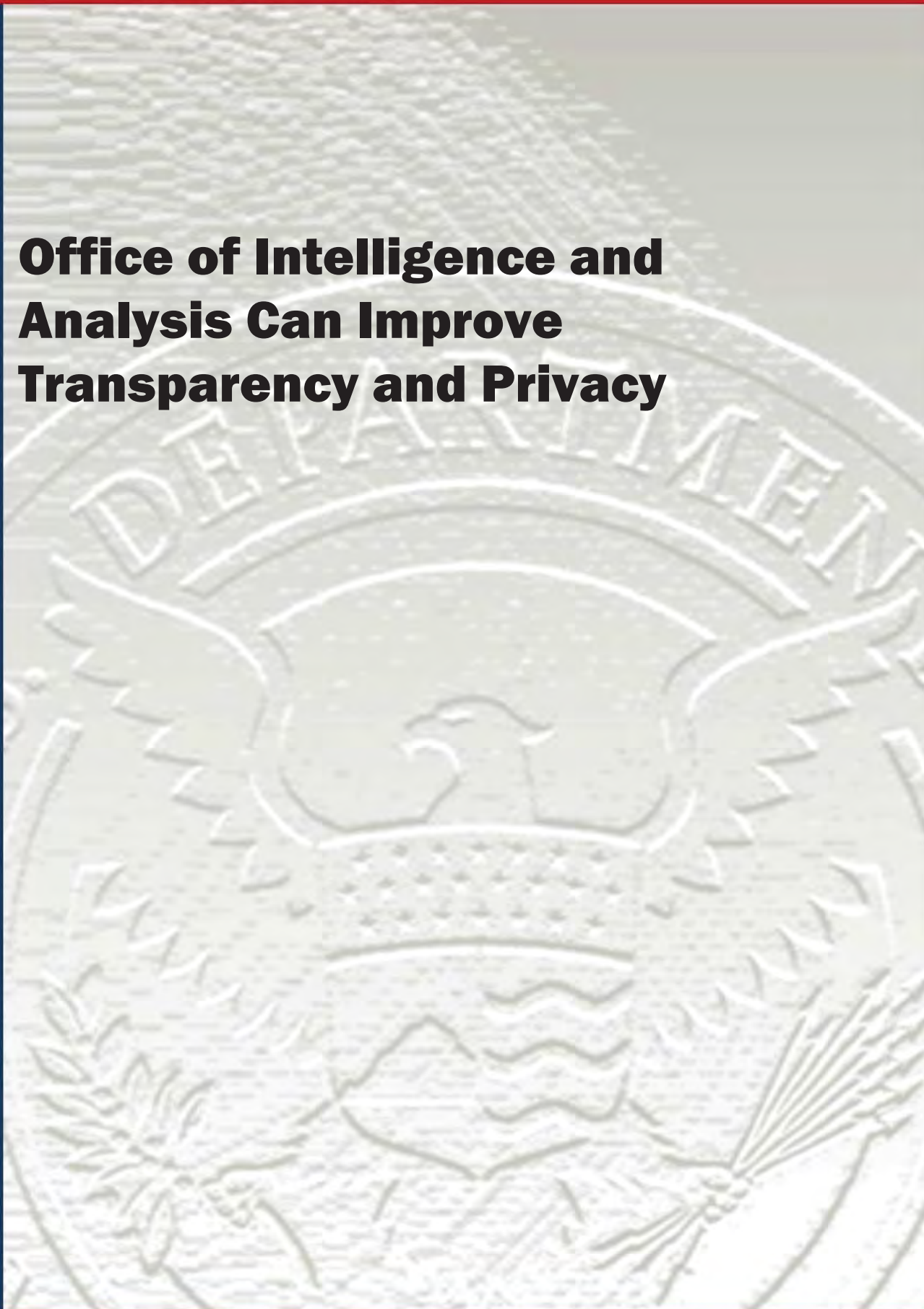


Office of Intelligence and Analysis Can Improve Transparency and Privacy





DHS OIG HIGHLIGHTS

Office of Intelligence and Analysis Can Improve Transparency and Privacy

May 17, 2016

Why We Did This Audit

We evaluated the Office of Intelligence and Analysis' (I&A) safeguards for the sensitive privacy and intelligence information it collects and maintains. Our objective was to determine whether I&A ensures compliance with Federal laws, regulations, and policies.

What We Recommend

We are making six recommendations to I&A, which, if implemented, should reduce the risk to privacy and intelligence information.

For Further Information:

Contact our Office of Public Affairs at (202) 254-4100, or email us at DHS-OIG.OfficePublicAffairs@oig.dhs.gov

What We Found

I&A has made progress in developing a culture of privacy. Specifically, I&A has centralized the oversight of privacy and civil liberties and has been working to ensure that it meets the requirements of pertinent legislation, regulations, directives, and guidance. I&A conducted specialized onboarding and advanced training that address safeguards for privacy and civil liberties in its intelligence processes. In addition, I&A designed intelligence oversight reviews to ensure that its employees observe the required safeguards.

However, I&A has faced challenges because it did not place priority on institutionalizing other capabilities and processes to ensure timely and complete compliance with requirements regarding privacy and intelligence information. Specifically:

- I&A has not responded timely to requests for agency transparency under the *Freedom of Information Act*, potentially creating financial liabilities.
- I&A continuity capabilities have not had an adequate oversight structure, risking the loss of essential records and intelligence information in an emergency.
- I&A has not implemented an infrastructure for risk assessment and end-to-end monitoring of high-impact solicitations and contracts that would ensure safeguards for sensitive data and systems throughout the acquisition processes.

I&A Response

I&A concurred with all six recommendations.



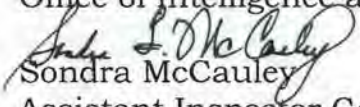
OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

May 17, 2016

MEMORANDUM FOR: The Honorable Brigadier General Francis X. Taylor
Under Secretary for Intelligence and Analysis
Office of Intelligence and Analysis

FROM: 
Sondra McCauley
Assistant Inspector General
Office of Information Technology Audits

SUBJECT: *Office of Intelligence and Analysis Can Improve
Transparency and Privacy*

Attached for your action is our final report, *Office of Intelligence and Analysis Can Improve Transparency and Privacy*. We incorporated the formal comments provided by your office.

