GSA's Email Records Management Policy and Technology Architecture

- Federal agencies are required to manage their email records in accordance with the Federal Records Act, 36 CFR Chapter XII Sub-chapter B, Office of Management and Budget *Memorandum M-12-18, Managing Government Records, and* NARA Capstone Guidance *(NARA Bulletin 2013-2).*

- In an effort to help agencies manage and store the government's email records, NARA developed the Capstone approach to managing emails.

- This approach was developed in recognition of the difficulty in practicing traditional records management on the overwhelming volume of email that Federal agencies produce and is designed to provide them with feasible solutions to email records management challenges, especially as they implement cloud-based solutions.

- According to NARA, Capstone offers agencies the option of using a more simplified and automated approach to managing emails.

- Currently, agencies are implementing the Capstone approach to email record management in order to meet the President's Management Agenda goal of eliminating paper records by December 21, 2022.

- GSA uses Google's G Suite Business package of services which is designed to provide users with unlimited storage for Gmail messages, Google Photos, and files in Google Drive and Archiving storage in the Google Vault.

- According to Google, its Vault retains, archives, searches, and exports an organization's data for eDiscovery and compliance needs.

- As of today, GSA employees are required to comply with the email record keeping policies contained in *CIO 2160.2B CHGE 1, Electronic Messaging and Related Services, June 17, 2015 and GSA Order 1828.1 OAS Email Records Management Policy.*

- GSA's email policy implements the NARA Capstone guidance and describes how the agency makes determinations about email retention and disposal based on employee roles and responsibilities rather than on the content of each email record so it does not provide any instructions on how employees should manage email records.

- Instead the Office of the Chief Information Officer stores all of GSA's emails in the Google Vault and assigns a retention period based on an employee's role at the agency.

- However, *CIO 2160.2B CHGE 1 June 17, 2015, Electronic Messaging and Related Services, Number 10, Record keeping of email messages,* says that authorized email users are responsible for maintaining their email records within assigned storage limitations and NARA records management requirements so they are advised to apply the same decision-making process to e-mail for records maintenance and disposition that they apply to other documentary materials, regardless of the media used to create them, and store them accordingly.

- Because NARA requires email records to be stored in official records systems and the GSA Gmail system isn't an official system, the policy requires employees to identify email records and move them to a NARA-approved document management system—for example, a shared network drive, or the user's workstation.

- So right now, the agency is operating under two different email record management policies that could be construed as conflicting with one another. The first one doesn't require employees to manage emails according to records management rules for paper records and the other one does.

- And, even though NARA rules allow agencies to remove transitory, non-record, or personal email messages from their email storage systems either manually or through automated procedures, GSA's Google Vault contains GSA's non-records because the agency doesn't allow employees to delete materials.

- In 2013, NARA moved its email data onto the cloud using the G Suite package of services which includes Gmail, and applied a technology solution called ZL Unified Archive to it to allow the agency to comply with its Capstone email management rules.

- After it completed the migration, the agency posted instructional materials on its website that describe how NARA manages email records in the cloud and how agency end-users should use the system to manage email records.

- The NARA End User Guide outlines how the ZL Archive technology provides an automated mechanism for managing email record archiving by managing all aspects of record declaration, categorization and disposition without requiring end –users to take any actions. In addition, the technology provides an option for end-users to mark emails as records and categorize them into a file plan.

- The Gmail/ZL Archive system provides litigation support by allowing employees to manage legal holds, and search across billions of documents in seconds and produces emails and files in native format but also supports seamless conversions of emails between multiple formats.

- If all of the above is accurate, those technological capabilities would benefit the FOIA program which spends considerable time waiting for IT to pull data from the Vault and then the FOIA staff spends time converting the data into a usable format so they are able to redact it.

- If FOIA staff were able to conduct the FOIA related email searches from their own workstations, we would be able to make the FOIA process more efficient and GSA could eliminate spending on eDiscovery contractors.

- The NARA Email End Users Guide and other related materials can be accessed by clicking on the following link- https://www.archives.gov/records-mgmt/email-management/sample-agency-implementation-on-capstone.html

Conclusion

Currently, GSA email records management policy is requiring employees to comply with NARA guidance through two conflicting email management policies. One doesn't require employees to manage emails according to records management rules for paper records and the other one does. GSA should determine which set of policies it wants to use to manage email records, and update its policies accordingly. If GSA determines it wants to allow end-users to tag email records the same way employees will be tagging electronic documents using the Alfresco system for items that will be stored in the Electronic Document Management System repository, staff should review the NARA email management documents posted on the agency's website.

The technology GSA uses to store its email records, the Google Vault, contains all of the agency's records plus every employees' transitory, non-records and personal emails because the agency doesn't delete them. This means that FOIA Google Vault data pulls generate non-records and personal emails which may, in some circumstances, be released to the public, unless all or part of the content meets one of the nine FOIA exemptions. The Office of General Counsel also pulls data from the Google Vault.

If GSA decides to use the NARA email management model the Office of Accountability and Transparency is prepared to support that effort by developing all of the necessary employee training and communication messages.

OFFICE OF THE INSPECTOR GENERAL OF THE INTELLIGENCE COMMUNITY

Approved for Public Release
ODNI/IMD 13 Nov 2018

(U) Assessment of IC Freedom of Information Act (FOIA) Programs

September 28, 2018 **Report INS-2018-001**

~~*(U) This report contains information that the Office of the Inspector General of the Intelligence Community has determined is confidential, sensitive, or protected by Federal Law, including protection from public disclosure under the Freedom of Information Act (FOIA), 5 U.S.C. § 552. Recipients may not further disseminate this information without the express permission of the Office of the Inspector General of the Intelligence Community personnel. Accordingly, the use, dissemination, distribution, or reproduction of this information to or by unauthorized or unintended recipients may be unlawful. Persons disclosing this information publicly or to others not having an official need to know are subject to possible administrative, civil, and/or criminal penalties. This report should be safeguarded to prevent improper disclosure at all times. Authorized recipients who receive requests to release this report should refer the requestor to the Office of the Inspector General of the Intelligence Community.*~~

TABLE OF CONTENTS

(U) Executive Summary **4**
(U) Introduction **5**
(U) Methodology **6**
(U) Roles and Responsibilities **7**
(U) Department of Justice, Office of Information Policy 7
(U) National Archives and Records Administration Office, Office of Government Information Services 7
(U) Chief FOIA Officers Council 7
(U) Intelligence Community 8
(U) Simplified Overview of FOIA Processing 8
(U) Assessment Results **9**
(U) Finding 1: ODNI has not fully exercised its leadership responsibility to foster integration and collaboration to improve IC execution of FOIA. 9
(U) Finding 1.1: ODNI IMD did not implement the FOIA improvement plan briefed to the EXCOM in 2016. 10
(U//~~FOUO~~) Finding 1.2: The IC is not making use of all available technology to support FOIA programs, and there is no consolidated IC-wide approach to technology application. 11
(U) Finding 1.3: ODNI's Difficult Issues Forum has not met since 2015 and there is no regular IC-wide group to address ongoing IC FOIA issues. 13
(U) Finding 1.4: ODNI has not engaged with OIP on IC-wide FOIA issues. 13
(U) Finding 1.5: ODNI has not had discussions with OGIS on strategic IC-wide FOIA issues, access concerns, or challenges with the Act. 14
(U) Finding 2: IC Element FOIA programs are pursuing initiatives to improve effectiveness but are not consistently meeting statutory response deadlines. 16
(U) Observation 2.1: Between FY16 and FY17, all IC Element FOIA programs reduced average processing times for simple requests while changes in processing times for complex cases varied. .. 17
(U) Observation 2.2: IC Element FOIA programs have focused efforts to close their oldest cases. ... 18
(U) Finding 2.1: All IC FOIA programs report backlogs but not all have current backlog plans. 19
(U) Finding 2.2: Consultations are a significant cause of processing delays and the IC does not have an established process or guidance for consultations. 21
(U) Finding 2.3: Chief FOIA Officers are reviewing programs annually but have not made recommendations for improvements to IC FOIA programs to the heads of their agencies. 23
(U) Finding 3: IC Element FOIA programs have various approaches to communicating with requesters but could further increase transparency. 24

(U) Observation 3.1: IC FOIA programs are proactively engaging with requesters by telephone, email, or letter. 25

(U) Observation 3.2: IC Element FOIA programs are not routinely providing information to the public about the types of records they maintain on their website in part due to national security restrictions.26

(U) Observation 3.3: NGA has posted few frequently requested documents to its public website. 26

(U) Observation 3.4: The IC FOIA programs are proactively disclosing information to the public, but implementation challenges exist to routine posting of FOIA released documents to websites. 27

(U) Observation 3.5: Some IC FOIA programs have implemented the Release to One, Release to All draft policy. 27

(U) Observation 3.6: IC FOIA programs could more effectively use their websites to educate the public by providing a description of their various FOIA processing tracks and average response times. 28

(U) Commendable 1: NRO conducted a survey of its FOIA requesters to solicit feedback. 29

(U) Finding 3.1: The IC has not strategically evaluated the effect of IC initiated proactive review and release initiatives on FOIA programs. 29

(U//~~FOUO~~) Finding 4: The IC has mechanisms in place to reduce the likelihood of inconsistent FOIA release determinations. 30

(U) Observation 4.1: ODNI's 2016 FOIA Improvement Plan includes recommendations that should mitigate the chances inconsistent FOIA release determinations occur. 31

(U) Appendix A: Acronyms List 32

(U) Appendix A: Acronyms List Continued 33

(U) Appendix B: Comments 34

(U) Appendix C: Summary of FOIA Exemptions 35

(U) Appendix D: Summary of Recommendations 36

(U) EXECUTIVE SUMMARY

(U) *The Freedom of Information Act* (FOIA) is the primary means for the public to access federal executive branch records.[1] The Inspector General of the Intelligence Community (IC IG) Inspections & Evaluations Division (I&E) reviewed FOIA programs of the Central Intelligence Agency (CIA), Defense Intelligence Agency (DIA), National Geospatial-Intelligence Agency (NGA), National Reconnaissance Office (NRO), National Security Agency (NSA), and Office of the Director of National Intelligence (ODNI). We also reviewed ODNI's role as an IC-wide integrator. We initiated this assessment after determining that ODNI Information Management Division raised IC FOIA program concerns to the Executive Committee, its senior governance forum.

(U) I&E examined the effectiveness of the six IC elements' efforts to manage FOIA requests, with a focus on how programs prioritize, coordinate, and process requests to meet statutory requirements, including response timeliness and communications with requesters. We found that while CIA, DIA, and NSA receive more FOIA requests than ODNI, NGA, and NRO, all face similar challenges. Many common issues affecting these programs are outside the IC's control, such as increased volume and complexity of incoming requests, as well as demands from FOIA litigation. Internally, the IC's approach is inefficient. The programs are not supported by adequate technology, and there is a lack of structured processes for coordination of requests across agencies.

(U) We found that ODNI could do more to lead the collective IC FOIA enterprise. The statute gives responsibility to heads of departments and agencies to manage their own FOIA programs, so ODNI's IC-wide authority is limited. However, to date ODNI has not fully exercised its significant integration role, despite shared challenges. In particular, ODNI has not resolved persistent issues related to coordination of FOIA requests across IC elements. In addition, ODNI could improve planning of IC transparency initiated declassification reviews that have implications on FOIA programs across IC elements. In addition, ODNI has a responsibility to interact more with the key external governance organizations that publish guidance and make recommendations to Congress to increase their understanding of IC FOIA challenges.

(U) We also examined the conditions that contribute to inconsistent FOIA release determinations and the mechanisms to prevent inconsistent releases. We determined the IC has mechanisms in place to reduce the chance of inconsistent release decisions. Implementation of the recommendations in this report should mitigate the likelihood of inconsistent release decisions.

[1] (U) 5 U.S.C. § 552, as amended.

(U) INTRODUCTION

(U) The Inspector General of the Intelligence Community (IC IG) reviewed *Freedom of Information Act* programs of the following six Intelligence Community (IC) elements: Central Intelligence Agency (CIA); Defense Intelligence Agency (DIA); National Geospatial-Intelligence Agency (NGA); National Reconnaissance Office (NRO); National Security Agency (NSA); and the Office of the Director of National Intelligence (ODNI), collectively, the IC elements. We also reviewed ODNI's role as an IC-wide integrator. In this report, references to "IC FOIA programs" relate only to the six elements within the scope of this assessment.

(U) The *Freedom of Information Act* (hereafter "FOIA" or "the Act") is the primary means for the public to access federal executive branch records.[2] The Act allows any person, broadly defined to include attorneys filing on behalf of an individual, corporation, or organization, to file a request for records. Any member of the public may request access to information held by federal agencies without showing a need or reason for seeking the information.[3] Agencies within the Executive Branch of the federal government, independent regulatory agencies, and some components within the Executive Office of the President are subject to the Act. It is one of the most important means for citizens to obtain information about government activities.

(U) The objectives of this assessment were to:

- (U) Assess the effectiveness of each IC element's efforts to manage FOIA requests;
- (U) Describe the conditions that contribute to inconsistent FOIA release decisions and identify IC elements' mechanisms to help prevent or lessen the likelihood of inconsistent releases; and
- (U) Describe the conditions that contribute to inconsistent FOIA release decisions across the IC and identify IC-wide mechanisms to help ensure or strengthen consistent release decisions.[4]

(U) Our assessment covered Fiscal Years (FY) 2016 and 2017. The assessment did not address IC elements' application of particular FOIA exemptions in specific cases. Instead, we examined FOIA processes aimed at providing timely responses to requests. We also reviewed IC element mechanisms to ensure that release determinations for the same information are consistent. We identified mechanisms for ensuring consistent responses to FOIA requests within each IC element and across IC elements. We did not examine processes related to Privacy Act (PA) requests. We did not interview members of the public who are FOIA requesters, primarily due to concerns about interfering with FOIA cases that are in the process of ongoing litigation. However, we did review publicly available information related to our objectives, some of which was from the websites of FOIA requesters.

---

[2] (U) 5 U.S.C. § 552, as amended.

[3] (U) Requesters seeking a preferential FOIA fee category or expedited processing are asked to show a need or reason for seeking the records.

[4] (U) IC IG initially announced that objective 2 would focus on the effectiveness of each IC element's mechanisms to prevent inconsistent FOIA release determinations and objective 3 would assess the effectiveness of IC-wide mechanisms to ensure consistent FOIA release determinations across the IC. We revised objectives 2 and 3 when we learned through our field work that IC elements do not have the capability to identify all previous official releases that have occurred across the IC and that IC elements do not have their own measures of effectiveness related to consistent release determinations.

(U) METHODOLOGY

(U) To conduct this assessment, the IC IG interviewed officials from each of the six IC elements, including Chief FOIA Officers, FOIA Public Liaisons, FOIA professionals, transparency officers, and representatives from Offices of General Counsel. We also interviewed Department of Justice (DOJ) Office of Information Policy (OIP) and the National Archives and Records Administration (NARA) Office of Government Information Services (OGIS) officials. In addition, we spoke with Department of State (DOS) and Department of Homeland Security (DHS) FOIA officials. We reviewed IC element Office of Inspector General (OIG) reports on FOIA programs and discussed the status of recommendations with OIGs. We also reviewed each IC element's FOIA program annual reports and Chief FOIA Officer's report to OIP. We obtained a demonstration of the tools used to process FOIA requests.

(U) We asked IC element FOIA professionals to provide examples of what they considered inconsistent release determinations provided to FOIA requesters. Specifically, we requested examples of all documents programs had knowledge of that reflected an inconsistent FOIA release determination for the same information (e.g., information was withheld, same information was released). If programs were unable to locate the documents, but were aware of these instances, we asked that they provide a brief description. We also conducted open source research and if we uncovered examples of inconsistent release decisions, we discussed those examples with FOIA professionals in the IC FOIA programs.

(U) We conducted this assessment from February to September 2018 in accordance with the Council of the Inspectors General on Integrity and Efficiency 2012 Quality Standards for Inspection and Evaluation. We provided a draft of this report to each IC element. See Appendix 2 for official comments.

(U) This report includes 9 findings with 10 recommendations, 9 observations, and 1 commendable. Findings identify areas where we recommend action. Each finding has at least one recommendation the IC IG will monitor through completion. Observations are provided for situational awareness.

