NATIONAL ARCHIVES

OGIS
OFFICE of GOVERNMENT INFORMATION SERVICES

OFFICE OF GOVERNMENT INFORMATION SERVICES

COMPLIANCE REVIEW OF

THE DEPARTMENT OF HOMELAND SECURITY PRIVACY OFFICE

Privacy Office Meets Chief FOIA Officer Responsibilities by Aiding FOIA Implementation and Oversight and Supporting Customer Service

A Message from the Director

OGIS periodically conducts independent, systematic reviews of agencies to evaluate their compliance with the Freedom of Information Act (FOIA), 5 U.S.C. § 552(h)(2). These reviews assess the agency's FOIA operations, programs, and policies, and may include aspects such as program design, implementation, and results. An OGIS review may result in a report that we provide to the agency and release publicly, and may include recommended improvements and administrative actions. This assessment of the Department of Homeland Security (DHS) Privacy Office is in line with this purpose.

The DHS Privacy Office is led by DHS's Chief Privacy Officer, also designated to be the Department's Chief FOIA Officer, who has several responsibilities under FOIA to ensure agency implementation of the statute, oversight and customer service. This report addresses the Privacy Office's compliance with certain provisions of FOIA and is based on observations made during our compliance assessments of the FOIA programs at six DHS components; review of DHS Privacy Office policies, procedures and other materials; and interviews with agency employees and FOIA officials at the DHS Privacy Office and the six components we reviewed.

We hope this report will assist the DHS Privacy Office in its efforts to fulfill its FOIA responsibilities.

Nikki Gramian

NIKKI GRAMIAN
Deputy Director

Executive Summary

What OGIS Found

FOIA requires each agency to designate a senior official at the Assistant Secretary or equivalent level to act as the agency's Chief FOIA Officer. The statute gives the agency Chief FOIA Officer several specific responsibilities for ensuring implementation of the statute, oversight and customer service, 5 U.S.C. § 552(j). The DHS Privacy Officer serves as the DHS Chief FOIA Officer.

In August 2011, the DHS Secretary delegated the responsibility to fulfill duties related to FOIA to the Chief Privacy Officer. These responsibilities are carried out by a FOIA branch under the DHS Privacy Office.

The DHS Privacy Office meets its obligation to support implementation of the FOIA by providing targeted services to components, including the creation of a department-wide FOIA processing and tracking system; assisting with processing requests from component backlogs; and providing guidance on FOIA policy issues. During our assessments of DHS components, we observed that the Privacy Office's assistance processing requests was key to reducing Customs and Border Protection's backlog in Fiscal Year (FY) 2015. During our assessments, we also observed a large variation in the use of the department-wide FOIA system's capabilities by participating components and varying levels of success using technology to process requests by components that opted to not participate in the department-wide system. Our assessments also showed that some components were not aware of or not compliant with DHS FOIA policies.

The Privacy Office meets its responsibility to provide oversight through its reporting program in which it monitors the status of component FOIA programs monthly and raises issues with component Chief FOIA Officers as necessary. The Privacy Office also prepares statutorily required reports for the Attorney General.

The Privacy Office also supports customer service as required by providing requesters with information on its FOIA webpage about how to make a FOIA request that furthers public understanding of FOIA. The Privacy Office also has a FOIA Public Liaison who is responsible for assisting to resolve disputes with requesters. Additionally, the Privacy Office has launched information technology efforts that are intended to improve customer service across the department.

Introduction

The Freedom of Information Act (FOIA) directs the Office of Government Information Services (OGIS) to review agency FOIA policies, procedures and compliance, and identify procedures and methods for improving compliance, 5 U.S.C. § 552(h)(2). OGIS compliance assessments are independent and systematic evaluations of an agency's compliance with FOIA, and include the design, implementation, and results of an agency's FOIA operations, programs, and policies. The assessments 1) provide factual and analytical information; 2) review compliance with the law, regulation, and policy; and 3) share best practices. The assessments also include recommendations for improvement.

What We Reviewed

This report is based in part on observations made during our assessments of FOIA programs at six Department of Homeland Security (DHS) components: the Federal Emergency Management Agency (FEMA), United States Coast Guard (USCG), Transportation Security Administration (TSA), United States Customs and Border Protection (CBP), United States Secret Service (USSS), and United States Immigration and Customs Enforcement (ICE). Our agency assessments rely on direct observations of initial request and appeal case files; a review of DHS FOIA regulations, the agency's FOIA web page, and other written material such as memorandums of understanding, position descriptions, and FOIA Reports to the Attorney General; interviews with FOIA officials and staff; results of an online staff survey; and a review of agency FOIA litigation since 2009.

This report differs from our standard assessments in that we reviewed the DHS Privacy Office's compliance with the statutory duties of the Chief FOIA Officer, who heads the DHS Privacy Office. We did not review FOIA case files as we did at the six components nor did we survey DHS Privacy Office FOIA staff; we did review DHS Privacy Office written policies and guidance, strategic and backlog reduction plans, interagency agreements, organizational charts and internal management reports. We also interviewed seven key FOIA staff members.