The report contains six recommendations aimed at improving transparency and privacy. Your office concurred with these six recommendations. As prescribed by the Department of Homeland Security Directive 077-01, *Follow-Up and Resolutions for the Office of Inspector General Report Recommendations*, within 90 days of the date of this memorandum, please provide our office with a written response that includes your (1) agreement or disagreement, (2) corrective action plan, and (3) target completion date for each recommendation. Also, please include responsible parties and any other supporting documentation necessary to inform us about the current status of the recommendation. Until your response is received and evaluated, the recommendations will be considered open and unresolved.

Once your office has fully implemented the recommendations, please submit a formal closeout letter to us within 30 days so that we may close the recommendations. The memorandum should be accompanied by evidence of completion of agreed-upon corrective actions and of the disposition of any monetary amounts. Please send your response or closure request to OIGITAuditsFollowup@oig.dhs.gov.

Consistent with our responsibility under the *Inspector General Act*, we will provide copies of our report to congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post the report on our website for public dissemination.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Please call me with any questions, or your staff may contact Marj Leaming, Director of Information Privacy and Security Division, at (202) 254-4172.

Attachment



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Table of Contents

Background	3
Results of Audit	6
I&A Progress in Complying with Privacy Requirements	7
I&A Faces Challenges in Protecting Sensitive Data	9
Responding to <i>Freedom of Information Act</i> Requests	9
Recommendations	14
Continuity Capability for Safeguarding Essential Records and Intelligence Information	15
Recommendations	17
Securing Sensitive Information in Acquisitions.....	18
Recommendation	20

Appendixes

Appendix A: Objective, Scope, and Methodology	21
Appendix B: I&A Comments to the Draft Report.....	22
Appendix C: Office of Information Technology Audits Major Contributors to This Report	25
Appendix D: Report Distribution.....	26

Abbreviations

CEWG	Continuity and Exercise Working Group
COOP	continuity of operations
ERMS	electronic records management system
EO	Executive Order
FCD	Federal Continuity Directive
FOIA	<i>Freedom of Information Act</i>
HSAR	Department of Homeland Security Acquisition Regulations



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

I&A	Office of Intelligence and Analysis
ICB	Information Compliance Branch
ISE	information sharing environment
IT	information technology
NARA	National Archives and Records Administration
NIST	National Institute of Science & Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
PII	personally identifiable information



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Background

The Office of Intelligence and Analysis (I&A) ensures that information related to threats is collected, analyzed, and disseminated to relevant customers. I&A is involved in the routine collection, maintenance, or use of intelligence information, which may include personally identifiable information (PII). I&A provides intelligence support across the range of Department of Homeland Security missions, including preventing terrorism and enhancing security, securing and managing our borders, enforcing and administering our immigration laws, and safeguarding cyberspace. I&A is part of a larger Homeland Security Enterprise that includes departmental leaders and components; state, local, tribal, territorial, and private sector partners; and other Intelligence Community members, all of whom require and generate homeland security information and intelligence. Table 1 indicates the various purposes for which I&A collects or uses PII to carry out its mission.

Table 1. PII Collected by I&A

I&A Source	PII From Whom?	What PII May be Collected?
DHS State, Local, and Regional Fusion Center Initiative	Any person deemed a suspect, witness, or other person of interest whose actions or statements are “reasonably believed to be” in a collection category (knowledge or involvement in an act of terrorism, terror-related event or incident)	Relevant information, including PII in any form, may be collected for the purposes of preventing, disrupting, or halting terrorism-related incidents and for analytical purposes to identify possible trends and provide general analytical products that inform other components as well as non-Federal users, agencies, or organizations.
DHS Information Sharing Environment Suspicious Activity Reporting Initiative	Suspects or witnesses of terror-related activity or events; DHS employees, contractors, submitters, or analysts; private sector officials whose agency is part of the Nationwide Suspicious Activity Reporting Initiative	PII may relate to identifying, assessing, or analyzing threats of a terroristic nature.

Source: Office of the Inspector General (OIG)-compiled from I&A documentation

Various laws, executive orders, regulations, and policies ensure the protection of privacy rights and civil liberties of United States Persons.¹ The *Privacy Act of*

¹ United States Person means a United States citizen, an alien known by the intelligence agency concerned to be a permanent resident alien, an unincorporated association substantially composed of



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

1974, as amended, imposes various requirements on agencies whenever they collect, use, or disseminate PII. The *Privacy Act* establishes Fair Information Practice Principles that govern the collection, maintenance, use, and dissemination of PII about individuals in systems of records maintained by Federal agencies. The *Intelligence Reform and Terrorism Prevention Act of 2004* requires the issuance of guidelines to protect privacy and civil liberties in the development and use of the “information sharing environment” (ISE).

Executive Order (EO) 12333, *United States Intelligence Activities*, dated December 4, 1981, defines protected information for the Intelligence Community. Specifically, the U.S. Government is obligated, in the conduct of intelligence activities under this order, to protect fully the legal rights of all U.S. Persons, including freedoms, privacy, and civil liberties guaranteed by Federal law. EO 12333 was amended by EO 13470 in 2008 to strengthen the role of intelligence activities. EO 13388, *Further Strengthening the Sharing of Terrorism Information to Protect Americans*, provides guidelines for ensuring information privacy, civil liberties, and legal rights of Americans in the development and use of the ISE. Further, ISE Privacy Guidelines ensure that the information privacy and other legal rights of Americans are protected in the development and use of the ISE.

The ISE requires that each agency designate a senior official for information privacy issues, as designated by statute or executive order, or as otherwise identified in response to Office of Management and Budget (OMB) Memorandum M-05-08, dated February 11, 2005. The *Homeland Security Act of 2002*, as amended, requires that the DHS Secretary appoint a senior official in the Department who shall report directly to the Secretary, to assume primary responsibility for privacy policy, as well as for being familiar with the agency’s activities as they relate to the ISE, such as:

- ensuring the agency’s policies, procedures, and systems are appropriately designed and executed in compliance with the ISE Privacy Guidelines;
- providing intelligence oversight training to personnel authorized to share protected information through the ISE regarding the agency’s requirements and policies for the collection, use, and disclosure of protected information;²
- reporting violations of agency privacy protection policies;

United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments.

² Intelligence Oversight training applies to Federal employees, contractors, detailees, and individuals who perform foreign intelligence or counterintelligence functions.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

- receiving reports (or copies thereof if the agency already has a designated recipient of such reports) regarding alleged errors in protected information that originate from that agency;
- implementing adequate review and audit mechanisms to enable the agency's ISE privacy official and other authorized officials to verify that the agency and its personnel are complying with the guidelines for the development and use of the ISE; and
- executing authority and resources, as appropriate, to identify and address privacy and other legal issues arising out of the agency's participation in the ISE.