(U) Roles and Responsibilities

(U) Department of Justice, Office of Information Policy

(U) The OIP has government-wide statutory responsibility to encourage and oversee agency compliance with FOIA.[5] OIP develops and issues legal and policy guidance on FOIA implementation. All agencies are required to report to the Attorney General each year on their performance in implementing the FOIA and DOJ FOIA Guidelines.[6] [7] OIP establishes reporting requirements and assesses agency progress under FOIA. OIP also adjudicates administrative appeals of FOIA requests made to DOJ and handles the defense of certain FOIA litigation cases.[8]

(U) National Archives and Records Administration Office, Office of Government Information Services

(U) The *OPEN Government Act of 2007* created OGIS to review FOIA policies and agency compliance as well as to recommend ways to improve FOIA.[9] The Act requires OGIS to mediate disputes between FOIA requesters and federal agencies, review policies and procedures of administrative agencies under FOIA, review agency compliance with FOIA, and identify procedures and methods for improving compliance, including through legislative and regulatory recommendations. In addition, OGIS provides administrative and logistical support for the FOIA Advisory Committee (FAC). The FAC advises on improvements to the administration of FOIA and makes recommendations to the Archivist of the United States.

(U) Chief FOIA Officers Council

(U) The *FOIA Improvement Act of 2016* established the Chief FOIA Officers Council, which is composed of all agency Chief FOIA Officers, the Directors of OIP and OGIS, and the Deputy Director for Management from the Office of Management and Budget.[10] The council is tasked with developing recommendations for increasing FOIA compliance and efficiency; disseminating information about agency experiences, ideas, best practices, and innovative approaches related to FOIA; identifying, developing, and coordinating initiatives to increase transparency and FOIA compliance; and promoting the development and use of common performance measures for agency compliance with FOIA.

---

[5] (U) Office of Information Policy, *About the Office*, February 15, 2017.

[6] U) 5 U.S.C. § 552 (e)(i).

[7] (U) Office of the Attorney General Memorandum for Heads of Executive Departments and Agencies, *Freedom of Information Act*, March 19, 2009.

[8] (U) Office of Information Policy, *Organization, Mission, and Functions Manual*, September 9, 2014.

[9] (U) *Openness Promotes Effectiveness in Our National Government Act of 2007* (The *OPEN Government Act of 2007*) Pub. L. 110-175 (December 31, 2007).

[10] (U) *The Freedom of Information Act Improvement Act of 2016*, Pub. L.114-185 (June 30, 2016).

(U) Intelligence Community

(U) ODNI's Strategy and Engagement, Information and Data, Information Management Division (IMD) manages ODNI's FOIA program and has an IC-wide role in FOIA integration. IMD develops, implements, and manages programs that provide guidance for the IC's records, classification, declassification, public release, and FOIA officers.[11]

(U) Each of the IC elements responds individually to FOIA requests received by their element. Each Non-Department of Defense (DoD) IC element has its own Chief FOIA Officer. DIA, NGA, NRO, and NSA are both IC elements and Defense Intelligence Components.[12] As such, these IC elements are subject to both IC and DoD FOIA guidance. These elements do not have a Chief FOIA Officer, but instead a single DoD Chief FOIA Officer serves them all.

(U) Simplified Overview of FOIA Processing

(U) Requesters submit FOIA requests to agencies via email, mail, website, or electronic portals. When an agency receives a request, FOIA professionals generally log it into the agency's tracking system, assign a tracking number, and review the request for complexity. The agency sends acknowledgment of receipt to the requester. FOIA professionals then route the request to the appropriate record owner or subject matter expert (SME) to conduct a search for responsive records or conduct a search themselves. Next, FOIA professionals review the responsive records and determine whether the agency should withhold all or part of a record based on the Act's exemptions.

(U) The Act provides nine categories of information that are exempt from disclosure, such as information properly classified by Executive Order or personnel and medical files. See Appendix C for a list of the nine exemptions. FOIA professionals may consult with or refer records to other agencies when the records are the responsibility or contain the equities of another agency. After processing the records, applying appropriate FOIA exemptions, and redacting information accordingly, the agency releases the documents to the requester, or notifies the requester of the agency's inability to locate the requested records, or the agency's decision to withhold the requested records. The requester may then challenge an agency's final decision on a request through an administrative appeal or lawsuit. A requester has the right to file an administrative appeal and agencies have twenty working days to respond to an administrative appeal.

[11] (U) ODNI Instruction 80.06 *The ODNI Information Management Program*, Rev 1, March 1, 2017.

[12] (U) DoD Directive 5143.01, Under Secretary of Defense for Intelligence (USD)(I)), Change 1 Effective April 22, 2015.

(U) Assessment Results

(U) In FYs 16 and 17, FOIA requesters submitted a total of 11,804 requests to the IC elements we reviewed. Each individual case may generate one document that is responsive to the request or entire repositories of documents that require review, or may necessitate an exhaustive search that yields no responsive documents. Total FOIA costs during this time for these IC elements was over $51 million. Figure 1 illustrates the rise in FOIA costs since 2005. In FY17, these IC elements employed 164 FOIA professionals to process FOIA cases. IC elements collectively acknowledge that FOIA processes have not matured to keep pace with the increase in the complexity of requests. Factors that contribute to the complexity of a FOIA case include the volume of the information requiring review, the extent to which the information is technical or difficult to comprehend, the number of different offices that may have responsive documents, and the need to consult with other agencies. Although complexity of requests has grown, the IC elements' processes have not advanced to meet the demands. Further, ODNI has not taken a comprehensive strategic approach to address persistent FOIA challenges shared across the IC.

(U) Figure 1: The Rising Cost of FOIA

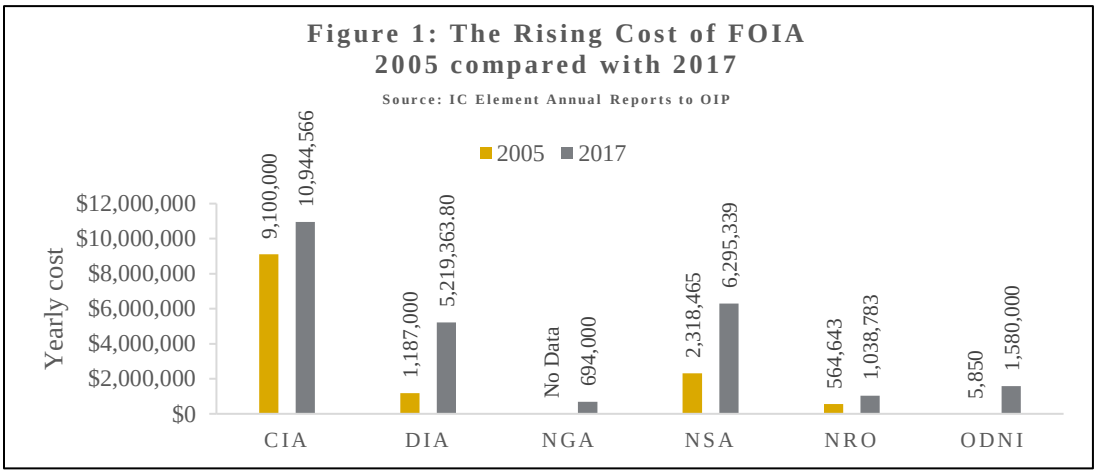

Figure 1 – Unclassified

(U) Finding 1: ODNI has not fully exercised its leadership responsibility to foster integration and collaboration to improve IC execution of FOIA.

(U) In its official mission and vision statements, ODNI identifies that a key component of its mission is to unify, meaning ODNI fully leverages the IC's diverse expertise by planning and acting together. However, with regard to the FOIA discipline, IC FOIA programs currently operate independently with minimal information sharing regarding FOIA management. While the statute gives each individual agency responsibility to manage its own program, the ODNI, because of its mission to integrate the IC, has a responsibility to address common IC FOIA issues. We assess that ODNI/IMD is in a unique position, and has an opportunity to influence the community in the interest of greater FOIA integration and collaboration. Throughout our review, FOIA professionals in all of the IC elements called for ODNI to do more to lead FOIA efforts in the IC. Specifically, FOIA professionals requested that ODNI establish more avenues for information sharing and provide guidance and a technical solution for consultations. Consultations occur when an agency coordinates with another organization that has

equities in the records being reviewed. Director, IMD, agreed that ODNI could assume more of a leadership role in the IC.

(U) Finding 1.1: ODNI IMD did not implement the FOIA improvement plan briefed to the EXCOM in 2016.

(U) In 2015, ODNI's Director, IMD, briefed ODNI's Executive Committee (EXCOM), its senior governance forum, that there was a burdensome and inefficient process for coordinating and responding within the IC to FOIA requests. The IC EXCOM then charged ODNI's IMD with leading a working group to develop an IC FOIA Improvement Plan. The working group, composed of FOIA and transparency professionals across the IC, explored challenges faced by IC elements. The resulting plan, briefed to the EXCOM in October 2016, featured recommendations to improve IC execution of FOIA as an enterprise. In the briefing, then-Director, IMD, said that if approved, IMD would begin to implement the recommendations and provide an annual update.

(U) The recommendations focused on four themes: rules of the road; connectivity and the use of technology; training/personnel; and templates.

- (U) Rules of the road highlighted that the IC FOIA community must find the balance between openness and protecting what really matters.
- (U) For technology, the working group agreed to continue to explore development of collaborative space, with each agency participating to help define rule sets. Agencies should update the collaborative space with points of contact and post their FOIA logs. The IC should have the capability to analyze the FOIA logs on the site to find similar requests. Agencies with an IC element should ensure that their FOIA office has access to at least one Joint Worldwide Intelligence Communications Systems (JWICS) terminal and secure communication system.[13]
- (U) For training, ODNI IMD agreed to create a training section on the site and make existing training available, as well as expand one of the IC FOIA Days into a substantive training session.[14]
- (U) Regarding templates for consistency, the group agreed the IC should implement a standard policy to address the minimum requirements for the referral or coordination of requests. The group also agreed to continue to develop templates.

(U) Although the IC elements agreed with the plan, ODNI disbanded the working group and did not implement the plan. IMD officials at the time of the briefing indicated the EXCOM agreed in principle with the recommendations; the EXCOM may not have given specific direction to move forward, but expected IMD to continue to work with the IC on the issues. The current Director IMD attributes the delay in pursuing improvements to uncertainty about EXCOM approval, conflicting priorities, and high personnel turnover within her organization. Without implementation of the plan, FOIA within the IC will remain disjointed and unable to make essential progress.

---

[13] (U) JWICS is a network connecting IC members.

[14] (U) ODNI periodically hosts an IC FOIA Officers' Information Day with sessions for IC FOIA professionals that include inside and outside speakers.

(U) Recommendation 1: For ODNI Director, IMD – Update, obtain EXCOM approval, and begin implementation of the recommendations of the 2016 FOIA Improvement Plan.

(U) ODNI concurred with Recommendation 1.

(U//FOUO) Finding 1.2: The IC is not making use of all available technology to support FOIA programs, and there is no consolidated IC-wide approach to technology application.

(U) In 2009, the President issued a FOIA memorandum that states, "All agencies should use modern technology to inform citizens about what is known and done by their Government."[15] OIP consistently requires agencies to include descriptions of the steps taken to greater utilize technology in their Chief FOIA Officer reports.

(U) The aforementioned 2016 FOIA Improvement Plan featured multiple connectivity and technology-related solutions, including use of IntelShare, IntelDocs and IC ITE Apps Mall-hosted tools to facilitate the referral and consultation process, develop a collaboration space, and provide all agencies with an IC element the JWICS connectivity and secure communications needed to enable effective FOIA referrals and consultations.

(U//~~FOUO~~) The DNI/USDI's *Consolidated Intelligence Guidance (CIG): Fiscal Years 2020–2024* is "the first step of a multi-year transformational effort to re-set and strengthen intelligence capabilities." The CIG is meant to "reinforce intelligence integration and unity of effort, ensuring the IC operates as an efficient and effectives enterprise."[16] Two of the CIG strategies have particular impact for leveraging technology on behalf of IC FOIA processes and procedures, "Augmenting Intelligence Using Machines" and "Modernization of Data Management and Infrastructure." Both priorities set strategic outcomes and prescribe programmatic actions relevant to developing and sustaining enterprise-level improvements to IC FOIA activities.

(U) IC elements identified several common areas for applying technological solutions to their organizations' FOIA processes. Most describe challenges from a lack of or an ad-hoc combination of systems and software applications that do not meet full requirements for effective FOIA functioning, including: enterprise search, de-duplication, document review, redaction, internal coordination, and inter-agency referral/consultation. Figure 2 shows the key areas where IC elements are pursuing new technology or updating technology to enhance FOIA programs.

[15] (U) White House Memorandum for the Heads of Executive Departments and agencies, *Freedom of Information Act*, January 21, 2009.

[16] (U) The DNI/USDI's Consolidated Intelligence Guidance (CIG); Fiscal Years 2020-2024.

(U) Figure 2: Technology to Support FOIA Programs

Areas of Effort or Interest: Technology Assistance to FOIA	CIA	DIA	NGA	NRO	NSA	ODNI
Case Management	●		●	●	●	●
Archive & Retrieval of Prior Releases	●			●	●	
Search	●	●	●	●	●	●
De-duplication	●	●	●	●	●	
Document Conversion/Preparation (e.g., text or PDF to OCR)	●			●	●	
Document review	●		●		●	●
Redaction	●	●	●	●	●	●
Internal coordination	●		●	●	●	
Inter-agency referral/consultation	●	●	●	●	●	●
Public access	●	●	●	●		●

Figure 2 – Unclassified

(U) Challenges to more strategic application of technology are rooted in a range of circumstances. In some IC elements, the key FOIA-related business lines of records management, information systems technology, and disclosure/release reside in different offices, with little sustained focus on integrating their activities to enhance FOIA processing. At DIA and NGA, in particular, the end-of-year unfunded requirement process is the single source of funding for system improvements/upgrades to their FOIA programs.

(U) Within the IC elements, we characterize the execution of FOIA responsibilities as an industrial age process applied to a digital age challenge. The most profound outcome of this mismatch is inefficiency that affects ability to meet statutory deadlines. Challenges include duplication of effort as requests move between offices for review; multiple transformations of documents from soft-to-hard copy and back to soft; or re-entering redactions of information made on one system into records on another. These inefficiencies extend overall processing time and increase opportunities for human error and inconsistencies. Cumbersome data transfer and collaboration methods between IC elements further delay critical consultations and referrals. Without a strategic approach, the IC will continue to struggle to comply with statutory deadlines and the resulting litigation.

(U) Recommendation 2: For ODNI Director, IMD – Revise the 2016 FOIA Improvement Plan to align the IT recommendation to appropriate IC strategic priorities (e.g., within the *CIG; Fiscal Years 2020–2024*, and other relevant strategic documents).

(U) ODNI concurred with Recommendation 2.

(U) Finding 1.3: ODNI's Difficult Issues Forum has not met since 2015 and there is no regular IC-wide group to address ongoing IC FOIA issues.

(U) According to the Government Accountability Office, interagency groups are an effective mechanism to facilitate collaboration among agencies to address policy development, program implementation, and information sharing challenges.[17] The ODNI FOIA program sponsors an IC FOIA Officer's Information Day that as many as 120 officers attend. This event was previously held twice a year, but was only held once in 2017 and will be held only once in 2018. Until early 2015, the ODNI FOIA program also led the Difficult Issues Forum (DIF), a smaller IC-wide working group, as needed, to address common FOIA challenges. During our review, FOIA professionals spoke to the forum's value as a venue for FOIA programs to collaborate and address IC-specific issues. FOIA professionals agree there are FOIA issues unique to the IC that ODNI is better suited to address than OIP. One program said the forum maximized exposure to IC-wide challenges and work solutions, activities that had an impact on their ability to improve processes. Agenda topics included consultations, using technology, and narrowing the scope of requests. The DIF held its last meeting in early 2015. Some of the DIF members continued to meet for several months as part of the working group for FOIA improvement, but larger DIF meetings were not held. Chief of ODNI's FOIA program has not held the DIF since then because of the demands on ODNI's internal FOIA program. Without a collaborative forum, IC FOIA professionals miss the opportunity to address common FOIA challenges.

(U) Recommendation 3: For ODNI Director, IMD – Reestablish the Difficult Issues Forum or another IC body for IC element FOIA programs to collaborate.

(U) ODNI concurred with Recommendation 3.

(U) Finding 1.4: ODNI has not engaged with OIP on IC-wide FOIA issues.

(U) All of the IC FOIA programs interact with OIP, one of the two organizations with Government-wide FOIA responsibilities, but interaction has not been focused on strategic IC-wide issues. OIP provides government-wide FOIA guidance. IC FOIA programs look to OIP for FOIA best practices guidance and reach out to OIP for clarification on that guidance. IC FOIA professionals also incorporate OIP guidance into their programs. In FYs 2016 and 2017, IC FOIA programs submitted 16 inquiries to OIP's FOIA counselor service, which is available to answer questions from agencies on FOIA issues. Each of the IC FOIA programs, with the exception of NGA, requested assistance through the service. OIP addressed topics related to policy or compliance with the Act such as questions on procedural provisions and the exemptions.[18] Given OIP's substantial role in the government-wide FOIA enterprise, it is important for the IC to ensure OIP understands the IC's unique issues with regard to FOIA implementation.

