altered (i.e., integrity).

e. A CA that acts as a trusted third party to facilitate a secure communication between users over a PKI framework. Practical use of public key cryptography requires that whenever a relying party receives a public key said to be associated with an entity, someone or some organization that the relying party trusts musts have vouched for the fact that the key does indeed belong with that entity.

f. The use of cryptography in application layer protocols to ensure secure communication specifications for email communication, World Wide Web access, Domain Name Service (DNS) validation, and secure remote logins to computing systems and other applications.

g. The use of cryptography in transport protocols that are not application specific and do not have any in-depth knowledge of the application behavior. Rather, the transport protocol focus on the end-to-end connection between the communicating system, such as secure socket connection and connectionless communication.

h. Boundary cryptographic policies to determine what traffic can be encrypted/ decrypted/signed/hashed, and what traffic is blocked across a boundary. A boundary policy is the set of cryptographic policies for a boundary, including metadata about that policy.

II - 4.1.2.3 BOUND-E Tool Functionalities

The following is a non-exclusive list of tool functionalities that support BOUND-E capability:

- Email digital signing technique to identity of the sender of the email message
- Digital key management systems

- Network access authentication using digital certificates
- Certificate management (creation, issuing, and revocation) systems
- Email encryption to obfuscate the content of the email message (e.g., S/MIME encryption)
- DNS records signed using Domain Name System Security Protocol
- Secure remote logins (e.g., Secure Shell)
- Transport encryption at the link-layer (e.g., MACsec)
- Network-layer (e.g., IPSec) or transport-layer (e.g., Transport Layer Security [TLS], Datagram Transport Layer Security [DTLS]) security protocol used to protect data in transport across the network.

II - 4.1.3 BOUND-P Requirements

The BOUND-P capability ensures that personnel and vehicle access through a protected facility boundary is properly authenticated as required by policy, is properly authorized as required by policy, and the events are properly monitored. Physical Access Control Systems (PACS) are the underlying systems that provide policy rules and events to the BOUND-P services for electronically protecting facility access boundaries. “Properly authenticated” means that the individual presented FIPS 201 approved credentials and that a cryptographic validation was performed to verify that the individual is as represented. Credential validation uses only approved algorithms; ensures that cryptographic keys used are supplied by the approved key management system; and ensures that cryptography is applied utilizing the correct network security protocols at the correct layers within the protocol stack.

II - 4.1.3.1 BOUND-P Operational Requirements

BOUND_OR-3-1: Shall integrate with IP-addressable PACS components to support all CDM capabilities.

II - 4.1.3.2 BOUND-P Functional Requirements

This capability requires CDM tools and sensors to collect information about attributes in the OU and FISMA containers, the MDR, the MUR, and the MSR. This capability is related to CRED if credentials for physical access employ cryptography. This capability supports the Access Control CSF Category under the Protect CSF Function and the Detection Process CSF Category under the Detect CSF Function.

BOUND_FR-3-1: Shall collect and report information related to

a. Physical boundary authentication for providing identification and authentication of the person requesting access, as well as the validation requirements for identification/authentication. Boundary authentication is described in terms of the CDM Phase 2 CRED attributes, the authentication mechanism from FIPS 201 (e.g., Personal Identity Verification [PIV] + Biometric [BIO]), and the validation methods (e.g., Certificate Revocation List check) for the certificate attributes outlined for BOUND-E.

b. Boundary authorization to record and describe the policy for authorizing access to the controlled area. Boundary authorization records need to be described in terms of the

CDM Phase 2 CRED identity, attributes from the MUR (e.g., CDM Phase 2 BEHAV, TRUST, and/or PRIV attributes), environmental attributes (e.g., time of day), and/or previous boundary authorization actions.[5]

c. Physical boundary filtering policies determine what access for personnel or vehicles is allowed to a given space or facility. A physical boundary policy is the set of authentication and authorization policies for a boundary, including metadata about that policy.

II - 4.1.3.3 BOUND-P Tool Functionalities

The following is a non-exclusive list of tool functionalities that support this capability:

- Possession of a valid token
- Identification, authentication (e.g., token with Personal Identification Number)
- Identification, strong(er) authentication (e.g., biometrics)
- "Need-to-know" (e.g., group membership, security clearance) required
- Training/certification (e.g., physical security training specific to the area) required
- Movement between less trusted and more trusted areas incorporates previous access control decisions (e.g., moving to a Limited area from a Controlled area is granted only if access to the Controlled area has been granted previously and within a specified time)

II - 4.2 Manage Events (MNGEVT) Requirements

MNGEVT and OMI capabilities integrate to provide complementary processes and procedures to strengthen Agencies' security postures.

The MNGEVT capability provides the identification of security threat vectors, detection of security violation events, and classification of event impacts. MNGEVT utilizes an incident management system to report and share events with OMI.

The Phase 3 MNGEVT capability covers the following areas:

- Incident response
- Privacy
- Contingency planning
- Audit and accountability
- Ongoing assessment

[5] For example, access to a highly controlled area in a facility can be granted only if the same credential has already been granted access to the facility.