In addition, the *E-Government Act of 2002* requires Privacy Impact Assessments on systems of records, including I&A's information technology (IT) systems containing PII and other activities with potential privacy impacts. The Privacy Policy Guidance Memorandum 2008-02, *DHS Policy Regarding Privacy Impact Assessments*, December 30, 2008 and the *DHS Instruction 047-01-001, Privacy Policy and Compliance*, implement this legislation within the Department. The DHS Deputy Secretary's "Memorandum Designation of Component Privacy Officers," dated June 5, 2009, directs each of the Department's 10 major components, including I&A, to designate a senior-level Federal employee as a full-time Privacy Officer. Also, I&A is required to designate a Privacy Officer per Intelligence Community Directive 107. Privacy Officers are to:

- oversee implementation of Federal privacy law and regulations and DHS privacy policies and guidance;
- report on privacy program,³ activities and accomplishments;⁴
- provide component personnel with mandatory annual privacy training developed by the DHS Privacy Office, as well as advanced or supplementary training, as needed;
- address complaints and incidents; and
- manage records retention schedules.

However, an organization's culture of privacy results from how well the privacy commitment is understood, implemented, and enforced by executive management, the Office of the Chief Information Officer, the Privacy Office, and program offices, managers, and employees in their respective roles. Promotion of an effective culture of privacy leads to embedded shared attitudes, values, goals, and practices for complying with the proper handling of PII.

³ A privacy program is a comprehensive approach to managing privacy compliance and risk in programs and activities.

⁴ OMB Memorandum M-15-01, *Fiscal Year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices*, October 3, 2014.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Results of Audit

We evaluated the safeguards for sensitive privacy and intelligence information collected and maintained by I&A. Our objective was to determine whether I&A ensures compliance with applicable Federal laws, regulations, and policies. We examined internal controls for managing all I&A information but did not look at classified content as part of this audit.

I&A has made progress in developing a culture of privacy. Specifically, I&A centralized the oversight of privacy, civil liberties, and intelligence information under its I&A Intelligence Oversight Officer/Information Compliance Branch (ICB) Chief. Among other functions, this Branch has been responsible for ensuring proper handling of sensitive data, preparing documentation, and reporting on I&A's privacy activities. The ICB assisted in developing a culture of compliance with pertinent Federal laws, regulations, and policies, such as the *Freedom of Information Act*, *Federal Executive Branch National Continuity Program and Requirements*, *Improving Cybersecurity Protections in Federal Acquisitions*, and EO 12333. In addition, the I&A Intelligence Oversight Officer conducted reviews of intelligence operations to ensure safeguards are observed and provided intelligence oversight training emphasizing requirements for the privacy and civil rights of U.S. Persons.

However, I&A faces challenges because it did not place priority on institutionalizing other capabilities and processes needed to ensure timely and complete compliance with requirements regarding privacy and intelligence information. Specifically:

- I&A did not timely respond to requests for agency transparency under the *Freedom of Information Act*, potentially creating financial liabilities.
- I&A continuity capabilities did not have an adequate oversight structure, risking the loss of essential records and intelligence information in an emergency.
- I&A did not implement an infrastructure for continuous risk assessment and end-to-end monitoring of high-impact solicitations and contracts that would ensure safeguards for sensitive data and systems throughout the acquisition processes.

We are making six recommendations to I&A, which if implemented, should reduce the risks to privacy and intelligence information.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

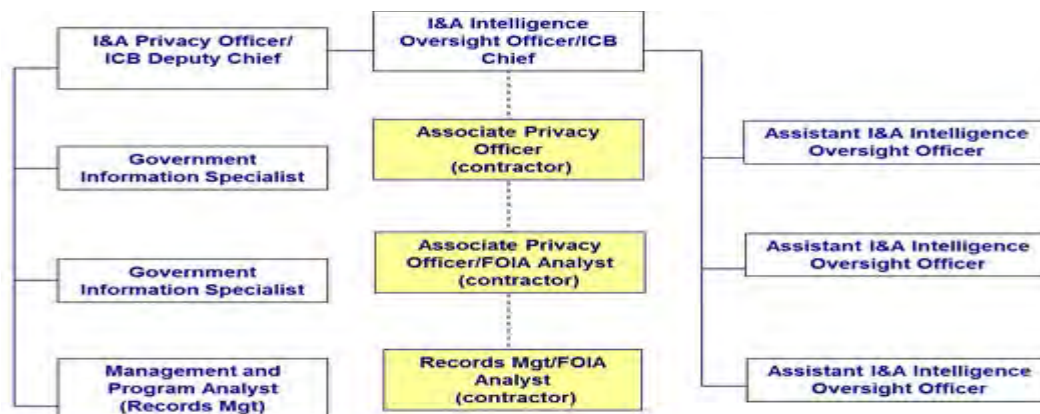
I&A Progress in Complying with Privacy Requirements

I&A has made progress in developing a culture in which employees are trained and work daily to safeguard privacy and civil liberties of U.S. Persons. I&A has instituted a centralized approach to ensuring compliance with pertinent legislation, regulations, directives, and guidance.

Oversight Structure for Complying With Privacy Requirements

I&A's Intelligence Oversight Officer/ICB Chief has responsibility for managing a comprehensive intelligence oversight program. There are three Assistant I&A Intelligence Oversight Officer positions under the ICB Chief to provide specialized and advanced training on privacy and civil liberties and review I&A's intelligence processes to ensure that safeguards are observed. I&A's Privacy Office had one Federal employee and one contractor for assistance. The Freedom of Information Act (FOIA) Officer and the Records Management Officer also each had one contractor for assistance. The organizational structure for the oversight of the privacy, FOIA, and intelligence information compliance at the time of our field work is shown in figure 1.

Figure 1. Information Compliance Branch



Source: I&A organization chart

According to I&A's Intelligence Oversight Officer/ICB Chief, the branch has the following responsibilities for:

- overseeing I&A's implementation of Federal privacy law and regulations, including compliance with the ISE Guidelines;
- conducting privacy threshold analyses for National Security Systems;
- ensuring employee and contractor completion of mandatory annual privacy training developed by the DHS Privacy Office;



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

- providing specialized training regarding I&A's requirements and policies for collection, use, and disclosure of protected information;
- conducting privacy and civil liberties risk assessments as part of I&A's intelligence oversight review program;⁵
- managing I&A's records retention and disposal schedules;
- addressing and reporting complaints and violations of I&A's privacy protection policies; and
- reporting on privacy activities and accomplishments.