---

[17] (U) Government Accountability Office, *Managing for Results: Key Considerations for Implementing Collaborative Mechanisms*, September 27, 2012.

[18] (U) OIP provided IC IG with these general topic areas. Specific queries to OIP's Counselor Service are attorney-client privileged communications.

(U) OIP has provided training to IC elements and has participated in ODNI's Annual FOIA Information Days, but indicates it would welcome more interaction with ODNI. As of July 2018, ODNI/IMD leadership had not spoken with OIP on IC-wide issues, but recognized that more interaction could be valuable. OIP, as the government-wide FOIA interlocutor, could better assist IC FOIA programs and be more informed as it prepares government-wide guidance, if it gains a greater understanding of the IC from ODNI engagement. Therefore, ODNI/IMD leadership should initiate discussions with OIP.

(U) Recommendation 4: For ODNI Director, IMD – Initiate discussions with OIP on IC-wide FOIA issues.

(U) ODNI concurred with Recommendation 4.

(U) Finding 1.5: ODNI has not had discussions with OGIS on strategic IC-wide FOIA issues, access concerns, or challenges with the Act.

(U) One of ODNI's strategic goals for the IC is to integrate the collective capabilities, data, expertise, and insights of partners, consistent with law and policy. IC element FOIA programs work with OGIS when OGIS is mediating disputes with FOIA requesters. OGIS provides mediation as a non-exclusive alternative to litigation. Once a requester has gone to court, the requester cannot come to OGIS for mediation. Typically, OGIS will explain exemptions and help the requester through the FOIA process. OGIS also performs reviews of agency FOIA programs to determine compliance and conducts assessments of FOIA-specific issues. However, IC elements' systems of records notice do not allow OGIS access to IC FOIA files. For both its mediation and compliance roles, OGIS cannot review FOIA records without the individual requester's consent in each case OGIS has to review. Due to this lack of access, a sponsor introduced a bill in the House of Representatives in March 2018 that would allow OGIS access to agencies' FOIA records, but it has not advanced to a vote.[19]

(U) Between October 1, 2017 and May 1, 2018, nearly 200 FOIA requesters sought assistance from OGIS involving the six IC elements within the scope of this assessment. Sixty-six percent of these inquiries were general ombuds cases in which OGIS provided general assistance with the FOIA process. Thirty-three percent of the inquiries related to delays in responding to FOIA requests and denials of information under various FOIA exemptions, including "Glomar" responses.[20] The number of inquiries OGIS received from requesters during this time-period per IC FOIA program is as follows: CIA: 121, NSA: 42, DIA: 19, ODNI: 8, NRO: 2, NGA: 1.

(U//~~FOUO~~) OGIS officials indicate they have limited visibility into the IC and do not have access to internal IC FOIA policies or procedures. OGIS believes it could help educate requesters if it had more information from the IC, but acknowledges it has yet to engage with the IC on this issue. ODNI's IMD leadership agrees that more communication with OGIS would better inform the public, but as of July 2018, they had not reached out to OGIS.

[19] (U) H.R. 5253 *Office of Government Information Services Empowerment Act of 2018.*

[20] (U) A Glomar response is one in which an agency refuses to confirm or deny the existence of responsive records.

(U) OGIS is responsible for recommending legislative and regulatory changes to Congress and the President to improve the administration of the FOIA. During our review, FOIA professionals highlighted the need for statutory change and debated the merits of possible amendments to the FOIA law.[21] IC FOIA professionals suggested OGIS consider the following when proposing changes to the law:

- (U) the effectiveness of the fee structure;
- (U) data that demonstrates the required response times are unattainable;
- (U) allowing response times to vary by additional request queues beyond simple and complex;
- (U) the uniqueness of the IC, given the volume of classified and highly sensitive records;
- (U) a limit to the number of requests an individual requester may submit in a given time period;
- (U) restricting record requests to those that are focused on an agency's mission so that requests for cafeteria menus, number of geese on facilities, and similar such requests are not accepted;
- (U) greater flexibility for the government to argue that some requests are arbitrary and capricious; and
- (U) the concern that commercial requesters who request records and sell them for profit are using the FOIA system for business purposes and, as a result, the Act may not be serving the public as intended.

(U) OGIS will continue to have partial knowledge of IC-unique FOIA issues and limited ability to inform and educate requesters on IC FOIA cases and processes until the IC collaborates with them more fully. Furthermore, without a full understanding of IC challenges with the statute and the potential impact to the IC of proposed changes, OGIS may not consider all IC equities when making recommendations to Congress.

(U) Recommendation 5: For ODNI Director, IMD – Initiate discussions with OGIS regarding strategic IC-wide FOIA issues, access concerns, and the IC's perspective on the FOIA statute.

(U) ODNI concurred with Recommendation 5.

[21] (U) 5 U.S.C. § 552, as amended.

(U) Finding 2: IC Element FOIA programs are pursuing initiatives to improve effectiveness but are not consistently meeting statutory response deadlines.

(U) The Act requires that agencies reply to requesters within 20 working days of receipt of a perfected request with responsive documents unless there are unusual circumstances as defined by the Act.[22] [23] A perfected request reasonably describes the records requested and is made in accordance with published rules. In "unusual circumstances," as defined within the Act, the agency may extend the response time by written notice to the requester, setting forth the reasons for the extension and a date when the determination is expected.[24] [25] The agency may provide the requester with an opportunity to limit the scope of the request or arrange with the agency an alternative timeframe for processing the request.

(U) Each IC FOIA program is pursuing initiatives to improve its ability to comply with the Act. However, all of the programs are not consistently meeting the 20-day response time requirement. Figure 3 illustrates the percentage of initial cases closed within 1–20 working days in FY17. In FY17, each IC FOIA program closed less than 60 percent of all initial cases within 20 working days. Only NSA and ODNI closed more than 50 percent of all initial cases, with NSA reporting 55 percent closure and ODNI reporting 59 percent closure.

(U) A number of factors contribute to the inability of IC FOIA programs to meet the response timeline. Factors include complexity of records requested, resource challenges, personnel turnover, the process for locating and processing records, consultations that involve extensive coordination with other agencies that have equities in the review, competing demands of litigation and other document declassification reviews, and inadequate information technology (IT).

(U) Some IC FOIA programs receive requests for large volumes of files or entire repositories of records. In addition, within the IC, certain classified documents require additional scrutiny and levels of review. Many IC FOIA programs also receive broad requests for "any and all" documents related to a topic, such as, "all agreements with foreign governments," or "all communications" to or from a senator over a ten-year period. These kinds of broad requests add to the complexity of a request because it is more difficult for FOIA professionals to identify the correct office to search for potentially responsive material, and because searches for such requests may yield high volumes of potentially responsive records that must be reviewed.

(U//~~FOUO~~) Litigation demands are noteworthy. OGIS and OIP recognize that FOIA litigation cases can easily overtake a FOIA program by usurping resources available to address the rest of the workload. In both documentation and in interviews during this review, four of the six IC FOIA programs (CIA, DIA, NSA, and ODNI) report that litigation has a profound impact on their programs. All four describe litigation actions as disruptive to processing new requests and clearing existing backlogs because

---

[22] (U) 5 U.S.C. § 552 (a)(6)(A)(i).

[23] (U) In 1996, pursuant to the *Electronic Freedom of Information Act Amendments of 1996,* Pub L. No 104-231 (October 2, 1996), Congress amended the Act to, among other things, increase the legal response period from ten working days to the current response period of twenty working days.

[24] (U) 5 U.S.C. § 552 (a)(6)(B)(i).

[25] (U) Unusual circumstances include the need to search for records from facilities separate from the office processing the request, the need to search for, collect, and examine a voluminous amount of separate and distinct records, or the need for consultation with another agency.

programs must redirect resources to address litigation related requirements. FOIA litigations have tremendous production deadlines; judges are giving disclosure orders and processing schedules that programs must meet. For example, programs may need to revisit all actions taken on a case and prepare declarations to explain how and why the program applied exemptions in a given response. One official described litigation so complex that it took a senior official a week to prepare one declaration. Many officials cited the concern that some requesters immediately seek litigation when the 20-day response window expires before programs have a chance to complete initial processing. NRO and NGA did not identify litigation as a significant impact on their FOIA programs.

(U) Figure 3: Percent of Initial Cases Closed in 1–20 days. (Source: IC elements annual reports to OIP).

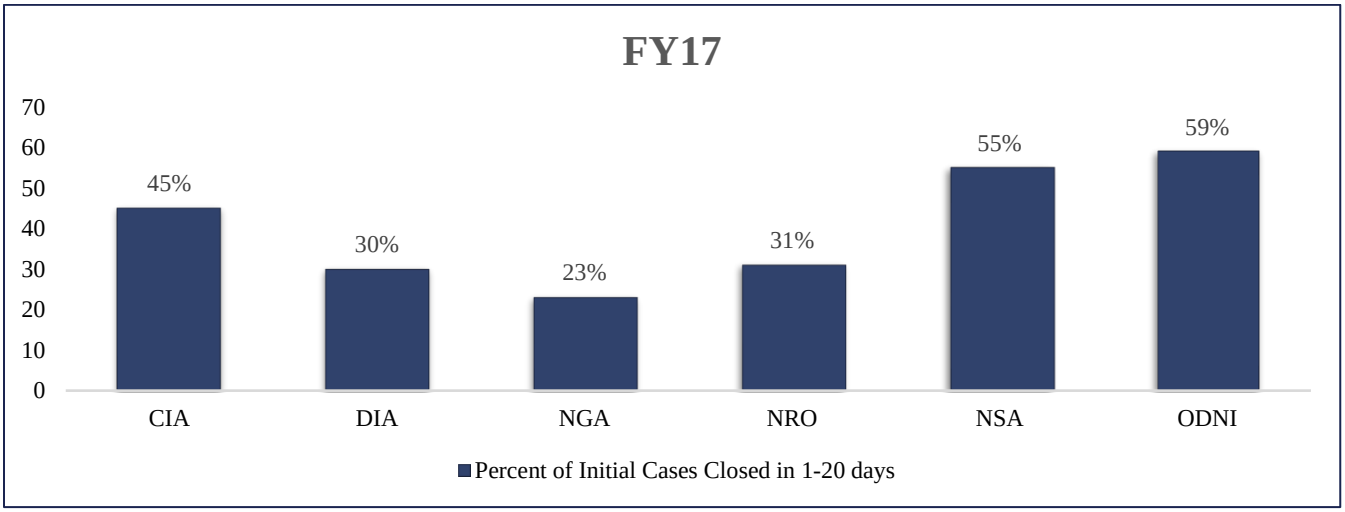

Figure 3 – Unclassified

(U) Observation 2.1: Between FY16 and FY17 all IC Element FOIA programs reduced average processing times for simple requests, while changes in processing times for complex cases varied.

(U) The 1996 amendment to the Act authorized agencies to multi-track requests. Multiple tracks allow an agency to process simple and complex requests concurrently on separate tracks to facilitate responding to relatively simple requests more quickly.[26] [27] We found that IC FOIA programs are following multi-track processing, using primarily a first in, first out methodology for each queue. NSA's system includes six queues including one labeled "super easy," addressing requests that produce no records or that require minimal specialized review. NRO includes a queue for consultations with other agencies. 2017 OIP guidance states that agencies should focus on ensuring that their simple track requests are responded to within an average of twenty days.[28] Figure 4 illustrates FY16 and FY17 average processing times for simple and complex requests. All programs reported a decrease in processing times for simple requests between FY16 and FY17. For complex requests, CIA and DIA saw increases in processing times, while

[26] (U) *Electronic Freedom of Information Act Amendments of 1996*, PL 104-231.

[27] (U) A simple request is a request that an agency using multi-track processing places in its fastest (non-expedited) track based on the low volume and/or simplicity of the records requested. A complex request is one that an agency places in a slower track based on the high volume or complexity of the records requested.

[28] (U) OIP Guidance for Further Improvement Based on 2017 Chief FOIA Officer Report Review and Assessment (Updated June 15, 2017).

ODNI and NRO experienced decreased times. NSA's processing time for complex cases remained relatively the same over the two years.

(U) Figure 4: Average Days to Process Simple and Complex Requests (Source IC elements' annual reports to OIP).

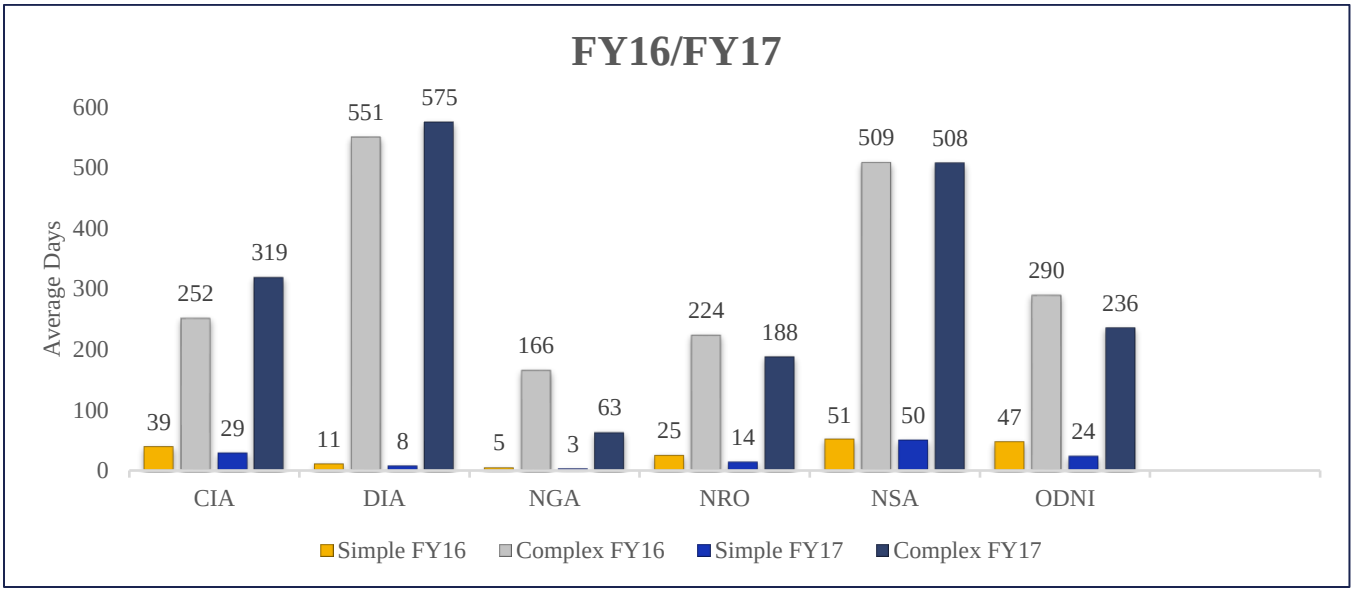

Figure 4 – Unclassified

(U) In addition to simple and complex requests, an agency may process requests on an expedited basis in cases in which the requester demonstrates a compelling need and in other cases determined by the agency. The Act requires agencies to determine within 10 calendar days whether a request meets the standards for expedited processing.[29] For FYs 16 and 17, not all IC FOIA programs reported expedited request determinations, but those that did made them in an average of less than 10 days. An agency that grants expedited processing must process the request "as soon as practicable."[30] However, some expedited processing requests are taking over a year to complete. For example, in FY17, ODNI reported an average of 565 days to process expedited requests and NSA reported 937 days. Reasons for delays in responding to expedited requests are the same as those cited for delays in processing all other types of FOIA requests.

(U) Observation 2.2: IC Element FOIA programs have focused efforts to close their oldest cases.

(U) OIP advises that a critical element to improving timeliness is closing the oldest pending requests each year. OIP guidance states that agencies should focus on prioritizing their oldest requests to ensure that the age of pending requests continues to improve. It also states agencies that do not close their ten oldest cases should implement best practices such as actively tracking the status of the oldest requests.[31]

[29] (U) 5 U.S.C. § 552 (a)(6)(E)(ii).

[30] (U) 5 U.S.C. § 552 (a)(6)(E)(iii).

[31] (U) OIP Guidance, *Closing the Ten Oldest Pending Requests and Consultations*, August 21, 2014.