II - 4.2.1 MNGEVT Operational Requirements

II - 4.2.1.1 Incident Response

MNGEVT_OR_1-1: Shall have policies and procedures for the implementation of controls and processes to perform incident response.

MNGEVT_OR_1-2: Shall implement methods to perform incident response, which may include one or more of the following:

a. Tracking incident response processes and procedures managed and maintained by a configuration management repository system.
b. Monitoring incident response policies for an Agency network and infrastructure by the ongoing assessment of security policies.
c. Sharing and communicating incident response about cyber threat information to internal and external organizations.

II - 4.2.1.2 Privacy

MNGEVT_OR_2-1: Shall conduct security checks to verify that a privacy policy exists.

MNGEVT_OR_2-2: Shall notify data owners of data privacy breaches in accordance with Agency policies, applicable statutes, and regulations.

II - 4.2.1.3 Contingency Planning

MNGEVT_OR_3-1: Shall have a contingency plan to restore and reconstitute full information system functionalities and the capability to apply new or additional security safeguards to prevent future compromise.

MNGEVT_OR_3-2: Shall implement contingency capabilities/functions/methods that may include one or more of the following:

- Backup and restoration methods, frequency and storage of backups, types of data to be archived, and the ability to restore data from appropriate backup storage devices to satisfy the Agency recovery time and recovery point objectives for the system.
- Geographically dispersed storage facilities to ensure continuity in the event the primary site is no longer accessible.
- Encrypting backup data as part of data backup per Office of Management and Budget Memorandum M-11-11 and performing integrity checks of backup data.
- Prioritizing Agency systems from highest to lowest regarding recovery/reconstitution based on the Agency's Business Impact Analysis.

II - 4.2.1.4 Audit Data Collection

MNGEVT_OR_4-1: Shall have policies and procedures for the implementation of controls and processes to perform audit data collection.

MNGEVT_OR_4-2: Shall implement methods to perform audit data collection that may include one or more of the following:

a. Including operating system (OS) syslog, application log messages, system utilities monitoring logs, security activities log, abnormal application behavior, and network security activity logs.
b. Generating the following audit data:
    1. Appropriate audit data that can be used to support security assessment and forensic analysis.
    2. Audit records that meet regulatory requirements
    3. Audit records that include "Who (asset or entity)," "What (action)," "When," and "Where (target)" attributes of log messages
c. Providing integrity-protected and/or tamper-evident functionality to provide evidence when the audit log data is compromised in transit or at rest.
d. Providing audit and accountability data to report authorization and authentication activities related to personally identifiable information and protected critical infrastructure information access and disclosure.

II - 4.2.1.5 Ongoing Assessment

MNGEVT_OR-5-1: Shall provide ongoing assessment data consolidation and assessment frequencies to deliver an effective continuous collection, analysis, and impact assessment of security policies in order to maximize automation and reduce human interaction.

MNGEVT _OR-5-2: Shall complete the ongoing assessment activities so that mitigation responses and operational recovery can be completed to reduce threat propagation to other Agency information and information systems.

II - 4.2.2 MNGEVT Functional Requirements

II - 4.2.2.1 Incident Response Monitoring

This capability requires CDM tools and sensors to collect information about attributes in the OU and FISMA containers, the MDR, the MUR, the MSR, and the MIR. This capability is related to BEHAVE when behavior events related to incidents recorded in the MIR influence attribute values in the MUR. This capability supports the Detection Process CSF Category under the Detect CSF Function, the Asset Management CSF Category of the Identify CSF Function, and the Analysis CSF Category under the Respond CSF Function.

MNGEVT_FR-1-1: Shall collect and report information related to the implementation of methods to perform incident response and that enforce incident response policies. Information collected and reported may include one or more of the following:

a. Events and incidents related to malicious and/or anomalous activities that could impact the security posture of an Agency's network and infrastructure assets using data from HWAM, SWAM, CSM, VUL, and BOUND capabilities.
b. Initial analysis to determine incident severity based on the types of events, threat source, threat signatures, and impacted systems.

c. Workflow activities to maintain records for each incident, status of the incident, ability to annotate incident reports, and ability to request additional information that may be helpful in evaluating the incident from external system.
d. Complex aggregation and correlation algorithms using large volumes of stored data in a timely manner to generate incident reports.
e. Automated response to critical events based on severity and urgency by using an escalation technique to report the event.
f. Incident information (including analysis and alerts) aligned to incident response.

II - 4.2.2.2 Privacy Monitoring

For privacy, the MNGEVT incident response security is augmented by additional policy requirements related specifically to privacy information. MNGEVT privacy covers various processes and procedures, some of which are automated and some that must be manually performed. For privacy, the automated policies for an Agency network and infrastructure will be enforced by the ongoing assessment of privacy policies for defects, which will be used to enhance or add new NIST SP 800-53 privacy controls and countermeasures. This capability supports the Data Security CSF Category under the Protect CSF Function.