Mandatory Annual Privacy and Civil Liberties Training

Routine training is a key element of developing and maintaining an effective privacy culture. I&A has used the DHScovery online learning system to provide training for new hires and DHS employees annually. This training, entitled "Privacy at DHS: Protecting Personal Information," meets the mandatory privacy training requirements of OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*.

Also, the Intelligence Oversight Officer provided specialized onboarding and an annual 2-hour training course, "DHS I&A Intelligence Oversight Training," addressing requirements when information on U.S. Persons is collected, retained, or disseminated. This training is designed for Federal employees, contractors, detailees, and individuals responsible for performing foreign intelligence or counterintelligence functions.

Intelligence Oversight Inspections to Ensure Compliance with Privacy Guidelines

The I&A Intelligence Oversight Officer conducted an Intelligence Oversight Program to ensure observance of the requisite safeguards. This program includes inspections during which the Officers ensure compliance with EO 12333 and other pertinent requirements. Review areas include: (a) authorized collection, retention, and dissemination of intelligence; (b) proper marking of intelligence materials; (c) tracking of hard and soft copy files containing information on U.S. Persons; and (d) information dissemination within the Intelligence Community. The program includes a combination of inspections and training to assess the extent to which I&A personnel have been complying with the ISE Privacy Guidelines.

⁵ A national security system is a telecommunications or information system operated by the Federal Government, the function, operation, or use of which involves intelligence activities, cryptologic activities related to national security, command and control of military forces, equipment that is an integral part of a weapon or weapons system, or is critical to the direct fulfillment of military or intelligence missions. [40 U.S.C. section 11103(a)]



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

I&A Faces Challenges in Protecting Sensitive Data

Although it has made progress, I&A faces challenges protecting the sensitive data it collects and manages to conduct its mission. Specifically:

- I&A did not timely respond to requests for agency transparency under the *Freedom of Information Act*, potentially creating financial liabilities.
- I&A continuity capabilities did not have an adequate oversight structure, risking the loss of essential records and intelligence information in case of an emergency.
- I&A did not implement an infrastructure for risk assessment and end-to-end monitoring of high-impact solicitations and contracts that would ensure safeguards for sensitive data and systems throughout the acquisition processes.

Lacking such improvements, accountability, and internal controls, I&A could not ensure adequate protection of sensitive data to support its mission operations.

Responding to *Freedom of Information Act* Requests

I&A did not always timely respond to requests for agency transparency under FOIA. FOIA provides any person the right, enforceable in court, to submit written requests for access to Federal agency records or information. All Federal Executive branch agencies must respond to FOIA requests within 20 business days for simple requests and up to 30 business days for complex requests. However, an agency may extend this response time by writing to the requestor and offering the opportunity to modify or narrow the initial request, which may shorten the overall time to complete the agency response. If an agency is not responsive, the requestor of government information has the right to an administrative appeal or may file a lawsuit in Federal district court. I&A inaction or tardiness could result in an investigation, forfeited fees, and costs related to a legal action.

Backlog of FOIA Requests

According to our review of I&A's response times to FOIA requests for fiscal year 2013, FY 2014, and FY 2015 (October 2014 through August 2015), I&A has not consistently met the timeliness requirements. New and unresolved FOIA requests have been carried over from year to year. Figure 2 shows trend lines for I&A's FOIA workload from FY 2013, FY 2014, and FY 2015 (11 months).

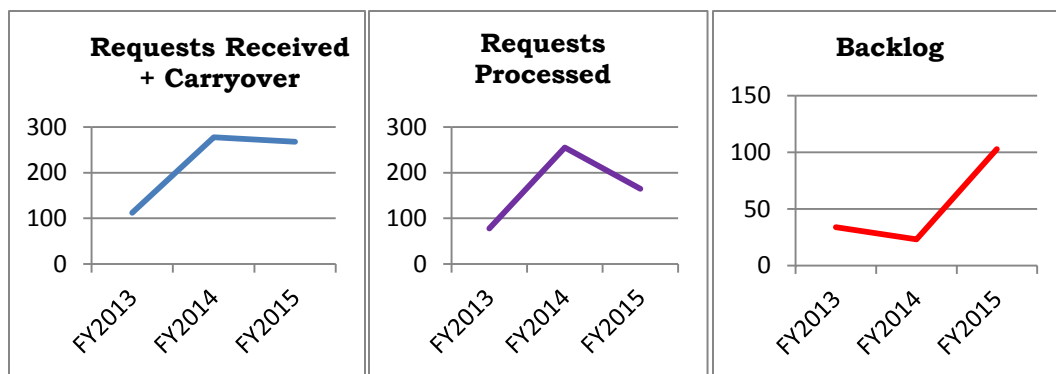


OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

- The first chart in figure 2 shows an increase in the combined number of new requests since FY 2013, including unresolved requests carried over from prior fiscal years (i.e., Requests Received + Carryover). Carryover of Requests includes new requests received and those requests that I&A was unable to process or that remained unresolved from the prior fiscal year(s).
- The second chart in figure 2 shows an increase in resolving requests in FY 2014 (i.e., Requests Processed). Total Requests Processed refers to those requests that I&A resolved during the fiscal year.
- The third chart in figure 2 shows an increase in workload (i.e., Backlog) since FY 2014. Unresolved requests accumulate over fiscal years as part of I&A's total backlog. The Annual Workload is the combination of new, processed, and unresolved requests during each fiscal year.