(U) We found that all of the IC FOIA programs placed priority emphasis on their ten oldest cases. NSA assigns senior reviewers to work the second level review of these cases. NGA assigns these cases to staff during weekly meetings based on caseload. CIA adds emphasis to their ten oldest cases and reviews them at a monthly panel. In FY17, ODNI assigned one FOIA professional to focus on its ten oldest cases. DIA refocuses staff on the ten oldest cases annually and meets monthly to discuss top ten case reduction efforts. NRO implemented a focused plan to close its ten oldest cases. NRO closed all of the ten oldest cases in FY16 that had been pending the prior FY. ODNI and DIA closed all of their ten oldest cases in FY17 that had been pending in FY16.

(U) Figure 5 illustrates the three oldest cases for each IC element. Across all six, the oldest cases are January 10, 2001, September 23, 2004, and February 16, 2007, respectively. The IC elements collectively acknowledge that these cases are normally the most complex, require more follow up, and involve the equities of numerous agencies. IC elements should continue to focus on their oldest cases.

(U) Figure 5: FY17 Three Oldest Requests by Months in Process (Source: IC elements' annual reports to OIP).

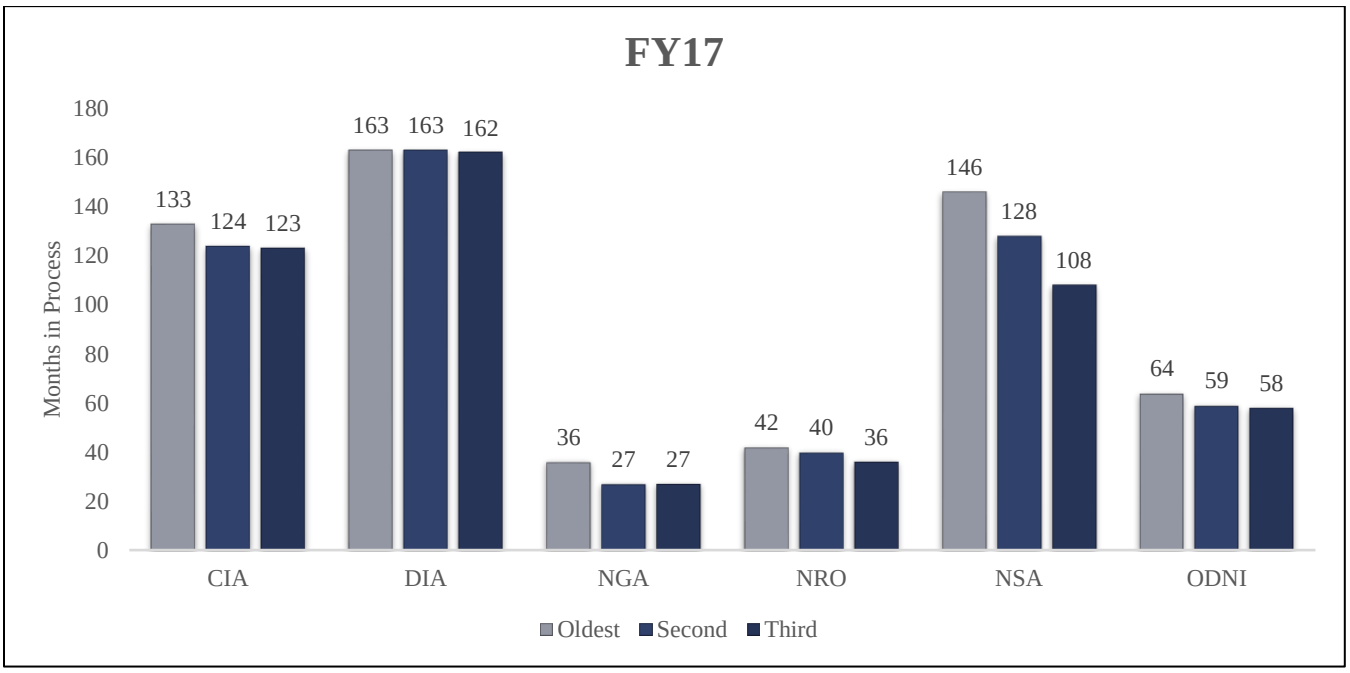

Figure 5 – Unclassified

(U) Finding 2.1: All IC FOIA programs report backlogs but not all have current backlog plans.

(U) FOIA professionals consider a request part of the "backlog" when it has been at any agency longer than the statutory time-period of twenty working days, or if unusual circumstances are present, up to thirty days. In 2008, the Attorney General required that each agency that had not reduced its backlog over the last two years prepare a backlog reduction plan.[32] In subsequent guidance, OIP identified a change to

[32] (U) OIP Guidance, *Guidance on Preparing Backlog Reduction Plans*, updated August 22, 2014.

that requirement and indicated that only agencies with more than 1,000 backlogged requests in a year were required to describe their plans to reduce their backlogs.[33]

(U//~~FOUO~~) Each of the IC elements has backlogs. CIA, NSA, and DIA received the most requests and have higher backlogs (over 1000 cases). ODNI, NRO, and NGA received fewer requests and have smaller backlogs. IC FOIA programs attribute their inability to reduce backlog to increases in request volume and complexity as well as litigation demands. There was also concern among some FOIA professionals that programs worked special declassification review projects without the benefit of additional resources and redirected focus away from processing routine FOIA requests, ultimately adding to backlogs. Figure 6 illustrates processed and pending requests.

(U) Figure 6: FY16/17 Requests Processed and Pending (Source IC elements' annual reports to OIP).

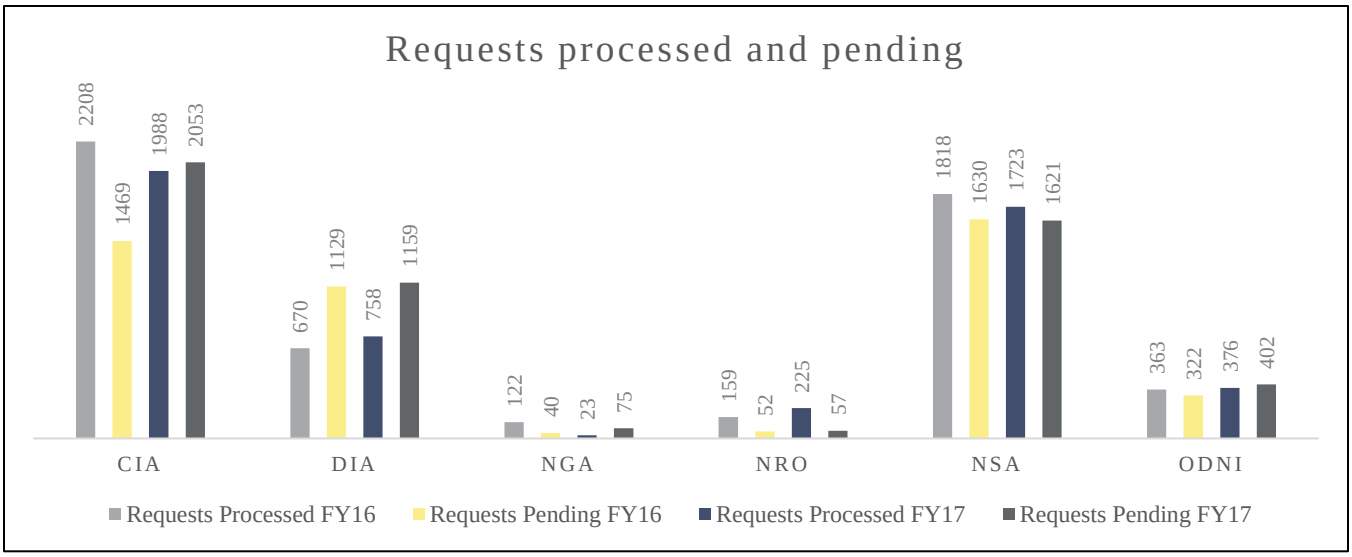

Figure 6 – Unclassified

(U//~~FOUO~~) Although all of the IC FOIA programs are undertaking efforts to reduce backlogs, four of the six IC elements had increases in backlogs between FY16 and FY17. Figure 7 illustrates backlogs. In FYs 16 and 17, CIA, NSA, and DIA had backlogs that exceeded 1000 requests and therefore were required to have backlog reduction plans, but only CIA and NSA had a backlog plan. CIA's plan streamlines levels of review for simple tasks and cases and implements improvements to workflows and coordination with other offices and agencies. NSA's plan outlines personnel increases, process improvement initiatives, and plans to create additional queues. NSA also plans to update website information and has identified IT requirements that would improve FOIA processing efficiency. NSA reports that significant increases in requests following the 2013 unauthorized disclosures had a substantial impact on their program.

(U//~~FOUO~~) DIA's FOIA Chief meets with staff monthly to monitor progress on backlog cases. DIA does not have a current backlog reduction plan, however. It is considering updating a legacy plan, but provided no period for the update. DIA advises that one reason for its backlog is that it is still recovering from a loss of contractors in 2015. Without a recent comprehensive plan to address backlog, DIA is unlikely to see sustained progress with backlog reduction.

[33] (U) OIP Guidance, *Guidelines for 2015 Chief FOIA Officer Reports*, updated December 11, 2014.

(U) Figure 7: FY16/17 Backlog Request Data (IC elements' annual reports to OIP).

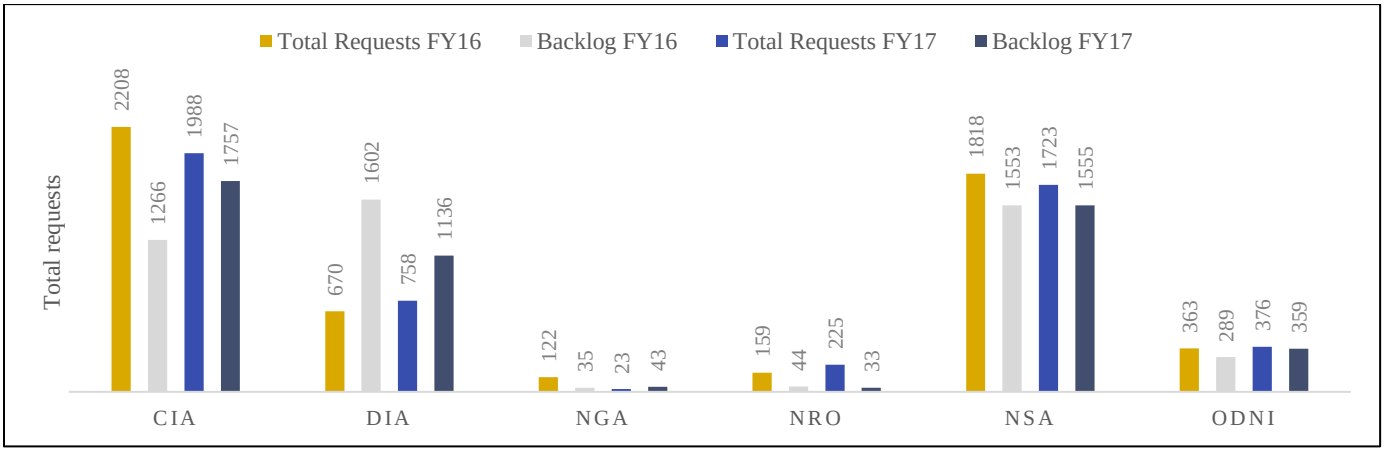

Figure 7 – Unclassified

(U) Recommendation 6: For DIA – Complete and begin implementation of a formal backlog plan.[34]

(U) DIA concurred with Recommendation 6.

(U) Finding 2.2: Consultations are a significant cause of processing delays and the IC does not have an established process or guidance for consultations.

(U//~~FOUO~~) The Act states that programs should conduct consultations with other agencies with all practicable speed. When a program locates responsive records, it should determine whether another agency has a substantial interest in the records and consult with the other agency. In these consultations, a FOIA program responding to a request first forwards a record to another agency or component within the same agency for its review. Once the agency in receipt finishes its review, it responds back to the agency that forwarded it, who then responds to the requester. Within the IC, it is common to process requests with records involving joint reports or other documents that contain information originating from or of interest to several agencies. For example, intelligence assessments may rely on more than one source of intelligence and often include sources originating from multiple agencies and containing multiple equities. OIP identifies CIA as one of the three agencies that account for nearly 70 percent of all consultations processed government-wide with CIA processing 14 percent or 819 consultations in FY17.[35]

(U) We found that consultations take extensive time to complete and can cause significant delays in overall processing. There are a number of contributing factors to consultation lags within the IC. Several agencies that have IC components, including DHS and DOS, do not have JWICS terminals in their FOIA offices. As a result, there is no easy method to transfer documents from one agency to another due to system incompatibility. FOIA professionals often print documents, scan them, and upload to a different

[34] (U) IC IG initially addressed this recommendation to, "DIA, Chief FOIA and Declassification Services Branch." DIA's official concurrence requested this recommendation be addressed to "DIA," and provided IC IG with a point of contact for action related to this recommendation.

[35] (U) OIP Summary of Annual FOIA Reports for Fiscal Year 2017, undated.

system or send via postal mail. For those that use email, file size of the records is an issue and can result in programs sending multiple emails to transmit one case. Further, programs do not always follow up to check on the status of consultations and in some instances, the receiving organization is unable to locate the case, requiring the process to restart. Programs that have success closing consultations report regular and persistent follow up. Figure 8 provides FY17 consultations data.

(U) Figure 8: FY16/17 Consultations Received/Processed, and Pending (IC elements' annual reports to OIP).

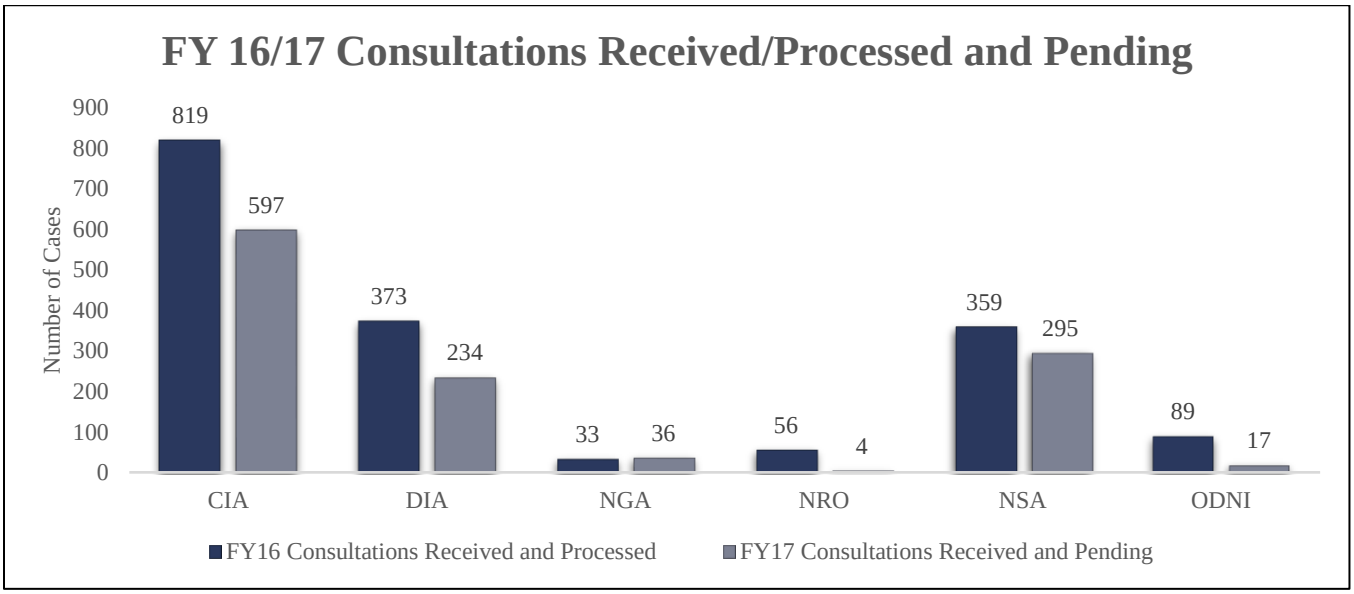

Figure 8 – Unclassified

(U//~~FOUO~~) OIP guidance states that when agencies routinely locate the same or similar types of documents or information that originated with another agency, or when agencies find that they routinely receive for consultation or referral the same type of record or information from another agency, they should look for ways to collaborate to see if they can adopt standard processing procedures to reduce the number of referrals or consultations that need to be made.[36] We found that a few agreements exist between some IC FOIA programs that describe how to handle each other's information or provide authority to make decisions. These agreements, if implemented properly, result in efficiencies because the program processing the case is empowered to make redactions and does not need to create a referral memorandum to the other organization. IC FOIA programs' greatest concern with these agreements is that the parties will go beyond their agreed upon authority to redact specific information, make a mistake, or inadvertently release classified or sensitive information.