The CDM tools and sensors privacy information to be collected and relationship with CDM objects will be covered in CDM Phase 4.

MNGEVT_FR-2-1: Shall continuously monitor for events and incidents related to privacy.

II - 4.2.2.3 Contingency Planning Monitoring

This capability requires CDM tools and sensors to collect information about attributes in the OU and FISMA containers, the MDR, and the MIR (as related to the activation of contingency operations). This capability supports the Business Environment CSF Category under the Identify CSF Function and the Information Protection and Data Protection CSF Categories under the Protect CSF Function.

MNGEVT_FR-3-1: Shall collect and report information related to the implementation of capabilities/functions/methods for contingencies and that enforce contingency policies. Information collected and reported may include one or more of the following:

a. Backup operations related to contingency planning.
b. Actions to respond and recover from events in accordance with the contingency plan.

II - 4.2.2.4 Audit Data Collection

This capability requires CDM tools and sensors to collect information about attributes in the OU and FISMA containers, the MDR, and the MIR (as related to the incident data). This capability is related to CSM to ensure that auditing configurations are properly implemented on system components. This capability supports the Detection Process CSF Category under the Detect CSF Function and the Analysis CSF Category under the Respond CSF Function.

MNGEVT_FR-4-1: Shall collect and report information related to the implementation of methods to collect audit data and which enforce audit data collection policies. Information collected and reported may include one or more of the following:

a. Audit/logging information that supports review, analysis, and reporting
b. Audit/logging information in standard formats (e.g., syslog or Common Event Format) so that evaluation and correlation can be performed across multiple log sources.
c. Audit/logging information retention in a searchable, retrievable format for the appropriate timeframes according to retention policies and to support additional retrospective analysis.
d. Analysis and alerts for security policies aligned to audit and accountability
e. Integration of operational log-based and netflow sources.

II - 4.2.2.5 Ongoing Assessment Monitoring

This capability requires CDM tools and sensors to collect information about attributes in the OU and FISMA containers. Ongoing assessment will require information about the attributes associated with the MUR, MDR, and MSR. This capability supports the Detection Process CSF Category under the Detect CSF Function.

MNGEVT_FR_5-1: Shall monitor for changes to the data elements/attributes for all CDM capabilities and report changes to OMI capabilities in order to support ongoing authorization.

II - 4.2.2.6 MNGEVT Tool Functionalities

The following is a non-exclusive list of tool functionalities that support MNGEVT capability:

- Event-driven polling reporting approach
- Event-driven interrupt reporting approach
- Log management system
- Near real-time analytic
- Initial incident report generation
- Confidentiality of privacy data
- Data minimization and retention for privacy data
- Backup and restore method
- Agency recovery time objective/recovery point objective
- Forensic tools (e.g., file/registry/email analysis, disk capture)
- Network packet capture
- Forensic analysis tools

II - 4.3 Operate, Monitor and Improve (OMI) Requirements

OMI and MNGEVT capabilities integrate to provide complementary processes and procedures to strengthen agencies' security postures.

OMI focuses on the in-depth security root cause analysis, prioritization of security mitigation response/recovery, notification, and post-incident activity. OMI uses an incident report to share mitigation information with MNGEVT.

Ongoing Authorization dynamically monitors the security risk level using the results of MNGEVT ongoing assessment to detect when changing threats, vulnerabilities, technologies, and mission/business processes may result in an unacceptable security risk level.

Ongoing Authorization uses data from:

- The System and Information Integrity controls to assess the implementation efficacy of the NIST SP 800-53 controls to protect the Agency information and information systems.
- The Risk Assessment controls to dynamically assess the risk posture of the Agency information systems and if required, provide policy changes to MNGEVT.
- The Security and Assessment controls to identify vulnerabilities that could enable an attacker(s) to conduct malicious activities within an Agency's system. Once a vulnerability is identified by MNGEVT tools and sensors and it is determined that remediation is required, a Plan of Action and Milestones (POAM) will be developed to mitigate the vulnerability.

The products to support OMI capability must be able to enforce and update policies for all CDM tools and sensors.

The OMI capability covers the following areas:

- Ongoing Authorization
- System and Information Integrity
- Risk Assessment
- Security Assessment and Authorization

II - 4.3.1 OMI Operational Requirements

II - 4.3.1.1 Ongoing Authorization

OMI_OR-1-1: Shall provide a practical approach to perform reasonable assessment frequencies that will provide, consistent with Agency policy and maturity, continuous collection, analysis, and risk assessment of security-related policies on information and information systems using automation to limit human interaction.

OMI_OR-1-2: Shall complete the Ongoing Authorization risk assessment activities so that mitigation responses can be completed to reduce the potential lateral movement of threat propagation to other Agency information and information systems.

OMI_OR-1-3: Shall be used to ingest and export security authorization package information that includes POAMs, security plans, and security assessment reports to and from the appropriate internal and external stakeholders.

II - 4.3.1.2 System and Information Integrity

OMI_OR-2-1: Shall have policies and procedures for the implementation of controls and processes to maintain system and information integrity.