Figure 2. Trends in I&A's FOIA Workload



Source: DHS FOIA Reports from I&A (FY 2013-FY 2014) and I&A Monthly FOIA reports for FY 2015 (October 2014 through August 2015)

Table 2 shows I&A FOIA Office Productivity Metrics for FY 2013, FY 2014, and FY 2015 (October 2014 through August 2015). The table illustrates how the total number of new requests and carry-over of old or unresolved requests (i.e., backlog) increased from 112 in FY 2013 to 278 in FY 2014, and then decreased to 247 by August 2015 constituting a net increase of 121 percent. Over this same period of time, the backlog of all FOIA requests increased by 203 percent. I&A's continued delays in addressing the FOIA workload could result in litigation and forfeiture of fees.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Table 2. I&A FOIA Office Productivity Metrics FY 2013, FY 2014, FY 2015 (October 2014 through August 2015)

I&A FOIA Workload	FY 2013	FY 2014	FY 2015 (through August)	Percentage Change for this period of time
New Requests and Backlog Requests from Prior Year(s)	112	278	247	121% increase
Total Requests Processed	78	255	144	85% increase
Backlog of All Requests	34	23	103	203% increase
Staffing Levels (full time) to Manage FOIA Workload	3	2.7	2.4	20%

Source: DHS FOIA Reports from I&A (FY 2013 and FY 2014) and I&A Monthly FOIA reports for FY2015 (October 2014 through August 2015)

Inadequate Staffing Hindered I&A's Efficiency in Resolving FOIA Requests

This backlog of unaddressed FOIA requests continued growing because I&A did not have the resources necessary to address them. Processing complex FOIA requests entailed identifying, tracking, and providing pertinent information, as well as maintaining communications with requesters to keep them updated on the status of their requests. However, I&A's FOIA Office had inadequate staffing to manage the workload. Table 2 above shows how I&A FOIA Office staffing decreased from 3 in FY 2013 to 2.4 in FY 2015 (from October 2014 through of August 2015), representing a change of negative 20 percent.

Compared to some DHS components, I&A was understaffed in relation to the number of FOIA requests received in FY 2014. Table 3 compares the total number of full-time FOIA employees and the corresponding average workload at I&A to two other DHS components—the Federal Emergency Management Agency and the OIG.

Table 3. FOIA Requests Received and Staffing Within I&A and Two DHS Components

DHS Component	Number of "Full Time FOIA Employees"	Average Requests Received per FOIA Employee
Office of Intelligence and Analysis	2	122
Federal Emergency Management Agency	13	59
Office of Inspector General	4	44

Source: OIG Analysis of DHS FOIA Report for FY 2014



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

In actual numbers, I&A received 244 requests, the Federal Emergency Management Agency had 772 requests, and the OIG had 177 requests for FY 2014.

Without adequate FOIA Office staff, I&A may not be able to resolve its backlog as new FOIA requests are being received. In addition, mistakes can occur in tracking and recording the status of requests, which can hamper their resolution. We reviewed FY 2014 FOIA requests and identified a number of recurring problems that would adversely affect the timeliness of responses. These problems included electronic FOIA requests that were misfiled, requests that had incorrect tracking numbers, and requests that had not been entered into the master FOIA log. If FOIA requests cannot be found or require additional time to find and address, I&A is in jeopardy of legal action.

Inadequate Records Management to Address FOIA Responses

I&A was recognized for outstanding continued improvement in records management, according to the 2014 DHS Records Management Maturity Model. However, at the time of our field work in September 2015, I&A had not implemented sound records management principles, such as an organization-wide program and procedures that would support operational staff members in locating pertinent information within the time allocated to address FOIA requests. Records are the foundation of open government and their ready access promotes the principles of transparency, participation, and collaboration. Well-managed and accessible records are important for operations to efficiently make decisions and carry out missions, such as addressing FOIA requests.

I&A had not placed priority on the implementation of an effective records management function. Instead, FOIA personnel, Division contacts, and operational staff had to search through different layouts, content, formats, and locations of I&A records to identify pertinent information. The lack of records management contributed to delays in locating pertinent records and meeting FOIA timeliness requirements.

For example, based on our review of the starting and closing dates in the I&A FOIA Office's tracking system, extensive time was expended waiting for information from operational staff. For five requests in FY 2014, the processing time ranged from 144 to 517 days. To resolve the 517-day-old request, I&A had to provide all processing notes, including search slips and the documentation pertinent to the original FY 2013 FOIA request—a difficult task given the lapsed time. Following are the primary deficiencies we identified in I&A's



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

records management program, which posed difficulties in responding to FOIA requests.

- Insufficient number of records management staff, and knowledgeable liaisons, and custodians: I&A has not appropriately staffed its records management function. I&A had one records officer and one contractor to meet records management requirements. Also, I&A has not identified records liaisons or custodians to assist in records management functions.
- Lack of I&A records management guidance: DHS Directive 141-01, *Records and Information Management*, requires the appointment of records liaisons or custodians, as well as the implementation of records management policies and procedures. Although I&A's Records Officer drafted policies and procedures, I&A management had not approved them at the time of our audit in September 2015.
- Lack of suitable training: OMB Memorandum M-12-18 required that, by December 31, 2014, agencies establish a method to inform all employees of their records management responsibilities and develop suitable records management training. I&A recognized the need for records management training in its FOIA report to the DHS Privacy Office in 2014; however, it did not provide training suitable to I&A's intelligence mission. Such training would enable FOIA staff to more accurately communicate to Division contacts the type and nature of information needed to respond to requests. The training would also instruct liaisons, records custodians, or operational personnel on how to search for or maintain pertinent information and FOIA-applicable records. When questioned regarding the lack of suitable training, I&A explained that all I&A staff were required to take mandatory records training through the DHS-online learning system. However, this training related to records management in general. Based on the FOIA delays, this training was insufficient to support I&A in making timely FOIA responses.
- Duplicative tracking systems: I&A maintained two systems for managing FOIA requests. Specifically, I&A used an executive secretariat system to issue task orders. This system was also used to task and track the status of FOIA requests and report that status to upper management. Concurrently, I&A's FOIA Office entered this information into its own commercially available web application solution to task and track search requirements within I&A. Rekeying some of the same information into two separate systems was time consuming, inefficient, and risked input mistakes and inconsistent information. For example, for FY 2014 there were requests that had not been entered into the FOIA Office system.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Employing new approaches and systems to locate pertinent records could expedite the retrieval of requested information. To further mature its records management system, I&A, along with counterparts, require programmatic guidance and additional resources from the Department. Also, I&A officials explained they intend to improve their records management capabilities as part of a DHS enterprise-wide effort to implement an Electronic Records Management System (ERMS), to meet requirements of OMB M-12-18. Although the memorandum required that by December 31, 2013, agencies develop and begin implementing plans to transition all permanent records to electronic format, DHS has not instituted a plan for all components. I&A has been waiting for further instructions from DHS headquarters on requirements for implementing a complete electronic records management program. Lacking instructions, the proliferation of records may require additional space and expose I&A's sensitive information to unnecessary risks of loss and misuse.

Recommendations

We recommend that the Principal Deputy Under Secretary for Intelligence and Analysis:

Recommendation 1: Prepare a plan of action and milestones for providing the FOIA Office appropriate staffing and capabilities to reduce its backlog of unresolved requests.