(U) Apart from these unilateral agreements, the IC lacks guidance for consultations and there is no consistent approach. The aforementioned 2016 FOIA Improvement Plan includes one recommendation that called for agencies to include specific language in the memos used during the referral and consultation process. Agencies were to include language that explains how they plan to treat the document, and when possible which other agencies are consulted. During our review, we found that the IC has not implemented this recommendation or issued any guidance for consultations because ODNI

[36] (U) OIP Guidance, *Referral, Consultations, and Coordination: Procedures for Processing Records When Another Agency or Entity Has an Interest in Them*, August 15, 2014.

IMD leadership focused on its own FOIA program and not the working group recommendations. FOIA professionals agree that IC-wide guidance for consultations would help address areas of common concern across the IC and provide visibility into cross-IC cases. Several officials acknowledged that the Act gives authority for management of FOIA programs to heads of departments and agencies and as a result, ODNI is not likely to issue a formal policy document, such as an Intelligence Community Directive. However, the Director, IMD agreed that in its integrator role, ODNI has the authority to prepare guidance specific to common IC FOIA issues. The IMD website indicates IMD's role is to provide "light guidance" to ensure consistent information management practices across the IC. In the absence of guidance, IC programs are likely to continue to follow existing burdensome and inconsistent consultation processes.

(U) Recommendation 7: For ODNI Director, IMD – In coordination with the CIA Chief FOIA Officer; the DNI Chief FOIA Officer; the DIA Chief FOIA and Declassification Services Branch; NGA Branch Chief, Declassification/FOIA/Privacy Act Branch; NRO Chief Information Review and Release Group; NSA Chief FOIA Privacy Act Division; and the DoD Chief FOIA Officer, develop IC guidance to address consultations.

(U) ODNI concurred with Recommendation 7.

(U) Finding 2.3: Chief FOIA Officers are reviewing programs annually but have not made recommendations for improvements to IC FOIA programs to the heads of their agencies.

(U) The *FOIA Improvement Act of 2016* requires that the Chief FOIA Officer of each agency review, not less frequently than annually, all aspects of FOIA administration by the agency, including: agency regulations, disclosure of records required under paragraphs (a)(2) [proactive disclosure provision] and (a)(8) [foreseeable harm standard], assessment of fees and determination of eligibility for fee waivers, the timely processing of requests, and the use of exemptions and dispute resolution services with the assistance of OGIS or the FOIA Public Liaison.[37] The Act also requires that the Chief FOIA Officer recommend to the head of the agency such adjustments to agency practices, policies, personnel, and funding as may be necessary to improve its implementation of the Act.[38]

(U//~~FOUO~~) IC FOIA programs reported that their Chief FOIA Officers are not performing comprehensive reviews of their programs. Each of the IC elements are reviewing their programs annually and submitting a Chief FOIA Officer report to the Attorney General as required. However, the involvement of the Chief FOIA Officers in these reviews is limited. In addition, we could not find evidence that the Chief FOIA Officers had made any recommendations to their agency heads for improvements to IC FOIA programs in FYs 16 or 17. CIA's Chief FOIA Officer reviews CIA's annual report and provides guidance but does not conduct a formal review of their program and/or processes. CIA advises that the Director, Agency Data Office, fulfills those functions on a daily basis in his management and oversight of all information management programs to include FOIA, and keeps the Chief FOIA Officer informed as appropriate. DoD includes DoD IC element data in their annual Chief FOIA Officer report to the Attorney General and in their annual report for the Secretary of Defense. The most recent DoD Chief FOIA Officer report to the Secretary of Defense, dated January 17, 2018, addressed ,among other items, the FOIA processing backlog and specifically mentioned DIA's backlog. However, the report covered the entire DoD and while it identified areas for improvement for the

[37] (U) 5 U.S.C. § 552 (a)(8)(j)(3), as amended by Public Law 114-185—June 30, 2016, *FOIA Improvement Act of 2016.*

[38] (U) 5 U.S.C. § 552 (a)(8)(j)(2)(C), as amended by Public Law 114-185 – June 30, 2016, *FOIA Improvement Act of 2016*.

Department, it did not speak to any improvements specific to DIA, NGA, NRO, or NSA. In addition, while the annual reports and Secretary of Defense reports are available for DoD IC FOIA programs to review, there is no formal feedback process to provide the four DoD IC FOIA programs with review findings and recommendations for improvement.

(U//~~FOUO~~) Further, DoD IC element FOIA programs do not consider the annual data gathering by the DoD Chief FOIA Officer to constitute a review. DIA, NGA, NRO, and NSA FOIA programs all reported regular communication with the Directorate for Oversight and Compliance, Office of the Chief Management Officer (CMO) of the DoD, Office of the Secretary of Defense, but each acknowledged that CMO had not conducted formal program reviews. The Directorate of Oversight and Compliance assists the CMO in the fulfillment of Agency Chief FOIA Officer statutory responsibilities and considers both the DoD Annual FOIA report to the Attorney General and the DoD Chief FOIA Officer's report to meet statutory requirements of review of the DoD FOIA program. ODNI's Chief FOIA Officer (ODNI's Chief Operating Officer) is new to her role and stated that once she has greater familiarity with the ODNI FOIA program, she plans to review the programmatic effectiveness of ODNI's program. However, as of June 2018, the ODNI Chief FOIA Officer had not conducted reviews of the ODNI FOIA program.

(U//~~FOUO~~) Comprehensive FOIA program reviews provide Chief FOIA Officers an opportunity to identify areas for FOIA program improvement and develop recommendations for increasing FOIA compliance and efficiencies. Data in the Chief FOIA Officer reports covering 2016 and 2017 illustrate how the FOIA programs struggle to keep pace with the growth of FOIA. Chief FOIA Officers, due to their senior placement within each organization, are uniquely positioned to have visibility into the complexity of the FOIA enterprise. Although Chief FOIA Officers are overseeing their programs' progress with meeting statutory requirements through annual reviews and reporting, it was not evident that they are advocating for their FOIA programs to their agency head.

(U) Recommendation 8: For CIA and ODNI Chief FOIA Officers – Actively participate in the annual review of your FOIA program and make recommendations, as necessary, for improvements to the FOIA program to D/CIA and DNI, respectively.

(U) CIA and ODNI concurred with Recommendation 8.

(U) Recommendation 9: For DIA, NGA Branch Chief, Declassification/FOIA/Privacy Act Branch, NRO Chief Information Review and Release Group, and NSA Chief FOIA Privacy Act Division – Contact the DoD Chief FOIA Officer to collaborate on how best to conduct the annual review and establish a feedback mechanism to ensure your program receives results of annual reviews.[39]

(U) DIA, NGA, NRO, and NSA concurred with Recommendation 9.

(U) Finding 3: IC Element FOIA programs have various approaches to communicating with requesters but could further increase transparency.

(U) Improving communication and working cooperatively with FOIA requesters are essential parts of implementing an efficient and effective FOIA system. The Act outlines procedures for an agency to

[39] (U) IC IG initially addressed this recommendation to, "DIA, Chief FOIA and Declassification Services Branch." DIA's official concurrence requested this recommendation be addressed to "DIA," and provided IC IG with a point of contact for action related to this recommendation.

discuss with requesters ways of tailoring large requests to improve responsiveness, recognizing that FOIA works best when agencies and requesters work together. In addition, according to OIP guidance, establishing good communication with FOIA requesters is an "essential element to ensuring that each agency's FOIA process is working in accordance with the President's and Attorney General's directives."[40] Additional OIP guidance states that agency FOIA offices "must be ready to assist the public in understanding all aspects of the FOIA and how it works at their agency" and "should be able to assist members of the public" by:

- (U) identifying sources of information that are already posted and available, thereby potentially obviating the need to make a FOIA request in the first instance;
- (U) informing potential requesters about the types of records maintained by the agency (or agency component) and providing suggestions for formulating requests; and
- (U) describing the agency's various processing tracks and providing the average processing times.[41]

(U) Proactively communicating with requesters may help avoid lawsuits. According to an OGIS official, personal contact is important and may prevent litigation. One IC official provided an example where engagement with the requester prevented a litigation action. We determined that all of the IC FOIA programs are communicating with requesters, but could make greater use of their websites to further share information.

(U) Observation 3.1: IC FOIA programs are proactively engaging with requesters by telephone, email, or letter.

(U) During our review, we found that all of the IC FOIA programs are communicating with FOIA requesters by telephone, email, or letter to acknowledge FOIA requests, clarify, and properly scope requests, thereby increasing the quality of the documents disseminated to requesters, and to relay anticipated response times. Of the IC elements reviewed, NRO appeared to have the most proactive relationship with its requesters. NRO's FOIA program reported that it acknowledges requester inquiries within 24 business hours, and provides the requester with a case number (if applicable) and hotline number. IC elements reported that engaging regularly with requesters has improved their FOIA request processing timelines. NGA's FOIA program provided an example of such engagement citing a case in which a requester initially asked for all records NGA possessed on Syria for the entirety of 2017. However, through negotiation with the requester, the FOIA staff was able to narrow the scope to months, thus facilitating a faster response.

(U) In one CIA example, in FY 2017, FOIA professionals had several discussions with an academic who requested all records on a specific political party in a specific country for a 16–year period. After FOIA professionals discussed his specific interest, the requester agreed to revise his request to documents about official corruption within the country's government, and documents about seven companies that were involved in those activities during the 16–year period. Through these negotiations, CIA was able to tailor

---

[40] (U) OIP Guidance, *The Importance of Good Communication with FOIA Requesters,* August 21, 2014.

[41] (U) OIP Guidance, *The Importance of Quality Requester Services: Roles and Responsibilities of FOIA Requester Service Centers and FOIA Public Liaisons*, June 12, 2018.

the request to what the academic was actually interested in and identify specific search parameters to locate the appropriate responsive material.

(U) Similarly, ODNI's Civil Liberties, Privacy & Transparency (CLPT) office reported that they spoke with a FOIA requester who initially requested "all documents" related to a particular topic, or "a conversation." By engaging in discussions with the requester, CLPT was able to provide the requester what he needed without FOIA processing. A reduced, well-defined scope can result in faster response times, but FOIA requesters are not always willing to adjust the scope of requests. IC elements should continue to engage with requesters.

(U) Observation 3.2: IC Element FOIA programs are not routinely providing information to the public about the types of records they maintain on their website in part due to national security restrictions.

(U) Many requesters lack knowledge of the types of records the IC maintains. According to the OGIS, both IC FOIA programs and requesters could benefit if IC elements educate requesters on their missions. FOIA Advisory Committee (FAC) discussions note that if requesters knew the types of records agencies had, they could make more informed requests, rather than "any and all" requests, but many times they do not know what they should be asking for, because they do not know what records exist and how they are maintained. Education of requesters plays an important role in reducing inadequate searches, and more informed requests allow the agencies to conduct adequate searches. The 2016–2018 FAC, in its Final Report, for example, recommended that agencies disclose all unclassified reports agencies provided to Congress, with any necessary privacy redactions and all unclassified testimony submitted to Congress, making reports that are already the subject of many requests proactively available.[42] In addition, the FAC recommended posting an agency's organization chart and a directory listing contact information for all offices to ensure that the public can identify and contact federal offices for assistance.

(U//~~FOUO~~) IC elements face challenges that other US government agencies may not in determining what information to post on their public websites due to the classified and sensitive nature of the intelligence mission. Classification guides typically do not specifically stipulate what aspects of an IC element's mission may be shared with the public. IC elements are permitted by statute to withhold from the public information such as intelligence sources and methods, and information pertaining to agency employees, specifically: the organization, functions, names, official titles, salaries, or numbers of personnel employed. Therefore, if IC FOIA programs decide to share more on their websites, they must consider national security limitations.

(U) Observation 3.3: NGA has posted few frequently requested documents to its public website.

(U) The *FOIA Improvement Act of 2016* requires agencies make available for public inspection in an electronic format, records that have been requested three or more times. OIP guidance states that FOIA websites "should include a link to the FOIA Library (formerly called electronic reading rooms)" and that an agency's FOIA website and Reading Room can be a vital resource for users to find information that is

[42] (U) *Report to the Archivist of the United States, Freedom of Information Act Federal Advisory Committee, Final Report and Recommendations 2016-2018 Committee Term,* April 17, 2018.

already publicly available.[43] OIP's 2017 guidance on proactive disclosures provides additional information and guidance on the content of FOIA Libraries.[44] In its 2017 DoD Chief FOIA Officer Report, NGA reported experiencing technical issues with the FOIA Library and that its system administration team was coordinating with technical support to improve functionalities. Several officials noted that NGA complies with the requirement to post records that have been requested three or more times, but that NGA does not often receive requests for the same document. All of the IC electronic FOIA Libraries we reviewed contained several released records, with the exception of NGA. A spot-check of NGA's FOIA webpage (https://www.nga.mil/ About/Pages/FOIA.aspx) in July 2018 revealed that NGA has a FOIA Library, but the Library contains only one FOIA document and three annual reports. NGA reported in August 2018 that it is planning to post more documents.

(U) Observation 3.4: The IC FOIA programs are proactively disclosing information to the public, but implementation challenges exist to routine posting of FOIA released documents to websites.

(U) The IC Principles of Transparency Implementation Plan states that the IC should follow the practice of publishing FOIA released information on its public websites.[45] Further, 2017 OIP guidance states that agencies should, as a matter of discretion, be routinely posting material that is of interest to the public.[46] IC FOIA professionals and transparency officials recognize the importance of proactive releases to inform the public. Members of the public post FOIA released documents on their blogs and websites and provide narratives about intelligence activities that often lack context and reflect an incomplete or erroneous understanding of the IC. Although not required by law, when the IC proactively releases documents on their IC websites, it is an opportunity for the government to provide context to information and share the official story with the public. IC FOIA programs continue to pursue proactive disclosures but have identified several factors that limit full implementation including litigation workload, a lack of funding, personnel shortfalls, technical issues, and dependencies on other components responsible for management of the website. IC FOIA programs should continue to work to post items of interest to the public.

(U) Observation 3.5: Some IC FOIA programs have implemented the Release to One, Release to All draft policy.

(U) In July 2015, OIP launched a pilot program with the participation of seven volunteer agencies that sought to assess the viability of a FOIA policy that would entail the routine online posting of records processed for release under FOIA.[47] The draft policy, "Release to One, Release to All," would result in access by all citizens to information released under FOIA, not just those making a request.[48] The pilot

---

[43] (U) OIP Guidance, *Agency FOIA Websites 2.0*, November 30, 2017.

[44] (U) OIP Guidance, *Proactive Disclosure of Non-Exempt Agency Information: Making Information Available Without the Need to File a FOIA Request*, January 17, 2017.

[45] (U) *The Implementation Plan for the Principles of Intelligence Transparency*, October 27, 2015.

[46] (U) OIP Guidance, *Proactive Disclosure of Non-Exempt Agency Information: Making Information Available Without the Need to File a FOIA Request*, January 11, 2017.

[47] (U) OIP Proactive Disclosure Pilot Assessment, June 2016.

[48] (U) 24 C.F.R. Part 50, Request for Public Comment on Draft "Release to One, Release to All" Presumption, December 9, 2016.

identified metrics regarding the time and resources associated with implementing this policy. ODNI participated in the pilot and has continued to post all documents released under their FOIA program.

(U) During our review, IC FOIA programs reported a correlation between release of FOIA records to the public at large via website posting, and the subsequent influx of FOIA requests related to the same topic. However, the OIP pilot drew no conclusion as to whether the routine posting of FOIA processed records would result in an increase in requests. OIP has solicited input from and engaged with the public and other stakeholders on the draft policy, and is currently evaluating how to move forward in consultation with the Chief FOIA Officer Council. OIP acknowledges the resource implications of any new requirement to post additional records online.

(U) We found that several IC FOIA programs are releasing to the larger public records that they have released through FOIA processing. Figure 9 provides the status of IC FOIA program's implementation of proactive disclosure of records released under FOIA.

(U) Figure 9: Implementation of proactive disclosure of records released under FOIA.

IC Element	Status	Description of Implementation
CIA	Partial	During our review, CIA indicates they intend to post records with priority given to frequently requested records.
DIA	Full	Posts all releases on a monthly basis. Working with Public Affairs to market information placed on FOIA website.
NGA	Partial	Considering whether to incorporate this practice into policy. Will re-evaluate when their website has been reconstructed.
NRO	Full	Posts all releases on a quarterly basis, but in FY17 noted they had a break in posting records when funding was not available.
NSA	Partial	Reports proactive releases during 2017 but notes NSA's website was recently reorganized and they are working to establish an office presence on the website.
ODNI	Full	Since August 2015 has posted all FOIA responses. During this review, indicated they post all releases within two weeks, but have not had many records to post lately because not many initial FOIA cases have been completed due to focus on litigation.