OMI_OR-2-2: Shall implement methods to maintain system and information integrity that may include one or more of the following:

a. Flaw remediation functionalities.

b. Recommended mitigating solutions appropriate to the required protection level for the system.
c. Detecting anomalous and suspicious network, system, application, and user behaviors (e.g., unauthorized access, modification or deletion of information, anomalous traffic/event patterns).

II - 4.3.1.3 Risk Assessment

OMI_OR-3-1: Shall have policies and procedures for the implementation of controls and processes to perform risk assessments for information systems.

OMI_OR-3-2: Shall implement methods to perform risk assessments that may include one or more of the following:

a. Dynamically assess the risk posture of its information systems and ensure that appropriate stakeholders participate in monitoring, assessing, and responding to risks against its information systems.
b. Determine which security controls need to be augmented or modified to maintain an acceptable level of risk.

II - 4.3.1.4 Security Assessment and Authorization

OMI_OR-4-1: Shall have policies and procedures for the implementation of controls and processes to perform security assessment and authorization for information systems.

OMI_OR-4-2: Shall implement methods to perform security assessment and authorization that may include one or more of the following:

a. Sharing security assessment results with authorizing officials and/or designated representatives in support of security authorization decisions.
b. Developing POAMs based on identified weaknesses and/or deficiencies and updating POAMs based on findings from security controls assessments, security impact analyses, and continuous monitoring activities.

II - 4.3.2 OMI Functional Requirements

II - 4.3.2.1 Ongoing Authorization

This capability requires CDM tools and sensors to collect information about attributes in the OU and FISMA containers. Ongoing authorization will require leveraging information about the attributes associated with the MUR, MDR, and MSR. This capability supports the Analysis and Mitigation CSF Category under the Respond CSF Function.

OMI_FR-1-1: Shall monitor (and report) the overall risk score for information systems, taking into consideration the presence of mitigations and countermeasures (e.g., POAM, compensating controls/processes), comparing that score with objective and threshold risk scores to support Ongoing Authorization decisions.

II - 4.3.2.2 System and Information Integrity

This capability requires CDM tools and sensors to collect information about attributes in the MDR. This capability is related to HWAM, SWAM, and CSM in that hardware inventory, software inventory, and configuration settings are components of system and information integrity that need to be maintained. Remediation actions will require CDM tools and sensors to collect information about attributes in the MIR. This capability supports the Information Protection, Maintenance and Protection Technology CSF Categories under the Protect CSF Function, the Detection Process CSF Category under the Detect CSF Function, and the Analysis and Mitigation CSF Categories under the Respond CSF Function.

OMI_FR-2-1: Shall collect and report information related to the implementation of methods to maintain system and information integrity and enforce system and information integrity policies. Information collected and reported may include one or more of the following:

a. Security posture changes or changes that affect the efficacy of NIST SP 800-53 security controls and countermeasures to mitigate component weaknesses and vulnerabilities for system and information integrity.
b. Vulnerability and threat remediation through response and recovery actions using automation to limit human interaction.
c. Protections from malicious code, actions, and threats and mitigation implementation when threats or malicious activities have exploited vulnerable conditions using automation to limit human interaction.
d. Incident information (including analysis and alerts) aligned to system and information integrity and integrating security and operational functionalities to support event response, including flaw remediation and incident management.

II - 4.3.2.3 Risk Assessment

This capability will require CDM tools and sensors to collect information about attributes in the MDR, MUR, MSR, and MIR to use with risk scores developed per C_Group-OR-1-2 (section II - 1.6) using the FISMA and OU context of the information system. This capability supports the Risk Assessment and Risk Management CSF Category under the Identify CSF Function and the Analysis CSF Category under the Respond CSF Function.

OMI_FR-3-1: Shall collect and report information related to the implementation of methods to perform risk assessments and that enforce risk assessment policies. Information collected and reported may include one or more of the following:

a. Continuously monitoring for incidents to support the categorization of systems, applications, and data sensitivity as well as the impact on mission essential/business functions within the Agency.
b. Integration with VUL and DBS to include the results of vulnerability scans in risk assessment decisions.
c. Incident information (including analysis and alerts) aligned to risk assessment.

II - 4.3.2.4 Security Assessment and Authorization

This capability requires CDM tools and sensors to collect information about attributes primarily in the OU and FISMA containers. System interconnections will require information about the attributes related to the CSM components associated with the MDR and MSR. Any information related to incidents requires CDM tools and sensors to collect information about attributes in the MIR. This capability supports the Analysis, Improvements, and Mitigation CSF Categories under the Respond CSF Function and the Recovery Plans and Improvements CSF Categories under the Recover CSF Function.

OMI_FR-4-1: Shall collect and report information related to the implementation of methods to perform security assessment and authorization and enforce security assessment and authorization policies. Information collected and reported may be related to one or more of the following activities:

a. Identifying internal and external system interconnections that match those requiring BOUND filtering policies.
b. Developing plans of action for mitigation and remediation of security policy defects that cause unacceptable levels of risk. This may include authorized workflows to identify and execute response and recovery actions.
c. Performing trend analysis of continuous monitoring data to identify systemic trends in risk posture changes.
d. Analyzing and alerting on security policies aligned to security assessment and authorization.