Recommendation 2: Provide specialized training for FOIA staff, Division contacts, and operational staff to improve I&A's responsiveness to FOIA requests.

Recommendation 3: Prepare a plan of action and milestones for instituting an organization-wide records management structure and processes to improve timeliness in identifying and locating pertinent records to address FOIA requests.

Management Comments and OIG Analysis

We obtained written comments on a draft of this report from the Under Secretary for Intelligence and Analysis. Management concurred with our recommendations. We have included a copy of the comments in their entirety in appendix B. The planned corrective actions and milestones satisfy the intent of these recommendations. We look forward to receiving updates on the implementation progress.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Continuity Capability For Safeguarding Essential Records and Intelligence Information

Through the *National Continuity Policy Implementation Plan*, dated August 2007, the President directed Federal executive branch agencies to achieve a national continuity capability. Federal Continuity Directive-1 (FCD-1), *Federal Executive Branch National Continuity Program and Requirements*, approved by the Secretary of Homeland Security and published in October 2012, provides direction for DHS' development of continuity plans and programs. FCD-1 directed that a viable continuity of operations program (COOP) should include 10 elements:

- Essential functions;
- Orders of succession;
- Delegations of authority;
- Continuity facilities;
- Continuity communications;
- Essential records management;
- Human resources;
- Tests, training, and exercises;
- Devolution of control and direction; and
- Reconstitution.

I&A had made progress in this regard through issuance of Policy Instruction IA-802, *Continuity Framework*, approved September 19, 2014, by I&A leadership. As implemented, the *Continuity Framework* laid the foundation for implementing continuity plans and continuity-related activities. I&A also addressed baseline requirements, such as defining which records were essential to its operations. Specifically, its June 2012 *Continuity Plan* established a classification of essential records relating to rights and interests. Records in this classification included official personnel records, contracting and acquisition files, payroll, and other records containing sensitive PII. Each I&A Division must identify specific essential records and Emergency Operating Records needed to continue essential functions. The *Continuity Plan* recognized essential records as a "critical element," defined as follows:

the identification, protection, and ready availability of electronic and hardcopy documents, references, records, information systems, and data management software and equipment (including classified and other sensitive data) needed to support essential functions during a continuity situation.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Further, at the time of our field work in September 2015, the *Continuity Framework* established a Continuity and Exercise Working Group (CEWG), a Continuity Coordinator, and a Reconstitution Manager as responsible for continuity planning. COOP plans support Federal agencies in responding to and recovering from business interruptions, emergencies, terrorism, or natural events rapidly and effectively.

However, the *Continuity Framework* neither adequately structured nor sufficiently provided authority for the CEWG to accomplish its assigned responsibilities. These responsibilities included ensuring:

- all I&A employees understand their continuity responsibilities;
- all I&A employees have the necessary equipment, records, and databases; and
- rosters of Division personnel assigned to the Emergency Relocation Group are current.

As of fall 2015, primary and alternate representatives from all I&A Divisions comprised the CEWG to implement the *Continuity Framework*. However, this group had limited success because its members were operations-level staff who lacked authority to task other employees or specialists needed to support continuity planning within I&A. The CEWG could have better fulfilled its responsibilities if a structure (i.e., a Charter) had required senior officials, such as Division Executive Officers, to comprise the CEWG. For example, Executive Officers have the authority to task out management assistance and support for records management, training, communications, acquisitions, human resources, and administrative assistance to address challenges in implementing continuity plans.

Further, at the time of our field work in September 2015, I&A did not address the FCD-1 requirement to designate an Essential Records Manager with responsibility for safeguarding its essential records and intelligence information. Without an Essential Records Manager, I&A had no means of meeting the requirement that its Divisions take a consistent approach to identifying, protecting, and ensuring the currency of essential and emergency records at I&A headquarters, relocation sites, or devolution sites in case of emergencies. An Essential Records Manager, working with the I&A Continuity Program Manager and CEWG, could help ensure proper implementation and administration of an essential records management program. An Essential Records Manager could oversee I&A's transfer and handling of essential records during tests, training, and exercises to resume operations after an interruption. In addition, an Essential Records Manager could perform the following essential records management requirements included in FCD-1:



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

- provide appropriate policies, authorities, and procedures;
- maintain a complete inventory of essential records, locations of, and instructions on accessing those records;
- review the essential records program annually and document the date and names of personnel conducting the review;⁶
- maintain a current essential records plan packet with a copy of the packet at the continuity facilities;⁷
- annually review, rotate, or cycle essential records so that the latest versions are available; and
- include instructions in the continuity plan on moving essential records (those that have not been prepositioned) from the primary operating facility to the alternate site.

Recommendations

We recommend that the Principal Deputy Under Secretary for Intelligence and Analysis:

Recommendation 4: Develop a Charter outlining the authorities of the Continuity and Exercise Working Group to carry out the full range of responsibilities for planning and instituting a continuity capability.

Recommendation 5: Provide a plan and timeline to fully implement an Essential Records Management Program that meets FCD-1 requirements for identifying, protecting, and ensuring the currency of essential and emergency records at I&A headquarters, relocation sites, and devolution sites in case of emergencies.

Management Comments and OIG Analysis

Management concurred with our recommendations. The planned corrective actions and milestones satisfy the intent of these recommendations. We look forward to receiving updates on the implementation progress.

⁶ Essential records program annual review is necessary to address new security issues, identify problem areas, update information, and incorporate any additional essential records generated by new organizational programs or functions or by organizational changes to existing programs or functions.