Figure 9 – Unclassified

(U) Observation 3.6: IC FOIA programs could more effectively use their websites to educate the public by providing a description of their various FOIA processing tracks and average response times.

(U) Processing time varies depending on whether the FOIA request is a simple request, a complex request, or a request requiring expedited processing. Processing times also vary depending on the FOIA program officers' workload and other factors. While DIA provides requesters with a queue number for their request in correspondence, a review of the six IC element FOIA websites as of July 2018 revealed that none is currently providing information to the public about average processing times. Providing requesters with more visibility into FOIA processes and processing times can help manage requester expectations. Therefore, IC FOIA programs should consider providing a description of their processing tracks and average response times on their websites.

(U) Commendable 1: NRO conducted a survey of its FOIA requesters to solicit feedback.

(U) NRO recently conducted an online survey of its frequent requester community in order to better assess and understand satisfaction with FOIA processes and response letters. The survey included a section in which requesters provided input on the type of information that is most desired under the agency's proactive release program. While IC elements have various initiatives through transparency and historical declassification programs to seek public input, NRO was the only program we found that had a survey to seek input on the FOIA program. Surveying FOIA requesters can be an effective method for soliciting customer feedback on agency FOIA processes and requester document needs. IC FOIA programs should consider conducting a survey of their requesters.

(U) Finding 3.1: The IC has not strategically evaluated the effect of IC initiated proactive review and release initiatives on FOIA programs.

(U) The ODNI CLPT focuses on high-priority intelligence and national security initiatives to help the IC protect civil liberties and privacy as it pursues its intelligence objectives. CLPT also has a mission to ensure the IC provides appropriate transparency to the public. In 2014, CLPT led the Intelligence Transparency Working Group (ITWG) that identified a need for guidance on how offices such as FOIA, general counsel, civil liberties and privacy, public affairs, and information management should interact to integrate transparency within and across the IC. On April 4, 2016, then DNI Clapper formalized the transition of the ITWG into a permanent IC Transparency Council (ITC) with his signature on the Council Charter. IC FOIA professionals have varying levels of interaction with transparency, historical program, and declassification review officials. Recently, the IC has undertaken a number of historical declassification and transparency efforts to release information to the public. The IC delivered records on topics related to the John F. Kennedy assassination, the Vietnam War TET offensive, the White House directed review on Argentina, and Section 702 of the Foreign Intelligence Surveillance Act, among others.[49]

(U) In some IC elements, FOIA programs must shift resources away from FOIA processing to search for records or perform document reviews in support of these efforts, resulting in longer processing times for FOIA cases. We found that FOIA professionals were not always knowledgeable about recent transparency or historical review efforts and officials leading these efforts were not aware of the impact on FOIA programs. Further, in some cases, FOIA professionals were processing FOIA cases and making redactions of information when they learned the same information had just been officially released by a proactive declassification review. Knowledge of the other information review and release effort could have informed the FOIA program's approach in the FOIA processing. Although CLPT has provided informal guidance and shared best practices through the ITC, the IC has not developed formal written guidance to address integration between these offices. In the absence of formal written guidance, there is a risk that these declassification reviews may not be properly coordinated and will continue to require redirection of FOIA program resources without adequate planning.

(U) Recommendation 10: For ODNI's CLPT Officer, in coordination with ODNI/IMD, IC FOIA programs, and appropriate information management professionals – Develop overarching written

[49] (U) Section 702 refers to the *FISA Amendments Act* that prescribes procedures for targeting certain persons outside the U.S. other than U.S. persons.

guidance that specifies roles, responsibilities, and processes for coordinating IC-wide transparency initiated declassification review and release projects.

(U) ODNI concurred with Recommendation 10.

(U//~~FOUO~~) Finding 4: The IC has mechanisms in place to reduce the likelihood of inconsistent FOIA release determinations.

(U//~~FOUO~~) The aforementioned 2015 initial briefing to the EXCOM on FOIA challenges spoke of inadequate insight into how other agencies are responding to the same or similar requests. In the briefing, the former Director, IMD noted this lack of insight has sometimes led to the same information processed differently or inconsistently redacted across agencies. The briefing highlighted the need for overarching guidance for releasable information when FOIA requests have equities originating in or across multiple agencies.

(U) For purposes of this assessment, we defined an inconsistent FOIA release determination as a decision to withhold information when in the past a decision had been made to officially release the same information or vice versa. As noted in the introduction and methodology sections of this report, IC IG asked IC elements for examples of inconsistent FOIA release determinations and performed open source research to locate examples; however, we did not address IC elements' application of particular FOIA exemptions in specific cases. We determined in some cases what appears to be an inconsistent release is actually the proper application of an IC element's statutory authority that allows one IC element to withhold information that another IC element may release such as an employee's official email address. Further, events may have transpired since the original release decision, such as a subsequent declassification of the same or similar information, which may legitimately result in a different decision on the same information upon a later review.

(U//~~FOUO~~) None of the IC FOIA program officials nor the current Director, IMD identified inconsistencies as a prevalent problem. In addition, our open source research did not yield information to suggest that inconsistencies were a significant issue. Further, we found IC FOIA programs practice a number of approaches to reduce the chance that inconsistent release decisions occur. Although there is no data available to perform a statistical analysis to measure occurrence of inconsistent decisions as a percentage of overall releases, several officials cite the large volume of pages released and the relatively small number of errors discovered. Nonetheless, we identified examples of different decisions on the same information. In April 2016, at ODNI's FOIA Officers' Information Day, a speaker, who was a frequent FOIA requester, provided examples of requesting information at separate times where the same documents were redacted differently. CIA shared a couple of examples in which there was a denial of information by a Glomar decision in one case and not in another for the same information. NSA reported a similar case in which DoD released a document containing NSA's information that should have been a Glomar decision, but NSA learned of it after the release. We also found an instance where redaction actions applied by multiple IC elements were not de-conflicted prior to release. NRO acknowledged a case in which they redacted a few words that had been previously released. In some cases, requesters brought these inconsistencies to the IC's attention and they were corrected.

(U) Factors that contribute to inconsistent FOIA release determinations include:

- (U//~~FOUO~~) Failure to conduct consultations with all organizations that have equities in the information being reviewed;
- (U//~~FOUO~~) No visibility across IC FOIA programs regarding requests for the same or similar information;
- (U//~~FOUO~~) Human error, primarily related to the volume of pages being reviewed and the manual nature of the review process;
- (U//~~FOUO~~) Inadequate research or limited search capability to determine if the information being reviewed was previously officially released; and
- (U//~~FOUO~~) A time gap between when the IC or other agencies officially release information and classification guides FOIA professionals use are updated to reflect a new classification or declassification decision.

(U) Observation 4.1: ODNI's 2016 FOIA Improvement Plan includes recommendations that should mitigate the chances inconsistent FOIA release determinations occur.

(U//~~FOUO~~) Although IC FOIA programs practice a number of approaches to reduce the chance that inconsistent release decisions occur, there are opportunities to improve these efforts. IC FOIA programs use a two or more person review of documents prior to release and employ senior reviewers. To be successful in minimizing inconsistencies, reviewers need expertise and longevity in their positions. IC FOIA programs also conduct research to locate previously released documents, but several identified inadequate enterprise wide systems to perform these searches. Several IC FOIA programs employ redaction software that uses code to identify words, but there is no common redaction software for the IC.

(U//~~FOUO~~) IC FOIA programs offer equities recognition training to reduce the chance that programs will mistakenly make a decision on information that belongs to another organization, which may be inconsistent with past decisions. We found this training raises FOIA professionals' awareness of organizational specific sensitivities to prevent inappropriate release of classified information. Several IC elements and the ODNI have hosted equities recognition sessions, but IC professionals believe the IC should sponsor more of this training.

(U//~~FOUO~~) In addition, when FOIA requesters submit requests for the same or similar information to multiple organizations, requesters are not required to notify each organization of the other's requests and the IC does not have a mechanism or IT tool that records FOIA requests received across the IC. As a result, the potential exists that IC FOIA programs could make different decisions on the same information if these requests are not properly coordinated through the consultation process. However, if ODNI implements Recommendation 1 of this report to execute its 2016 FOIA Improvement Plan, which is focused on greater collaboration, consultations, guidance, a collaborative site, and training, the IC should have a stronger framework to reduce inconsistent release determinations.

(U) APPENDIX A: ACRONYMS LIST

CIA	Central Intelligence Agency
CIG	Consolidated Intelligence Guidance
CLPT	Civil Liberties, Privacy and Transparency
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DIF	Difficult Issues Forum
DoD	Department of Defense
DOJ	Department of Justice
DOS	Department of State
E.O.	Executive Order
EXCOM	Executive Committee
FAC	FOIA Advisory Council
FOIA	Freedom of Information Act
FY	Fiscal Year
IC	Intelligence Community
IC IG	Intelligence Community Inspector General
I&E	Inspections and Evaluations Division
IMD	Information Management Division
IT	Information Technology
ITWG	Intelligence Transparency Working Group
JWICS	Joint Worldwide Intelligence Communications System
NARA	National Archives and Records Administration
NGA	National Geospatial-Intelligence Agency
NRO	National Reconnaissance Office
NSA	National Security Agency
ODNI	Office of the Director of National Intelligence
OGC	Office of General Counsel

(U) APPENDIX A: ACRONYMS LIST CONTINUED

OGIS	Office of Government Information Services
OIG	Office of Inspector General
OIP	Office of Information Policy
PA	Privacy Act
SME	Subject Matter Expert
USDI	Under Secretary of Defense for Intelligence

(U) APPENDIX B: COMMENTS

(U) ODNI concurred with Recommendations 1, 2, 3, 4, 5, 7, 8, 9, and 10. DIA concurred with Recommendation 6. CIA concurred with Recommendation 8. DIA, NGA, NRO, NSA concurred with Recommendation 9.

(U) CIA Comments

(U) CIA concurred with no comment.

(U) DIA Comments

(U) DIA concurred with no comment.

(U) NGA Comments

(U) NGA concurred with no comment.

(U) NRO Comments

(U) NRO concurred with no comment.

(U) NSA Comments

(U) NSA concurred with no comment.

(U) ODNI Comments

(U//~~FOUO~~) The Office of the Director of National Intelligence (ODNI) appreciates the opportunity to comment on the draft IC IG assessment. ODNI recognizes the need for improved FOIA processing and coordination within the IC, as well as its unique role in supporting such progress. ODNI will endeavor to implement the recommendations provided by the assessment in a manner that respects and adheres to ODNI's authorities, and as can be realistically achieved with the available resources. ODNI also recognizes that implementation of the IC IG recommendations may take time.

(U//~~FOUO~~) As such, ODNI concurs with the ICIG assessment with the following comments/recommendations:

- (U//~~FOUO~~) Recommended changes to references to Intelligence Transparency Working Group – The Intelligence Transparency Working Group (ITWG) was formalized into the Intelligence Transparency Council by a charter signed by then-DNI Clapper in April of 2016 and posted publicly. Accordingly, suggest, in the first paragraph under Finding 3.1, add a new sentence after the existing third sentence, as follows: "On April 4, 2016, then DNI Clapper formalized the transition of the ITWG into a permanent IC Transparency Council (ITC) with his signature on the Council Charter." In the second paragraph, replace "ITWG" with "ITC." (CLPT).

(U) IC IG made this change prior to publication.

- (U//~~FOUO~~) Adjust Updated Recommendation 1 to add EXCOM approval of the updated plan – Once ODNI updates the FOIA Improvement Plan, approval by the EXCOM would be necessary to elicit IC-wide commitment, and to enable IMD to implement the updated plan in successful collaboration with the IC elements.

(U) IC IG made this change prior to publication.

(U) APPENDIX C: SUMMARY OF FOIA EXEMPTIONS

(U) This appendix provides a summary of the FOIA exemptions. For the full statutory language, see 5 U.S.C. § 552 (b).

(b)(1) Records are currently and properly classified in the interest of national security.

(b)(2) Records that relate solely to the internal rules and practices of an agency.

(b)(3) Records that are protected by another law that specifically exempts the information from public release.

(b)(4) Trade secrets and commercial or financial information obtained from an individual or business which would cause substantial competitive harm to the submitter if disclosed.

(b)(5) Inter-agency or intra-agency documents which would not be available by law to a party in litigation with the agency (e.g., records protected by the deliberative process, attorney-client or attorney-work product privileges).

(b)(6) Records which if released would result in a clearly unwarranted invasion of personal privacy.

(b)(7) Investigatory records or information compiled for law enforcement purposes.

(b)(8) Records used by agencies responsible for the regulation or supervision of financial institutions.

(b)(9) Records containing geological and geophysical information regarding wells.

(U) APPENDIX D: SUMMARY OF RECOMMENDATIONS

(U) **Recommendation 1:** For ODNI Director, IMD – Update, obtain EXCOM approval, and begin implementation of the recommendations of the 2016 FOIA Improvement Plan.

(U) **Recommendation 2:** For ODNI Director, IMD – Revise the 2016 FOIA Improvement Plan to align the IT recommendation to the appropriate IC strategic priorities (e.g., within the *CIG: Fiscal Year 2020–2024* and other relevant strategic documents).

(U) **Recommendation 3:** For ODNI Director, IMD – Reestablish the Difficult Issues Forum or another IC body for IC element FOIA programs to collaborate.

(U) **Recommendation 4:** For ODNI Director, IMD – Initiate discussions with OIP on IC-wide FOIA issues.

(U) **Recommendation 5:** For ODNI Director, IMD – Initiate discussions with OGIS regarding strategic IC-wide FOIA issues, access concerns, and the IC's perspective on the FOIA statute.

(U) **Recommendation 6:** For DIA – Complete and begin implementation of a formal backlog plan.[50]

(U) **Recommendation 7:** For ODNI Director IMD – In coordination with the CIA Chief FOIA Officer, the DNI Chief FOIA Officer, the DIA, Chief FOIA and Declassification Services Branch, NGA Branch Chief, Declassification/FOIA/Privacy Act Branch, NRO Chief Information Review and Release Group, NSA Chief FOIA Privacy Act Division, and the DoD Chief FOIA Officer develop IC guidance to address consultations.

(U) **Recommendation 8:** For CIA and ODNI Chief FOIA Officers – Actively participate in the annual review of your FOIA program and make recommendations, as necessary, for improvements to the FOIA program to D/CIA and DNI, respectively.

(U) **Recommendation 9:** For DIA, NGA Branch Chief, Declassification/FOIA/Privacy Act Branch, NRO Chief Information Review and Release Group, and NSA Chief FOIA Privacy Act Division – Contact the DoD Chief FOIA Officer to collaborate on how best to conduct the annual review and establish a feedback mechanism to ensure your program receives results of annual reviews.

(U) **Recommendation 10**: For ODNI's CLPT Officer – In coordination with ODNI/IMD, IC FOIA programs, and appropriate information management officials – Develop overarching written guidance that specifies roles, responsibilities and processes for coordinating IC-wide transparency initiated declassification review and release projects.

[50] (U) IC IG initially addressed recommendations 6 and 9 to, "DIA, Chief FOIA and Declassification Services Branch." DIA's official concurrence requested this recommendation be addressed to "DIA," and provided IC IG with a point of contact for action related to this recommendation.

GENERAL SERVICES ADMINISTRATION
Washington, DC 20405

OAS P 1820.1
March 7, 2014

GSA ORDER

SUBJECT: GSA Records Management Program

1. Purpose. This Directive establishes principles, authorities, responsibilities, and requirements for managing GSA's records.

2. Background. The Federal Records Act of 1950, as amended (44 U.S.C. § 3101), requires all Federal agencies to make and preserve records containing adequate and proper documentation of its organization, functions, policies, decisions, procedures, and essential transactions. These records must be managed according to applicable authorities (refer to Appendix A for a citation of authorities).

The Federal Records Act also states: "The head of each Federal agency shall establish and maintain an active, continuing program for the economical and efficient management of the records of the agency" (44 U.S.C. § 3102). Essential elements of Records Management Programs customarily include:

- Issuing up-to-date records management directives;
- Training those responsible for the implementation of the agency's Records Management Program; and
- Evaluating the agency's Records Management Program to ensure adequacy, effectiveness, and efficiency.

Records serve a number of purposes, including:

- Planning administrative and program needs;
- Documenting GSA activities;
- Protecting the agency's legal and financial rights;
- Providing for adequate oversight by Congress and other authorized agencies;
- Documenting the agency's history; and
- Providing for continuity of operations during an emergency or disaster.

Records are critical to an organization's effective and efficient functioning in accordance with the law.