II - 4.3.2.5 OMI Tool Functionalities

The following is a non-exclusive list of tool functionalities that support OMI capability:

- Anomalous behavior detection (e.g., Netflow analysis)
- Patch (OS and application) management system for flaw mitigation
- Impact (including function, information, and mission/business) analysis tools
- Advanced analysis and visualization tools to identify response and recovery actions
- Mission essential/business function cyber dependency mapping (Business Impact Analysis)
- Threat intelligence feeds for Risk Assessment
- Security testing tools to support Risk Assessment

II - 4.4 Design and Build in Security (DBS) Requirements

The DBS capability addresses software acquired or newly developed to ensure that security is built in during all stages of the System Development Lifecycle (SDLC). DBS and the SCRM concepts are used to reduce the attack surface for network and infrastructure components in the Design, Development, and Deployment areas of the system component SDLC.

“DBS Design” means to design the system components that will be used for this system. “DBS Development” addresses the use of that development environment (i.e., it covers the system

development). “DBS Deployment” covers how agencies verify that the installed and running system is as it was designed and developed (i.e., that nothing has been changed or omitted).

The DBS Design area focuses on identifying and establishing motivation and goals for information and information system security needs. This includes assessing the environment risk posture and the design to mitigate those risks. Assessing the risk posture in the DBS Design area requires defining the security Concept of Operations (CONOPS) related to the business or mission needs, risk analysis, and assessment in order to identify potential weaknesses and vulnerabilities, and mandated policies related to regulation, governance, and compliance. This will enable the security architect to initiate a design that can incorporate appropriate security safeguards.

The DBS Development area focuses on developing and testing the information system to ensure that information system security needs are implemented effectively. This includes implementing secure coding practices, and identifying and addressing security weaknesses and vulnerabilities. Secure coding practices include fail-safe coding, critical code review, and secure code re-use. Weaknesses and vulnerabilities in this area are identified using a variety of testing methods on both source and compiled code. The Development area of the SDLC incorporates configuration and version management to track and minimize the introduction of errors (weaknesses and vulnerabilities) into information systems. Weakness and vulnerability testing supports the ability to identify and remediate errors that are introduced during the development of information systems.

The DBS Deployment area focuses on verifying that information system security needs have been met, to include the provenance of system components, securely deploying the information system, and maintaining the security control updates of the information system during operation. Securely deploying the information system in this area requires that the system installation is performed in a secure manner and that the information system is hardened (using secure configuration baselines). Maintaining information security in this area requires continuously monitoring the security posture of the information system and applying patches to mitigate vulnerabilities. The Deployment area of the SDLC incorporates release management to ensure that only versions of information system components that have properly completed development are deployed. Secure configuration baselines are developed and maintained to support secure installation and operation.

The SCRM area focuses on acquisition activities to help ensure that security goals are established and monitored. Such activities include sourcing of software, software purchase, mitigation of counterfeits, reputation scoring, and chain of custody.

II - 4.4.1 DBS Operational Requirements

II - 4.4.1.1 DBS Design

DBS_OR-1-1: Should identify relevant regulations, governance processes, compliance polices, and security CONOPS that malicious actors could exercise to compromise the information and information system, and perform risk assessment to evaluate impact to information and information systems.

DBS_OR-1-2: Should implement methods to minimize vulnerabilities or weakness during information system design activities, which may include one or more of the following:

a. Optimizing information system security using threat modeling to identify objectives and vulnerabilities and define countermeasures to prevent and mitigate the effects of threats to the system.
b. Using techniques to identify and eliminate available avenues of attack to information systems.
c. Implementing secure architecture and defense-in-depth design principles to ensure that security and software robustness are built in throughout the SDLC, preventing single points of failure in security mechanisms for the information system.

II - 4.4.1.2 DBS Development

DBS_OR-2-1: Should implement secure coding practices (including fail-safe coding, critical code and data protection, and secure code re-use) during information system development, which may include one or more of the following:

a. Implementing robust configuration, change, and version management during information system development.
b. Implementing the appropriate spectrum of testing (e.g., blackbox, whitebox, penetration, misuse case, dynamic and static analysis) to identify weaknesses and vulnerabilities during information system development (including scripts, batch files, and "applications" that are unique to the Agency).

II - 4.4.1.3 DBS Deployment

DBS_OR-3-1: Should execute secure acquisition (e.g., verify procurement supply chain, chain-of-custody) and disposal of components and data as part of information system deployment, which may include one or more of the following:

a. Implementing robust release management (including patches and security patches) as part of information system deployment.
b. Implementing secure installation principles (including hardening of systems and applications) as part of information system deployment.
c. Implementing methods to instrument and monitor runtime execution and track problems as part of information system deployment.
d. Implementing digital signing of software and signature verification to ensure the authenticity (provenance and integrity) of software components.[6]

II - 4.4.1.4 SCRM

DBS_OR-4-1: Should follow SCRM policies and procedures for baselining, tracking, and auditing the provenance of information system components (to include mitigation of counterfeits, reputation scoring, and chain of custody) for the acquisition/development of the information system.