⁷ An essential records plan packet is an electronic or hard copy compilation of key information, instructions, and supporting documentation needed to access essential records in an emergency situation.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Securing Sensitive Information in Acquisitions

A collection of Federal guidance calls for improved security of sensitive information in acquisitions. Specifically,

- OMB Memorandum, *Follow-Up to President's Management Council Cybersecurity Meeting, September 5, 2014*, dated September 16, 2014, requires each agency's Chief Information Officer and Chief Acquisition Officer to initiate a process for identifying the functional areas of expertise needed to ensure compliance with Federal requirements and guidelines for continuously reviewing functional areas such as contracting, solicitations, and security.
- National Institute for Science & Technology (NIST) Special Publication (SP) 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, dated April 2015, calls for agencies to identify, assess, respond to, and mitigate supply chain risks at all levels of their organizations.
- *Class Deviation 15-01* from the *Homeland Security Acquisition Regulation (HSAR) Safeguarding of Sensitive Information*, dated March 2015, provides special contract clauses that require strengthening the security of contractor IT systems that have high risk of unauthorized access to, or disclosure of, sensitive information. The *Regulations* require DHS components to provide IT security and privacy training; amendments to existing contracts, as needed; and requirements traceability matrixes as a means of assessing high-risk solicitations and contracts involving sensitive information. High-risk contracts are those that include PII and any other data the agency deems sensitive based on risk or mission.⁸

In early 2015, OMB tasked the Federal Chief Information Officer Council and the Chief Acquisition Officer Council to review current acquisition and IT policies and practices involving contractors and subcontractors to ensure they adequately secure Federal information consistent with the *Federal Information Security Modernization Act of 2014*. OMB planned to issue a memorandum, *Improving Cybersecurity Protections in Federal Acquisitions*, to provide guidance on strengthening cybersecurity protections in Federal acquisitions for products or services that generate, collect, maintain, disseminate, store, or provide access to Controlled Unclassified Information on behalf of the Federal Government. This memorandum, still in draft as of November 2015, will require that an agency's Chief Information Officer, Chief Acquisition Officer, Chief Information Security Officer, Senior Agency Official for Privacy, and other

⁸ Such-high risk data include, but are not limited to sensitive PII, for official use only/sensitive but unclassified information, protected health information, law enforcement sensitive information, business confidential information, trade secrets, procurement sensitive information, and proprietary information.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

key stakeholders work together to review continuously high-risk solicitations and contracts. This collaborative review and oversight process should begin at contract solicitation and continue over the period that each contract is active to ensure the OMB requirements listed in figure 3 will be met.

Figure 3. Improving Cybersecurity Protections in Federal Acquisitions

Upcoming OMB Requirements for Improving Cybersecurity Protections in Federal Acquisitions (Draft)
<ol style="list-style-type: none">1) Contractor systems that contain Controlled Unclassified Information meet National Institute of Standards and Technology Special Publication 800-53 Rev. 4 privacy and security controls2) Contractors report security incidents3) Contractor systems that contain Controlled Unclassified Information undergo information system security assessments4) Contractor systems have information security continuous monitoring5) Agency officials perform business due diligence to identify and prioritize planned acquisitions and contracts

Source: OMB draft memorandum, *Improving Cybersecurity Protections in Federal Acquisitions (Draft)*

I&A made progress in addressing the collective Federal guidance calling for improved security of, access to, or disclosure of sensitive information by providing mandatory training and posting “HSAR Safeguarding IT Determination” and “Safeguarding of Sensitive Information Checklist.”

Although the OMB memorandum was not yet published by the end of our field work in November 2015, I&A had begun implementing the requirements under the HSAR for identifying high-risk contracts. In addition, I&A’s Chief Financial Officer continues to improve due diligence in processing and safeguarding PII in contracting.

Further in line with requirements of the HSAR, I&A had already established in October 2014 an oversight team representing mission-support, financial, privacy, IT, security, and acquisition functions from across I&A to develop a template for reviewing all contracts. I&A had initiated a process for its Contract Officer Representatives to review its 72 existing contracts to determine whether they required amendments. At the conclusion of this review in March 2015, I&A determined that two contracts related to physical security and front desk services were high-risk and required additional clauses. This was a one-time activity, although I&A continued to identify new high-risk contracts and also had pertinent contract language available for new and existing contracts. Since the conclusion of this collaborative exercise in March 2015, I&A has been waiting for further instructions from OMB and DHS headquarters on how to move forward to address upcoming requirements for improving cybersecurity protections in acquisitions.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Going forward, I&A could further enhance its cybersecurity protections by increasing business due diligence in acquisitions. For example, continuous risk assessment and end-to-end monitoring of high-risk acquisitions would provide better understanding and visibility into how contractors develop, integrate, and deploy products, services, and solutions to support government operations. Such enhancements would also help ensure security, integrity, resilience, and quality in contracted operations.

Recommendation

We recommend that the Principal Deputy Under Secretary for Intelligence and Analysis:

Recommendation 6: Prepare a plan and milestones to improve I&A's risk assessment and end-to-end monitoring of high-impact acquisitions involving intelligence information, privacy, and security.

Management Comments and OIG Analysis

Management concurred with our recommendation. The planned corrective actions, measures, and milestones satisfy the intent of this recommendation. We look forward to receiving updates on the implementation progress.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Appendix A

Objective, Scope, and Methodology

The Department of Homeland Security Office of Inspector General (OIG) was established by the *Homeland Security Act of 2002* (Public Law 107-296) by amendment to the *Inspector General Act of 1978*.

Our objective was to determine whether I&A ensures compliance with Federal privacy regulation and policies. We examined internal controls for managing all I&A information, but did not look at classified content as part of this audit. As background, we reviewed I&A's responsibilities for privacy protection, and I&A guidance related to operations, testimonies, compliance documentation, training, and intelligence oversight management. As part of our field work, we interviewed I&A's Information Compliance Branch Chief, and 22 managers and employees. We evaluated I&A's implementation of the *Freedom of Information Act* to promote agency transparency, continuity planning and capability for essential records management, and monitoring of solicitations and contracts. We confirmed that I&A offers mandatory training on privacy and civil liberties; conducts intelligence oversight activities; and is working to ensure compliance with the requirements of pertinent legislation, regulations, directives, and guidance.

We conducted this performance audit between July and October 2015 pursuant to the *Inspector General Act of 1978*, as amended, and according to generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based upon our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based upon our audit objectives.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix B
I&A Comments to the Draft Report

U.S. Department of Homeland Security
Washington, DC 20528

APR 24 2016



**Homeland
Security**

RECORD

MEMORANDUM FOR: John Roth
Inspector General

FROM: Francis X. Taylor *Francis X. Taylor*
Under Secretary for Intelligence and Analysis

SUBJECT: Response to Draft Report: *OIG-16-XXX Office of Intelligence and Analysis Can Improve Transparency and Privacy*
(OIG Project No. 14-067-ITA-I&A)

The Office of Intelligence and Analysis (I&A) appreciates the opportunity to review and comment on the Office of Inspector General (OIG) Draft Report: *OIG-16-XXX Office of Intelligence and Analysis Can Improve Transparency and Privacy*. I&A is actively resolving the issues identified in the draft report, and provides the following responses to the recommendations in the report.

Recommendation 1: Prepare a plan of action and milestones for providing the FOIA Office appropriate staffing and capabilities to reduce its backlog of unresolved requests.