3. Scope and applicability. This Directive provides policies and procedures for identifying and managing GSA records. It addresses all records created or received by GSA under Federal law or in connection with transacting public business. Refer to Appendix B of this order for the definition for types of records. This Directive establishes specific requirements to:

- Provide effective and efficient records management to support GSA's programs and mission;
- Preserve official GSA records in compliance with applicable statutory and regulatory requirements; and
- Promote appropriate access to information by GSA staff, GSA affiliates, customers, and the general public.

This Directive applies to all GSA services, staff offices, regions, and GSA employees. The Office of Inspector General may exempt itself from any records management processes and policies issued by GSA that, in the judgment of the Inspector General, may conflict with the Office of Inspector General's mission or limit its independence, unless the law prohibits such exemption. (Inspector General Reform Act of 2008 (5 U.S.C. App. 3).

4. Cancellation. This Directive cancels CIO P 1820.1 CHGE 4, GSA Records Maintenance and Disposition System, dated June 8, 2007.

5. Nature of revisions. This Directive reflects changes to the:

- GSA Records Management Program;
- Use of electronic records versus paper records as the primary media for records preservation; and
- Office of Mission Assurance's responsibility to manage the vital records program and its associated policy.

6. Signature.

/S/ 3/7/2014
CYNTHIA A. METZLER Date
Chief Administrative Services Officer
Office of Administrative Services

/S/ 3/7/2014
SONNY HASHMI Date
Acting Chief Information Officer
Office of the Chief Information Officer

GSA Records Management Program
Table of Contents

Paragraph **Page**

Introduction 1

Records Management Program Structure 1

Handling, Storage, Retention and Destruction of Records 2

Transferring Records 7

Responsibilities 8

- GSA employees 8
- Signatory official 8
- Administrator of General Services 9
- Chief Administrative Services Officer 9
- GSA Agency Records Officer 10
- Senior Records Officer 10
- Regional Administrator 12
- Head of Service and Staff Offices 12
- Records Management Coordinator 14
- Chief Information Officer (CIO) 15
- Program Manager 17
- Office of the General Counsel 17

Appendix A. - Authorities A-1

Appendix B. - Definitions B-1

Appendix C. - Required Records Management Program Training C-1

Introduction

GSA's Records Management Program governs GSA's statutory responsibility to make and preserve agency records by working closely with GSA employees and the National Archives and Records Administration (NARA). National Archives and Records Administration is the Government's oversight agency responsible for appraising all Federal records, approving their disposition, evaluating Records Management Programs, and storing permanent records.

Federal law requires that every agency establish a comprehensive Records Management Program and "…issue a directive(s) establishing program objectives, responsibilities, and authorities for the creation, maintenance, and disposition of agency records" (36 CFR 1220.34(c)). For a full listing of all relevant statutory authorities see Appendix A.

This GSA Directive provides policies and procedures for GSA's Records Management Program. The directive sets forth the program structure, roles and responsibilities and GSA's records management processes. For additional questions, contact your Records Management Coordinator.

Note: If an office needs an exception to the Records Management Policy, i.e., to control records separately or differently, any exceptions should be discussed with the Agency Records Officer before they are put into effect.

Records Management Program Structure

The Office of Administrative Services is responsible for GSA's Records Management Program and will work closely with the Office of the Chief Information Officer. Positions performing GSA's records management work throughout Central and Regional offices are outlined below.

Agency Records Officer

- GSA's Subject Matter Expert on Records Management Authority
- Liaison to National Archives and Records Administration
- Coordinates with the Chief Information Officer

Senior Records Officer

- Directly Supports Offices and Regions
- Liaison and support for Records Management Coordinators
- Coordinates with the Agency Records Officer

Records Management Coordinator

- Knowledge of area's records and file plan
- Answer records questions for local staff
- Works with Senior Records Officer

Handling, Storage, Retention and Destruction of Records

Determining record status

In developing recordkeeping requirements, the first step is to determine which documentary materials need to be identified as records and preserved to ensure complete and accurate documentation. Preserve records by filing, storing, or otherwise systematically maintaining them. Important items to keep in mind are outlined below.

- Work-related personal files can be difficult to distinguish from agency records. GSA employees must take care to keep personal files separate from agency records.

- In the event a personal file contains agency records material, GSA employees must extract official information included in personal files and copy or place it in an agency record file.

- Occasionally, the courts may determine that some materials considered personal files are agency records, depending on the circumstances surrounding their creation, maintenance and use, and disposition.

- The courts have developed legal decisions regarding these circumstances in deciding Freedom of Information Act (FOIA) cases. The meaning of "agency record" for purposes of FOIA is broader than the definition of "records" found in 44 U.S.C. 3301, cited in par. 1a, Appendix B.

Handling records

In conducting business, every GSA employee creates records in a variety of media. The following instructions are best practices on the proper handling of records.

- Managing records effectively ensures that permanent records become part of the National Archives and Records Administration (NATIONAL ARCHIVES AND RECORDS ADMINISTRATION) while other records and information of temporary value are retained for as long as needed and then properly disposed.

- Documents stored in "the cloud" or in any type of Social Media site might be considered records. Employees must ensure that GSA business-related internet and intranet postings, such as social media postings, Chatter postings, and

collaborative worksite postings containing records are maintained in accordance with GSA's recordkeeping requirements.

- Accessing records are a part of every GSA employee's job. However, employees may never remove records, regardless of media, from GSA without authorization from their supervisor. Employees involved in day-to-day GSA business must equally receive authorization before accessing and/or removing electronic files needed for working offsite.

- Employees who leave GSA cannot remove any non-personal records without their supervisor's approval and must return records not approved for removal before they leave the agency.

- It is common to maintain all types of information on a single computer at a single location. However, GSA employees must maintain personal papers, work in progress, and non-record materials separately from GSA records.

- The Records Management Coordinator (explained later in this Directive) must identify retired records stored within a region and disclose them to the Senior Records Officer if the location contains more than 20 linear feet; more than 20 containers of retired physical records, or more than 1 gigabyte of retired electronic records. Associated inventory descriptions and manifests (GSA Form 3711) of the records should likewise be shared.

- Offices that handle classified records must ensure they are maintained separately from unclassified records. Classified records should be stored in a secure location, whether paper or electronic. Records with classified portions must be stored and handled according to the Information Security handbook (CIO P 2100.1H) for the record with the highest classification level. Filing of unclassified and classified information is restricted to that information directly supporting, explaining, or documenting the record of the action and must be kept separately. In these cases, it is advisable to prepare a cross-reference page and place it in the unclassified file to indicate where the related classified records are located.

    - Information on the storage and destruction of classified information is available from the GSA Senior Agency Information Security Officer (SAISO) in the Office of the Chief Information Officer (OCIO).

Storage of records

To safely preserve records, storage is the first and best means of defense. Proper storage of both physical and electronic records is vital to being able to search and retrieve them. For specific National Archives and Records Administration regulations on the storage of records, go to http://www.archives.gov/records-mgmt/storage-standards-

toolkit/file8.pdf. To determine if a record is permanent or temporary, use the GSA Records Schedule (http://insite.gsa.gov/portal/content/500582).

- Permanent Records
  - Permanent Records are records, determined by the National Archives and Records Administration, to be permanent because of their continuing administrative, legal, scientific, or historical values. These records must be stored in a way that allows for their complete and organized transfer to National Archives and Records Administration.
  - Only a small percentage of records are identified and scheduled as being "permanent." When transferring permanent records to National Archives and Records Administration, GSA transfers all legal custody of permanent records to National Archives and Records Administration.
  - Electronic and audio/video records that have permanent worth should be discussed with the responsible Senior Records Officer.
  - Temporary and permanent records should be segregated. Records and non-records should be segregated.
- Temporary Records
  - Name and store temporary records so they can be located and easily retrieved as needed.
  - Segregate temporary and permanent records. Separate records and non-records, as well.
  - When electronic data systems are decommissioned, replaced, or significantly changed, archive records in electronic data systems in a non-proprietary manner. Archiving the records in this manner will ensure that they are still "readable" and can be destroyed or transferred as set forth by this policy. Applicability on legacy systems will be analyzed on a case by case basis, taking in consideration the cost and complexity of modifying a legacy system.
    - The term “Archived” is not the same as the term “Backed-up.” Customarily, “backing up” data refers to making an electronic copy of the data elsewhere for reinstatement if the original data is lost/destroyed. “Archiving” refers to storing a copy of the data in a non-proprietary format for easy retrieval after the originating system is no longer available. Even back-ups would be of no use in retrieving the records.
  - Every box of physical records stored locally, or at a professionally managed storage center, must have a box manifest in it (GSA Form 3711 or

equivalent). Each distinct group of boxes stored must be clearly and sequentially numbered on the outside of each box with a master copy of all of the box manifests in the group's first box.

- Send an electronic version of the master copy of all box manifests to the appropriate Senior Records Officer along with the associated storage location. Records sent to Federal Records Centers also require a Standard Form 135 – Records Transmittal and Receipt. The Standard Form 135 should be completed by the records owner and forward to the Records Management Coordinator, who will send the form electronically to the appropriate Senior Records Officer.

- Store Manifests (GSA Form 3711 or equivalent) for archived electronic records in an area accessible by the local Records Management Coordinator. These manifests may be needed during annual records inventories or by others authorized to search for and to access the records.

Retention of Records

Records, regardless of media, will be retained in accordance with the timeframes approved by the Archivist of the United States in GSA Records Schedules.

- Records that have a retention period of less than 180 days must be disposed of when no longer needed.

- Records that have a retention period longer than 180 days must be properly stored in an organized records management system and transferred to the Federal Records Center when no longer active.

- Records must not be destroyed before the end of their retention period. If there is a conflict with any authorities, they will be resolved by the Office of General Council.

- The GSA Records Schedule is found at: https://insite.gsa.gov/portal/content/500582

Destruction of records

Office file plans should contain accurate and up-to-date destruction authorities and retention periods for all records and non-records maintained in an office. Records should not be destroyed if there is a reasonable expectation that they will be needed for litigation or any investigation. Additionally, records should not be destroyed without previous approval of the records owner, Office of General Counsel and the Office of Inspector General.

- Temporary records (records that are not to be kept permanently), must be destroyed in a timely manner. However, agency records, physical or electronic, are not to be deleted or otherwise destroyed, except in accordance with this policy, which is consistent with National Archives and Records Administration regulations. GSA's authority to destroy records comes directly from the Archivist of the United States, who has approved GSA's Disposition Schedule. Records destruction cannot be done before the end of their retention period. Conflicts with any authorities will be resolved by the Office of General Counsel.

- Records covered by the Privacy Act are considered sensitive and offices must certify that they have been properly destroyed.

- Personal records and non-record information may be destroyed or removed at the discretion of the associate accumulating the information.

- All information systems, websites, mobile computing applications, and any other electronic systems containing GSA records must have disposition plans and be referenced in file plans.

- Large-scale destruction of records, regardless of media, such as those requiring assistance of outside companies, should be done without the knowledge and sign-off by the local Records Management Coordinator.

- If an employee or contractor knows of any actual or potential threat to records (e.g., removal, alteration, or destruction), contact the Office of Inspector General.

    - The Office of Inspector General or the Agency Records Officer must contact National Archives and Records Administration, as required by 44 U.S.C. 2905 and 3106 and 36 CFR 1230.14.

    - National Archives and Records Administration will assist the agency in the recovery of any unlawfully removed records, including contacting the Attorney General, if necessary.

    - Follow all agency internal reporting requirements, which may include reporting the threat to the agency's Office of General Council and to its Office of Inspector General.

Transferring Records

Records Transfers to National Archives and Records Administration

- The National Archives and Records Administration permanently preserve select historical records or records of continuing value (e.g. rights and interests). Permanent records are GSA documentary materials that are determined by National Archives and Records Administration to have sufficient historical or other value to warrant their continued preservation by the Government.
    - Only a small percentage of records are "Permanent."
    - When transferring permanent records to National Archives and Records Administration, GSA transfers all legal custody of those records to National Archives and Records Administration.
    - National Archives and Records Administration ensures preservation of permanent records and provides reference service to GSA and its customers.
    - National Archives and Records Administration will withhold information that is restricted under statute from the public.
- The Federal Records Centers operate under an Office of Management and Budget approved reimbursable program as the Records Center Program and are a functional operation within National Archives and Records Administration. These Centers provide low cost off-site storage of records for all Federal agencies.
    - Federal Records Centers provide temporary storage and reference services for records that are needed infrequently by the customer but are not yet eligible for disposal or transfer to the National Archives and Records Administration.
    - GSA records stored in a Federal Records Center remain in the legal custody of GSA.
    - The Senior Records Officers in conjunction with Records Management Coordinators are responsible for transferring records to the Federal Records Centers. Archives and Records Centers Information System (ARCIS) is a web-based system used by the Federal Records Centers to replace the need to mail or email forms for the transfer of records.

Responsibilities

GSA employees

All GSA employees are records custodians and are responsible for maintaining their records in accordance with Federal laws and regulations and GSA's records management policy. Employees have the following specific responsibilities:

- Understand privacy and security considerations. No record of any media, accessible by an employee or contractor, may be viewed without a clear need to know of the information contained in the record. The exception being when information contained in records—regardless of any media—is intended to be open to being viewed by anyone.

- Complete records management training every Fiscal Year (FY). Records management training courses are available on GSA's Online University (see Appendix C).

- New employees must take the training within the first 30 days of their employment start date. Records management training courses are available on GSA's Online University (see Appendix C).

- Maintain adequate records. Every employee is responsible for preserving records that adequately document the organization, functions, policies, procedures, decisions and essential transactions of GSA in their area of responsibility. Records can exist in email, Chatter, share drives, Google drive, chat within Gmail, file cabinets, and/or desks.

- Records (including those in email) that have a retention period longer than 180 days must be properly stored in an organized records management system. Adequate records also protect the government's legal and financial rights.

- Employees may never remove records, regardless of media, from GSA including when they are leaving the employment of GSA, without authorization from their supervisor, acting in accordance with GSA policies and procedures. Employees involved in day-to-day GSA business must equally receive authorization before accessing and/or removing electronic files needed for working offsite.

Signatory official

- Signatory officials are those employees whose signature is customarily required to make obligations and commitments on behalf of the agency. The following are signatory officials:

    - Administrator
    - Deputy Administrator

  - Regional Administrators
  - Head of Service and Staff Offices and other officials above the Division Director or equivalent level
  - Division Directors
  - Branch Chiefs
  - Section Chiefs
  - Contracting Officers; and
  - Career Civil Service associates and political appointees serving in positions equal to or comparable to those listed above.

- Signatory officials have the additional responsibility to send record copies of documents signed by them to the office(s) responsible for the functions to which the signed document applies. The responsible offices must ensure that records are disposed of as the law requires.

- Contracting Officers, Contracting Officer's Representative and Contract Oversight Managers are responsible for including in all contracts and agreements wording set forth by National Archives and Records Administration. Visit the National Archives and Records Administration website for the required language: http://www.archives.gov/records-mgmt/handbook/records-mgmt-language.html.

Administrator of General Services

- The Administrator of General Services is responsible for creating and preserving records that adequately and properly document the organization, functions, policies, decisions, procedures, and essential transactions of GSA.

- This role is delegated to the Chief Administrative Services Officer in the Office of Administrative Services (see ADM 5440.654) https://insite.gsa.gov/portal/content/567154.

Chief Administrative Services Officer

The Chief Administrative Services Officer, Office of Administrative Services, is responsible for the GSA National Records Management Program and provides GSA agency-wide leadership, planning, policy, and oversight of records management. The Chief Administrative Services Officer's responsibilities include:

- Incorporating records management requirements and policies into GSA's policy and planning framework.

- Designating GSA's Agency Records Officer.

- Communicating agency-wide records management federal requirements and agency goals, policies and procedures.

- Designating GSA's Records Branch Chief.

- Serving as the Senior Agency Official for Records Management.

GSA Agency Records Officer

The Agency Records Officer is GSA's subject matter expert for records management policy and National Archives and Records Administration regulations. The Agency Records Officer's responsibilities include:

- Providing guidance on the day to day agency recordkeeping requirements outlined in 36 CFR § 1222.22, Subpart B.

- Serving as the official GSA Records Management custodian of GSA's retired records to the National Archives and Records Administration.

- Serving as the point of contact for Records Management related issues to other Federal agencies, including the Office of Management and Budget (OMB), the Government Accountability Office (GAO), the Department of Justice (DOJ) and National Archives and Records Administration.

- Developing agency-wide records management policies and procedures.

- Coordinating and approving records schedules changes and the transfer of permanent records to National Archives and Records Administration.

- Providing guidance on policy and compliance to GSA organizations on establishing and maintaining effective records management practices.

- Representing GSA on the Federal Records Council and in other Federal records organizations.

- Managing reporting requirements for the Office of Management and Budget and the National Archives and Records Administration.