[6] Implementing digital signing and signature verification of software will require that additional attributes related to the certificate information of the signer (using the appropriate attribute information from BOUND-E) be collected by CDM Phase 1 SWAM (in addition to other provenance and reputation attributes about the software).

DBS_OR-4-2: SCRM should be an integral part of the overall risk management process and include risk assessment guidance and the use of security related controls to mitigate identified risk.

DBS_OR-4-3: SCRM should establish a process for identifying, preventing, assessing, reporting and mitigating the risks associated with the global and distributed nature of CDM product and service supply chains. The range of countermeasures selected should include appropriate risk reduction strategies and the best way to implement them.

II - 4.4.2 DBS Functional Requirements

II - 4.4.2.1 DBS Design

This capability will require CDM tools and sensors to collect information about attributes in the FISMA containers. This capability is related to VUL attributes related to the software components associated with the MDR and adds provenance of information system components to SWAM attributes. This capability supports the Risk Assessment and Risk Management CSF Categories under the Identify CSF Function.

DBS_FR-1-1: Shall collect and report information related to the implementation of modeling threats to information systems, including identifying vulnerabilities and corresponding countermeasures. Information collected and reported may be related to one or more of the following activities:

a. Identifying the possible attack surface of information systems.
b. Managing system/software security design and development requirements.

II - 4.4.2.2 DBS Development

This capability will require CDM tools and sensors to collect information about attributes in the FISMA containers. This capability is related to VUL attributes related to the software components associated with the MDR and adds provenance of information system components to SWAM attributes. This capability supports the Business Environment and Risk Assessment CSF Categories under the Identify CSF Functions.

DBS_FR-2-1: Shall collect and report information related to the implementation of methods for secure information system development and enforce secure information system development policies. Information collected and reported may be related to one or more of the following activities:

a. Configuration management, change control, and versioning for information system security artifact development.
b. Testing for weaknesses and vulnerabilities in information systems. These vulnerabilities should include those identified by the VUL capability.

II - 4.4.2.3 DBS Deployment

This capability requires CDM tools and sensors to collect information about attributes in the FISMA container and MDR. This capability is related to CSM where the initial configuration at deployment of the system and after system update become part of the baselines and benchmarks for CSM. This capability also is related to SWAM and CSM for releases and patches to update

information about the SWAM and CSM attributes related to the software components associated with the MDR. This capability supports the Risk Assessment CSF Category under the Identify CSF Function and the Analysis CSF Category under the Respond CSF Function.

DBS_FR-3-1: Shall collect and report information related to the implementation of methods for secure information system deployment and enforce secure information system deployment policies. Information collected and reported may be related to one or more of the following activities:

a. Managing releases and patches for information systems.
b. Developing and maintaining secure configuration baselines for information systems and information system components.
c. Instrumenting and monitoring information systems at runtime.
d. Tracking problems associated with information systems at runtime.
e. Digitally signing software before deployment.[7]

II - 4.4.2.4 DBS Tool Functionalities

The following is a non-exclusive list of tool functionalities that support the above DBS functional requirements:

- Application analysis for Common Weakness Enumerations (CWEs)
- Vulnerability scanners for CVEs
- Requirements change management and traceability tools
- Version and change control system
- Blackbox/whitebox/penetration testing
- Static/dynamic code analysis
- Patch management tools
- Deployment and release management tools
- Attack surface mapping and analysis tools
- Hardening operating system tools
- Problem tracking tools
- Software signing tools

[7] Implementing digital signing of software will require that additional attributes related to the certificate information of the signer (using the appropriate attribute information from BOUND-E) be collected by CDM Phase 1 SWAM (in addition to other provenance and reputation attributes about the software).