I&A Response: Concur. I&A's plan of action was to create and hire two additional Government Information Specialists, one at the GS-0306/11-13 level and one at the GS-0306/14 level, to assist in the processing of I&A FOIA requests. This additional staff enables I&A to undertake a systematic approach in resolving the backlog of unresolved FOIA requests. Lastly, I&A expects to resolve the backlog by the middle of FY17. Estimated Completion Date: March 31, 2017.

Recommendation 2: Provide specialized training for FOIA staff, Division contacts, and operational staff to improve I&A's responsiveness to FOIA requests.

I&A Response: Concur. As previously discussed, I&A is hiring an additional Government Information Specialist, at the GS-0306/14 level. The responsibilities of this position will include developing and implementing a policy instruction that will address I&A's FOIA program, including a training program for FOIA staff, and identified I&A personnel who routinely originate and provide responsive documents for FOIA requests. Furthermore, the training program will be directed towards FOIA officers, the records liaisons and custodians creating government records. I&A anticipates the position, Senior Government Information Specialist, GS-0306/14, to be filled by early Summer 2016 and the implementation of a training program completed by the end of FY16. Estimated Completion Date: September 30, 2016.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Recommendation 3: Prepare a plan of action and milestones for instituting an organization-wide records management structure and processes to improve timeliness in identifying and locating pertinent records to address FOIA requests.

I&A Response: Concur. I&A's plan of action first milestone was obtaining the issuance of Policy Instruction, titled *Records and Information Management*, and accompanying Records Disposition form, in response to the OIG's preliminary findings (TAB 1-2). The policy instruction codifies how I&A will follow the Records Management Program as required by the DHS Records Management Directive 141-01. I&A's second milestone includes the creation of a requirement for an additional government employee to serve as I&A's Chief Records Officer, GS-0306/11-13. I&A expects this addition to be in place by end of August 2016. Lastly, I&A anticipates the identification and initial training of the designated individuals to be completed by June 2016. I&A expects to complete all milestones by August 31, 2016. Estimated Completion Date: August 31, 2016.

Recommendation 4: Develop a Charter outlining the authorities of the Continuity and Exercise Working Group to carry out the full range of responsibilities for planning and instituting a continuity capability.

I&A Response: Concur. I&A developed a draft Continuity Exercise Working Group (CEWG) Charter (TAB 3) that outlines the authorities and responsibilities of the CEWG to ensure I&A can meet its continuity capability requirements. The CEWG Charter is expected to be signed within 30 days. Estimated Completion Date: May 22, 2016.

Recommendation 5: Provide a plan and timeline to fully implement an Essential Records Management Program that meets FCD-1 requirements for identifying, protecting, and ensuring the currency of essential and emergency records at I&A headquarters, relocation sites, and devolution sites in case of emergencies.

I&A Response: Concur. I&A's plan includes the full implementation of an Essential Records Management Program. I&A has already designated an I&A Records Officer as the I&A Essential Records Manager. The plan also includes having this manager work closely with I&A's Continuity Program Manager and the I&A CEWG representatives to train Emergency Relocation Group (ERG) members on what essential records are, work with them to identify essential records, and then ensure they are stored and accessible at the Emergency Relocation Site. I&A also recently issued Policy Instruction IA-102, *Records and Information Management* (TAB 1), which includes provisions addressing these internal coordination efforts and Essential Records. These provisions will also be incorporated into I&A's records and information management training program. Furthermore, I&A has already conducted Essential Records training with Emergency Relocation Group members and they have started to identify their Essential Records. I&A's plan and efforts timeline concludes with testing and validation by mid-May 2016 during I&A's Eagle Horizon exercise. Estimated Completion Date: May 17, 2016.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Recommendation 6: Prepare a plan and milestones to improve I&A's risk assessment and end-to-end monitoring of high-impact acquisitions involving intelligence information, privacy, and security.

I&A Response: Concur. I&A agrees that securing sensitive information at all classification levels is vital; and, as the Inspector General's report states, I&A and our partners have already undertaken several steps to comply with the anticipated but not yet finalized Office of Management and Budget memorandum, *Improving Cybersecurity Protections in Federal Acquisitions*. In addition to the steps identified in the report, I&A and its partners have developed several measures to fully assess the risk of high-impact acquisitions and monitor with quarterly updates the activities undertaken under those contracts. A comprehensive description of these measures and their associated implementation results will be provided within thirty days of the release of the report.

Technical Comments to the Draft Report were previously provided under separate cover. Should you require additional information, please do not hesitate to contact me, or have your staff contact Dr. Tammy Tippie, at 202-447-4894.

Attachments:

- 1) IA-102 - Records and Information Management-signed
- 2) IA Form 102-A_Records Disposition
- 3) Draft CEWG Charter



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix C
Office of Information Technology Audits Major Contributors to
This Report

Marj Leaming, Director
Eun Suk Lee, Privacy Audit Manager
Kevin Mullinix, Privacy Analyst
Richard Elias, Information Technology Specialist
Shawn Ward, Referencer



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Appendix D Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chiefs of Staff
General Counsel
Executive Secretary
Director, Government Accountability Office/OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
DHS Chief Privacy Officer
DHS Audit Liaison Officer
Acting Deputy Under Secretary for Intelligence and Analysis
I&A Audit Liaison Officer
I&A Chief, Intelligence Oversight Officer/Information Compliance Branch

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees
Senator Al Franken, Ranking Member, Senate Committee on the Judiciary
Subcommittee on Privacy, Technology and the Law
Representative Bennie G. Thompson, Ranking Member, House Committee on
Homeland Security
Representative Jason Chaffetz, Chairman, House Committee on Oversight and
Government Reform; Chairman, House Committee on the Judiciary
Subcommittee on Crime, Terrorism, Homeland Security, and Investigations
Congressman Michael T. McCaul, Chairman, House Committee on Homeland
Security

ADDITIONAL INFORMATION AND COPIES

To view this and any of our other reports, please visit our website at: www.oig.dhs.gov.

For further information or questions, please contact Office of Inspector General Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov. Follow us on Twitter at: @dhsoig.



OIG HOTLINE

To report fraud, waste, or abuse, visit our website at www.oig.dhs.gov and click on the red "Hotline" tab. If you cannot access our website, call our hotline at (800) 323-8603, fax our hotline at (202) 254-4297, or write to us at:

Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Hotline
245 Murray Drive, SW
Washington, DC 20528-0305