- Maintaining National Archives and Records Administration Records Management Certification.

Senior Records Officer

- A Senior Records Officer is responsible for implementing Records Management policy and procedures within an area of responsibility, with the exception of independent offices, who will work with Senior Records Officers at their discretion. A list of Senior Records Officers and Records Management Coordinators are available on InSite at https://insite.gsa.gov/portal/content/500582.

- One Senior Records Officer is assigned to the Federal Acquisition Service (FAS), one to the Public Buildings Service (PBS), and one to Central Office (covering all staff and independent offices).

- In addition, Senior Records Officers are assigned to cover the regions in a zonal capacity. Offices within the regions that operate essentially as extensions of the Central Office, should adhere to the agreed upon procedures and decisions of the Senior Records Officer responsible for the Central Office, unless an agreement exists between the Senior Records Officer of the Region and the Senior Records Officer of the Central Office.

- Senior Records Officers that reside in a regional location may also serve as that region's Records Management Coordinator, if requested by the Regional Administrator.

- Senior Records Officer's responsibilities include:

  - Assisting in the planning and implementing of information technology used for records management systems to make sure they conform to Federal statutory requirements, regulatory requirements and GSA policy.

  - Providing the requirements for records compliance, if records exist in an electronic data system, if it is a system of record.

  - Supporting their area of responsibility in developing file plans; and folder and file naming and indexing conventions.

  - Providing briefings to the Signatory Officials in their area of responsibility during the third quarter of each fiscal year.

  - Conducting exit briefings for senior officials (signatories above the level of Division Director) on the appropriate disposition of the records, including email, under their immediate control and document the briefings via emails to the departing officials and to the local Records Management Coordinator.

  - Providing a complete records inventory and file plan review to the Agency Records Officer every three years, due every third November, starting November 2014.

  - Advising and supporting the Records Management Coordinators on records management issues and promulgating records management policies and procedures.

  - Maintaining National Archives and Records Administration Records Management Certification.

Regional Administrator

Regional Administrator's responsibilities include:

- Ensuring the Records Management Coordinator maintains a records management plan (refer below for a description of the Records Management Coordinator). This plan consists of the local file plan, records maintenance procedures, electronic folder and file naming conventions, a local inventory of records, and security precautions.

- Designating at least one Records Management Coordinator for their region and forwarding the name to the region's Senior Records Officer within 30 days of the designation. If the designated Records Management Coordinator leaves, a new Records Management Coordinator must be appointed within 60 calendar days.

- Verifying the designated Records Management Coordinator has the appropriate authority and ability to perform their required responsibilities. This includes training, skills, resources, and time.

- Overseeing and carrying out the records management duties of this policy and procedure, such as having up-to-date file plans in place by appointing appropriate staff (in addition to the Records Management Coordinator), and assigning responsibility to a sufficient number of staff to ensure statutory requirements are fulfilled.

- Implementing procedures so records and other types of required documentary materials are protected from theft, loss, and unauthorized access or destruction by current and departing officials, employees, or other agents at GSA.

- Creating those records needed to ensure adequate and proper documentation of their organization.

Head of Service and Staff Offices

Head of Service and Staff Office's responsibilities include:

- Having their Records Management Coordinator maintain a records management plan (refer below for a description of the Records Management Coordinator). This plan consists of the local file plan, records maintenance procedures, electronic folder and file naming conventions, a local inventory of records, and security precautions.

- Designating at least one Records Management Coordinator for each office and location and forwarding that name to the Office's Senior Records Officer within 30 days after designation. If the designated Records Management Coordinator

leaves, a new Records Management Coordinator must be appointed within 60 calendar days.

- Verifying that the designated Records Management Coordinators have the appropriate authority and ability to perform their required responsibilities. This includes training, skills, resources, and time.

- Overseeing and carrying out the records management duties of this policy, such as having up-to-date file plans in place by appointing appropriate staff (in addition to the Records Management Coordinator), and assigning responsibility to a sufficient number of staff to ensure statutory requirements are fulfilled.

- Implementing procedures so records and other types of required documentary materials are protected from theft, loss, and unauthorized access or destruction by current and departing officials, employees, or other agents at GSA.

- The heads of the following offices are required to designate a Records Management Coordinator:

<u>Federal Acquisition Services (FAS) Central and Regional Office</u>

Office of Strategy Management
Office of Travel, Motor Vehicle, and Card Services
Office of Administration
Office of General Supplies and Services
Office of the Controller
Office of Integrated Technology Services
Office of the Chief Information Officer
Office of Assisted Acquisition Services
Office of Acquisition Management
Office of Customer Accounts and Research

<u>GSA– Staff Offices—Central and Regional Offices</u>

Office of Administrative Services
Office of the Chief Financial Officer
Office of the Chief People Officer
Office of General Counsel
Office of Small Business Utilization
Office of Government-wide Policy
Office of the Chief Information Officer
Office of Congressional and Intergovernmental Affairs
Office of Communications and Marketing
Office of Citizen Services and Innovative Technologies
Office of Civil Rights
Office of Mission Assurance

Regional Administrators

Independent Offices

Office of Inspector General
Civilian Board of Contract Appeals

Public Buildings Service (PBS) Central Office and Regional Offices

Office of Client Solutions
Office of Acquisition
Office of Real Estate Acquisition
Office of Budget and Financial Management
Office of Facilities Management and Services Program
Office of Real Property Asset Management
Office of Design and Construction

Records Management Coordinator

Records Management Coordinator's responsibilities include:

- Supporting the records management program within their area of responsibility through the knowledge of their areas programmatic, administrative records and records inventory.

- Knowing the agency's records management policies, plans, types, and dispositions. The timely transfer of permanent records to National Archives and Records Administration.

- Identifying record types in use within their area of responsibility, ensuring records retention and disposition instructions are communicated to records custodians, and promulgating the most responsive and cost-effective means for managing records.

- Segregating records of independent offices that require special handling, such as "Law Enforcement Sensitive," and making appropriate accommodations for such records, such as using generic descriptions when transferring to National Archives and Records Administration.

- Completing the advanced records management training course in GSA's Online University each fiscal year.

- Establishing office-wide electronic file and folder naming conventions and procedures so that records are maintained in such a manner that they are readily retrievable, and disposed of in accordance with the established agency file plan.

  - Offices within regions that operate essentially as extensions of the Central Office should adhere to the Central Office naming convention, unless both the Central Office Head and the Regional Administrator mutually agree to adhere to a regional naming convention.

- Supporting Senior Records Officers with:
  - Records inventories and reporting requirements.
  - Draft records schedule change requests for records created and maintained by their organization that do not exist in the GSA File Plan.
  - Review file plans and procedures during the three year records inventory process to ensure file plan(s) is/are current.
  - Notifying Senior Records Officers of opportunities to assist in the planning and implementing of information technology used for records management solution.

- Records Management Coordinators for the Office of Inspector General and Civilian Board of Contract Appeals have the additional authority to coordinate with the Agency Records Officer directly on all record management matters at all levels.

Chief Information Officer (CIO)

The Office of the CIO is responsible for incorporating recordkeeping requirements provided by OAS into GSA's electronic systems planning, design, acquisition, implementation and maintenance. Contemporary records creation and management primarily exist in electronic format. Electronic data systems house the majority of GSA's official record material, whether it is distributed across databases or in single files such as Adobe or Microsoft Word documents. Current records management laws and executive orders define specific responsibilities for offices that design, develop and manage electronic systems. The CIO's main recordkeeping responsibilities per federal law, OMB Circulars and OMB Directives include:

- Establishing procedures for addressing records management requirements, including recordkeeping requirements and disposition before approving new electronic information systems or enhancements to existing systems. Reference 36 CFR 1236.10.

- Incorporating records management and archival functions into the design, development, and implementation of information systems. Reference OMB Circular A-130, par. 8a (k).

- Incorporating recordkeeping requirements into all GSA investments during the capital planning process. Reference OMB Circular A-11.

- Implementing and enforcing applicable records management procedures, including requirements for archiving information maintained in electronic format, particularly in the planning, design, and operation of information systems. Reference Paperwork Reduction Act, §3506 par.(f).

- Managing the systems that contain permanent electronic records in an electronic format by December 31, 2019. Storing all permanent and temporary email records in an accessible electronic format by December 31, 2016. Reference OMB/ National Archives and Records Administration Directive M-12-18.

Additionally, Information Technology manager's responsibilities include:

- Working with Records Management Coordinators and Senior Records Officers to establish and update records schedules and record management requirements for electronic systems.

- Implementing proper record management procedures for existing information systems and verifying record management requirements are included in any proposed system; specifically the use of National Archives and Records Administration's General Records Schedule 20 "Electronic Systems."

- Incorporating Records Management (records capture, retrieval and retention according to GSA and National Archives and Records Administration disposition schedules) and archival functions (or manual archival processes) into the design, development, and implementation of the information system. This task should be performed by including the appropriate Records Management Coordinators and Senior Records Officers. Every electronic data system developed or acquired for the agency requires a Disposition Plan approved by an agency Senior Records Officer.

- Developing Disposition Plans and associated procedures for archiving data in a non-proprietary format, when data needs to be saved beyond the life of the system where it is stored. These systems include information systems, websites, mobile computing apps, and any other electronic system containing GSA records.

- Working with Records Management Coordinators and Senior Records Officers to transfer permanent records to National Archives and Records Administration in accordance with approved records schedules and National Archives and Records Administration requirements.

- Incorporating records management and archival functions (or manual archival processes) into any system acquired or developed, and including the Records

Management Coordinator and Senior Records Officer for record management in the planning of systems. Any electronic system acquired or developed requires a Disposition Plan approved by the appropriate Senior Records Officer.

Program Manager

Program managers have a primary responsibility for creating, maintaining, protecting, and disposing of records for their program area in accordance with GSA policy. Program Manager's responsibilities include:

- Creating the records needed to ensure adequate and proper documentation of their area of responsibility.
- Implementing procedures to protect records from theft, loss, unauthorized access, and unauthorized removal.
- Cooperating with Records Management Coordinators in requests for information and in the management of records.
- Notifying their Records Management Coordinators of organization or program changes that will result in establishment of new types of records, new uses of existing records, the transfer or termination of records no longer required, or a needed increase or decrease in the retention time of the records.

Office of the General Counsel

The Office of General Counsel notifies the Agency Records Officer of record litigation holds and other records freezes, and provides instructions directly to affected employees on retaining any potentially relevant records.

Appendix A. - Authorities

Authorities. According to Federal law (44 U.S.C. 2901), records management means: "the planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to records creation, records maintenance and use, and records disposition in order to achieve adequate and proper documentation of the policies and transactions of the Federal Government and effective and economical management of agency operations."

GSA's Records Management Program operates under the following authorities:

- 44 U.S.C. Chapter 31 – Records Management by Federal Agencies (Federal Records Act): http://www.archives.gov/about/laws/fed-agencies.html
- 44 U.S.C. Chapter 33 – Disposal of Records: http://www.archives.gov/about/laws/disposal-of-records.html
- 44 U.S.C. Chapter 35 – Coordination of Federal Information Policy (Paperwork Reduction Act of 1980, as amended, Paperwork Reduction Reauthorization Act of 1995, and Government Paperwork Elimination Act): http://www.archives.gov/about/laws/fed-information-policy.html
- 36 CFR Chapter XII, Subchapter B – Records Management: http://www.archives.gov/about/regulations/subchapter/b.html
- 36 CFR 1220.34 - What must an agency do to carry out its records management responsibilities: http://www.law.cornell.edu/cfr/text/36/1220.34
- OMB Circular A-123 – Management's Responsibility for Internal Control: http://www.whitehouse.gov/omb/circulars/a123/a123_rev.html
- OMB Circular A-130 – Management of Federal Information Resources: http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html
- Executive Order 12656 – Assignment of Emergency Preparedness Responsibilities Part 18, Sec. 1801(3): https://www.fas.org/irp/offdocs/EO12656.htm
- 2430.1 ADM – General Services Administration Continuity Program: https://insite.gsa.gov/portal/content/521730
- 2450.1 ADM – Alternate Sites for Continuity of Operations Plan (COOP) Relocation: https://insite.gsa.gov/portal/content/518978

- Federal Emergency Management Agency (FEMA) Federal Preparedness Circular 65 - Federal Executive Branch Continuity of Operations (COOP): http://www.fas.org/irp/offdocs/pdd/fpc-65.htm

- Federal Records Act of 1950 (44 U.S.C. chs. 21, 29): http://www.gpo.gov/fdsys/browse/collectionUScode.action?collectionCode=USCODE

- Freedom of Information Act (FOIA) (5 U.S.C. 552) and the Privacy Act (PA) of 974 regulate public access to Federal records: http://www.gpo.gov/fdsys/browse/collectionUScode.action?collectionCode=USCODE

- 18 U.S.C. 2071 - Penalties for unlawfully removing or destroying records: http://www.gpo.gov/fdsys/granule/USCODE-2011-title18/USCODE-2011-title18-partI-chap101-sec2071/content-detail.html

- Executive Memorandum M-12-18, Managing Government Records Directive: http://www.whitehouse.gov/sites/default/files/omb/memoranda/2012/m-12-18.pdf

Related documents.

The following publications prescribe actions and operational procedures to be followed by GSA:

- ISO 15489-1:2001 – Information and Documentation – Records Management – Part 1: General

- ISO/TR 15489-2:2001 – Information and Documentation – Records Management – Part 2: Guidelines

- Memo on Increasing Data Sharing, Transparency and Reuse at GSA – February 14, 2014: can be found at GSA's Records Management website: http://insite.gsa.gov/portal/content/500582

- CIO 2100.1K - GSA Information Technology (IT) Security Policy; can be found on GSA's InSite Website: https://insite.gsa.gov/portal/content/553345.

- Additional documents, including forms, and other relevant information are maintained on GSA's Records Management website: http://insite.gsa.gov/portal/content/500582

Appendix B. - Definitions

Records

- Definition. The term "records" according to 44 U.S.C. 3301, includes all books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, that are:
    - Made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business; and
    - Preserved or appropriate for preservation by that agency (or its legitimate successor) as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in them.
- If documentary material is made or received by a GSA associate when performing their assigned duties, it is presumed to be a record, and safeguards should be instituted to prevent unauthorized destruction/deletion or removal from GSA electronic systems or physical files.
- Examples. The following are examples of records:
    - The official file copy of any Government business document;
    - Any classified document;
    - Any document containing information required to transact the official business of GSA;
    - Any document used in or documenting an official decision of the agency;
    - Any information provided to GSA that has been identified as a trade secret or proprietary information; and
    - Electronic data in shared information systems may be records; it is up to system owners to determine what record types exist in the system.
    - With email, it is up to the GSA employee to determine if the email is a record or not. Any email meeting the definition of a record, such as those requiring a decision or authorizing an action.
    - When a record is migrated from one format or media to another, both the data and associated metadata/associated supporting and descriptive data, (such as the author and date of an email), should be migrated to the new storage media or formats so that records in their totality are retrievable and usable as

long as needed to conduct agency business and to meet National Archives and Records Administration approved dispositions.

Non-record materials and copies of records

- Definition: Informational materials kept for convenience of reference.
- Examples. The statute that defines records (44 U.S.C. 3301; cited in par. 5a) sets out three types of non-record materials:
  - Extra copies of documents and other materials that an associate drafts, signs, reviews, or otherwise acts upon, provided that the record copies are properly filed;
  - Library materials acquired solely for reference; and
  - Stocks of forms, publications and processed documents.

Personal files

- Definition: Documentary materials containing information that is created and maintained solely for personal use and reference.
- Examples. Papers that may be considered personal include:
  - Personal calendars, appointment books, schedules, and diaries created solely for the convenience of the GSA associate in managing his/her time;
  - Documentary materials created on Government time, using Government equipment and supplies, which do not document Government activity and therefore do not meet the standard for record status, or personal copies of records of interest to the associate; and
  - Personal files should be filed separately from the record, and marked as "Personal files."

Appendix C. - Required Records Management Program Training

Records Management Training

- Employees are required to take records management training each fiscal year to understand what constitutes a record, and how to manage records in accordance with GSA's recordkeeping requirements and Federal laws and regulations.

- New employees must take this training within the first 60 days of their employment start date. Records management training courses are available on GSA's Online University.

- Beginning in Fiscal Year (FY) 2014, the Agency Records Officer and Senior Records Officers are required to have a National Archives and Records Administration records management training certification. This certification should be obtained within one year of their designation.

- The Agency Records Officer and Senior Records Officer must stay current with all needed records management training including on National Archives and Records Administration Bulletins, National Archives and Records Administration's Electronic Records Archives (NARA ERA) and National Archives and Records Administration's Archives and Records Centers Information System (NARA ARCIS).