III - References

1. Continuous Diagnostics and Mitigation (CDM) System Architecture: Architecture Principles Document, Version 0.5, August 31, 2016
2. Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, February 12, 2014
3. Phase 1: Attachment N Requirements, Section 9
4. Phase 2: Attachment N-2 Requirements, February 12, 2015
5. Phase 3: Attachment N-3-BOUND Requirements, 2nd Issue November 15, 2016
6. Phase 3: Attachment N-3-Manage Events Requirements, June 7, 2016
7. Phase 3: Attachment N-3-Operate, Monitor and Improve, August 5, 2016
8. Phase 3: Attachment N-3-Design and Build in Security, September 16, 2016
9. Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (draft), January 10, 2017
10. NIST SP 800-53, https://nvd.nist.gov/800-53/Rev4/
11. Security Requirements for Cryptographic Modules, FIPS 140-2, May 25, 2001, http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf
12. Standards for Security Categorization of Federal Information and Information Systems, FIPS 199, February 2004, http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf
13. Common Platform Enumeration (CPE) https://nvd.nist.gov/products/cpe
14. Common Configuration Enumeration (CCE) https://nvd.nist.gov/config/cce/index
15. Common Vulnerability Enumeration (CVE) https://nvd.nist.gov/vuln/search
16. NISTIR 7502 The Common Configuration Scoring System (CCSS): Metrics for Software Security Configuration Vulnerabilities, December 2010, http://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7502.pdf
17. National Vulnerability Database (NVD) https://nvd.nist.gov/
18. Common Vulnerability Scoring System CVSS https://nvd.nist.gov/vuln-metrics/cvss
19. Federated Identity, Credential, and Access Management (FICAM) https://www.idmanagement.gov/IDM/s/article_content_old?tag=a0Gt0000000XNYG
20. Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks (X.509 ITU-T) http://www.itu.int/rec/T-REC-X.509/en
21. Personal Identity Verification (PIV) of Federal Employees and Contractors, FIPS 201-2, August 2013, http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf
22. Common Weakness Enumeration (CWE) https://nvd.nist.gov/vuln/categories
23. HPE Security ArcSight Common Event Format, version 23, May 16, 2016
24. Security Content Automation Protocol (SCAP) https://scap.nist.gov/

IV - Appendix A: Acronyms, Terms and Definitions

Acronym	Term	Definition
	Attributes	A set of labels, values, and hierarchies that describe a characteristic or dimension of a CDM object.
	Attribute Values	A list of possible value assignments or types for an attribute.
	BOUND	BOUND provides boundary protection for the interior of the network from all interconnections to other external networks.
	Data Element	A piece of information about CDM objects, their attributes, and/or associated policy to support the identification of defects.
	CDM Dashboard	The tool that aggregates and displays CDM information at the Agency or Federal level. The dashboard provides consistent, timely, targeted, and prioritized information to security decision makers from cross-agency and Federal-level managers to systems administrators to identify and support fixing the worst problems first.
AC	Access Control	This family of controls addresses the ability to allow authorized subjects to gain access to system resources and data, and to prevent all other accesses.
AT	Awareness and Training	This family of controls addresses that system designers, administrators, operators, and users have the appropriate awareness and training to securely perform their roles.
AU	Audit and Accountability	This family of controls addresses the ability to record actions that occur in the system, to analyze those records, and to correctly attribute each action to the entity that caused it to happen.
BEHAVE	Manage Security-Related Behavior	The BEHAVE capability ensures that authorized users with or without special security responsibilities exhibit the appropriate behavior for their role.

Acronym	Term	Definition
CA	Security Assessment and Authorization	This family of controls addresses the steps involved in authorizing a system to operate under specific conditions in a specific environment with a defined and acceptable level of risk.
CDM	Continuous Diagnostics and Mitigation	Provides Federal Departments and Agencies with capabilities and tools that identify cybersecurity risks on an ongoing basis, prioritize these risks based upon potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first. Congress established the CDM program to provide adequate, risk-based, and cost-effective cybersecurity and allocate cybersecurity resources more efficiently.
CM	Configuration Management	This family of controls addresses the steps involved in understanding and controlling the components of a system and how those components are configured.
CMaaS	Continuous Monitoring as a Service	The collection of elements that are not in the scope of the Dashboard.
CP	Contingency Planning	This family of controls addresses whether the system can operate and carry out its mission despite any defined set of events that may occur.
CRED	Credentials and Authentication Management	The CRED capability ensures that only proper credentials are authenticated to systems, services, and facilities.
CSF	Cybersecurity Framework	OMB Memorandum 16-03, “Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements,” calls out the federal adoption of the NIST Cybersecurity Framework (CSF) for improving critical infrastructure cybersecurity.
CSM	Configuration Settings Management	CSM ensures that authorized security configuration benchmarks exist and contain acceptable value(s) for each relevant configurable setting for each IT asset type.
CVE	Common Vulnerability Enumeration	A dictionary of common names (i.e., CVE Identifiers) for publicly known cybersecurity vulnerabilities.

Acronym	Term	Definition
CVSS	Common Vulnerability Scoring System	CVSS provides an open framework for communicating the characteristics and impacts of IT vulnerabilities.
CWE	Common Weakness Enumeration	The CWE Specification provides a common language for discussing, finding, and dealing with the causes of software security vulnerabilities found in code, design, or system architecture.
DBS	Design and Build in Security	Describes preventing exploitable vulnerabilities from being effective in the software/system while in development or deployment.
DHS	Department of Homeland Security	Federal Agency whose missions include preventing terrorism and enhancing security; managing our borders; administering immigration laws; securing cyberspace; and ensuring disaster resilience.
FISMA	Federal Information SecurityModernization Act 2014	The U.S. legislation that defines a comprehensive framework to protect Government information, operations and assets against natural or man-made threats. FISMA was signed into law part of the Electronic Government Act of 2002. [2014 Act changed Management to Modernization.]
HWAM	Hardware Asset Management	The HWAM Function is to discover unauthorized or unmanaged hardware on a network.
IA	Identification and Authentication	This family of controls addresses knowing who or what each entity in the system is and on whose behalf, it is operating.
IR	Incident Response	This family of controls addresses how the organization will respond to a security incident that occurs during operation.
IT	Information Technology	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency.

Acronym	Term	Definition
MA	Maintenance	This family of controls addresses events that occur in ensuring that the system is operating correctly, is updated when needed, and can be repaired with minimal security impact when a problem does occur.
MDR	Mater Device Record	A set of attributes or assertions about a user, with the device as the primary key.
MIR	Master Incident Record	Represents activities associated with security controls that require an action when an event occurs; deals with “what is happening on the network?”
MNGEVT	Manage Events	Describes preparing for events/incidents, gathering appropriate data from appropriate sources, and identifying incidents through analysis of data.
MP	Media Protection	This family of controls addresses the creation, management, distribution, storage, and disposal of electromagnetic or optical storage media.
MSR	Master System Record	A set of attributes or assertions about a user, with the system as the primary key.
MUR	Master User Record	A set of attributes or assertions about a user, with the user as the primary key.
NIST	National Institute of Standards and Technology	The Federal technology Agency that works with industry to develop and apply technology, measurements, and standards.
OMB	Office of Management and Budget	OMB is the business division of the Executive Office of the President of the United States that administers the United States federal budget and oversees the performance of federal agencies.
OMI	Operate, Monitor and Improve	Describes audit data collection and analysis, incident prioritization and response, and post-incident activities (e.g., information sharing).
OU	Organizational Unit	The Government Department or Agency responsible for the information system.

Acronym	Term	Definition
PACS	Physical Access Control System	An automated system that manages the passage of people or assets through an opening(s) in a secure perimeter(s) based on a set of authorization rules.
PDP	Policy Decision Point	Repository for policies that are distributed to enforcement points; mediates or de-conflicts DPs per MPs in some implementations.
PE	Physical and Environmental Protection	This family of controls addresses the controlling of the spaces in which system components operate, to ensure that components cannot be accessed, modified, replaced, stolen, or removed in a manner that would violate security policy.
PEP	Policy Enforcement Point	A service that resides on and directly interacts with network objects (e.g., servers, asset scanners, firewalls), which exchanges policy-related messages with the Policy Decision Point. The PEP enforces organizational policy via the configuration applied to the object.
PL	Planning	This family of controls addresses the organization's security plans. Factors include how the plan is developed; contents of the plan; and the plan's impact on security, privacy, and organizational operations.
PRIV	Managing Account Access Capability	This CDM capability is to provide an agency the assurance that users and systems have access to, and control of, only the appropriate resources. The capability identifies access beyond what is needed to meet business requirements.
PS	Personnel Security	This family of controls addresses vetting of the authorized organizational users of the system and system components.
RA	Risk Assessment	This family of controls addresses that the development, deployment, and operation of the system is controlled by and is compatible with the organization's overall risk assessment process.
RMF	Risk Management Framework	A structured approach used to oversee and manage risk for an enterprise.
SA	System and Services Acquisition	This family of controls addresses how the organization acquires and operates the system.

Acronym	Term	Definition
SC	System and Communications Protection	This family of controls addresses how the system is designed and operated to detect and defeat attempted attacks.
SCRM	Supply Chain Risk Management	The process of identifying, assessing, and mitigating the risks associated with the distributed and interconnected nature of IT/operational technology (OT) product and service supply chains. It covers the entire life cycle of a system (including design, development, distribution, deployment, acquisition, maintenance, and destruction), as supply chain threats and vulnerabilities may intentionally or unintentionally compromise an IT/OT product or service at any stage.
SDLC	System Development Life Cycle	The process of planning, creating, testing, and deploying an information system. The SDLC concept applies to a range of hardware and software configurations, as a system can be composed of hardware only, software only, or a combination of both.
SI	System and Information Integrity	This family of controls addresses protecting the system from attacks using malicious code; monitoring system behavior to detect flaws or attacks; and acting to remediate the situation when a flaw or attack is detected.
SP	Special Publication	NIST Special Publications that include SP 800 subseries (computer security), SP 1800 subseries (NIST Cybersecurity Practice Guides) and selected SP 500-series (information technology) publications directly relevant to computer/cyber/information security and privacy
SWAM	Software Asset Management	The SWAM Function is to discover unauthorized or unmanaged software on a network.
TFA	Tool Functional Area	DHS is implementing the CDM program, made up of 15 BPA TFAs, that addresses “what is on the network,” “who is on the network,” and “what is happening on the network.”
TRUST	Manage Trust in People Granted Access Capability	This CDM capability assesses the inherent risk to an Agency from insider attacks for the purposes of granting trust to users and authorizing each user for certain attributes.

Acronym	Term	Definition
USB	Universal Serial Bus	An industry standard for connecting devices to computers.
VUL	Vulnerability Management	The VUL Function is to discover and support remediation of vulnerabilities in IT assets on a network as defined in NIST SP 800-53 controls.