Background

The DHS mission is to ensure a homeland that is safe, secure, and resilient against terrorism, disasters and other hazards.[1] DHS is organized into 16 directorates and components that have distinct missions and structures.[2] Most of the directorates and components are responsible for processing FOIA requests and appeals for their records. However, policy and program oversight is centralized. In August 2011, the DHS Secretary delegated the responsibility to fulfill duties related to FOIA to the Chief Privacy Officer.[3]

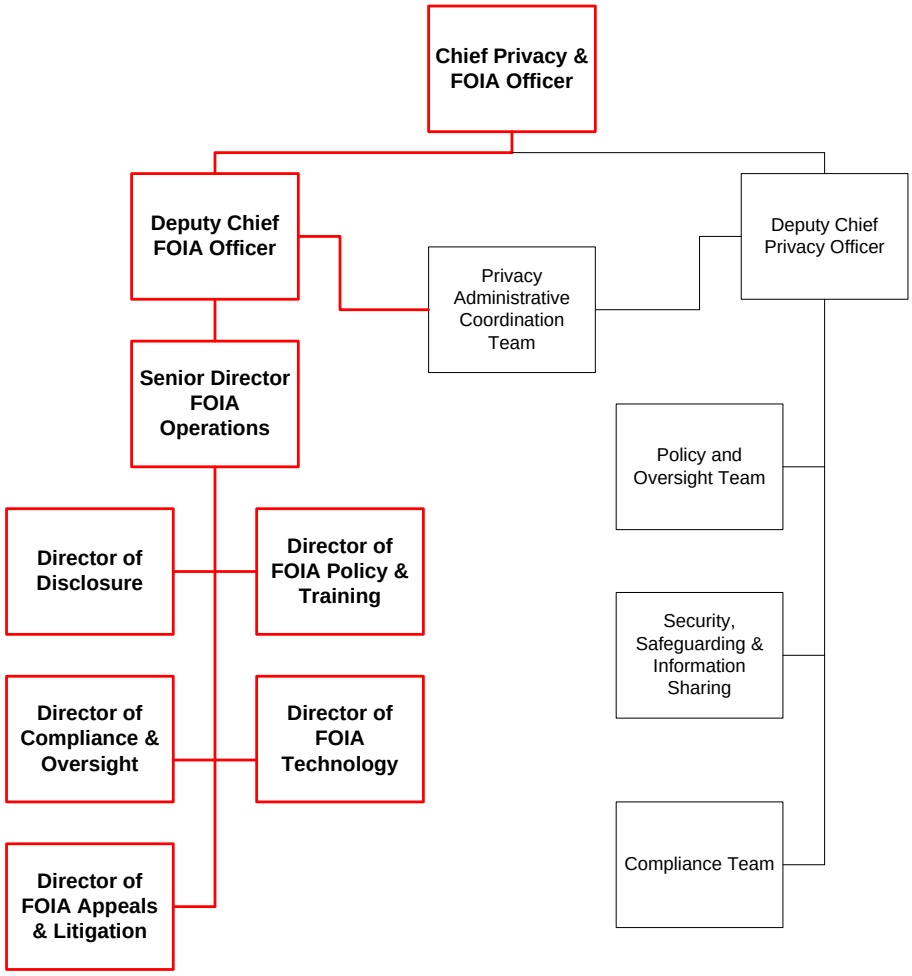
---

[1] "About DHS," last modified August 29, 2016, https://www.dhs.gov/mission#.
[2] "Department of Homeland Security Operational and Support Components," last modified June 28, 2016, https://www.dhs.gov/operational-and-support-components.
[3] "Department of Homeland Security Delegation No. 13001," accessed November 23, 2016, https://www.dhs.gov/sites/default/files/publications/cpo-delegation-letter-for-foia-2011_0.pdf.

FOIA requires each agency to designate a senior official at the Assistant Secretary or equivalent level to act as the agency's Chief FOIA Officer. The statute gives the agency Chief FOIA Officer several specific responsibilities for ensuring implementation of the statute, oversight and customer service, 5 U.S.C. §552(j). The DHS Privacy Officer serves as the DHS Chief FOIA Officer.[4]

A Deputy Chief Privacy Officer and a Deputy Chief FOIA Officer report to the Chief Privacy Officer and an administrative team supports both the Privacy and FOIA teams. The FOIA branch of the Privacy Office has a broad range of responsibilities. In addition to providing program and policy oversight, the Privacy FOIA Office processes requests for records from 14 DHS offices and components, and manages the administration of the Privacy Office appeals process on behalf of the Office of the General Counsel (OGC). The Privacy FOIA Office also provides DHS components with specific services intended to ensure the efficient implementation of the law.

Figure 1, DHS Privacy Office Organizational Chart



[4] The DHS Chief Privacy Officer is a political appointee, although at the time of this assessment, the Chief Privacy Officer was not (and is not) a political appointee but rather acting after the politically appointed Chief Privacy Officer departed.

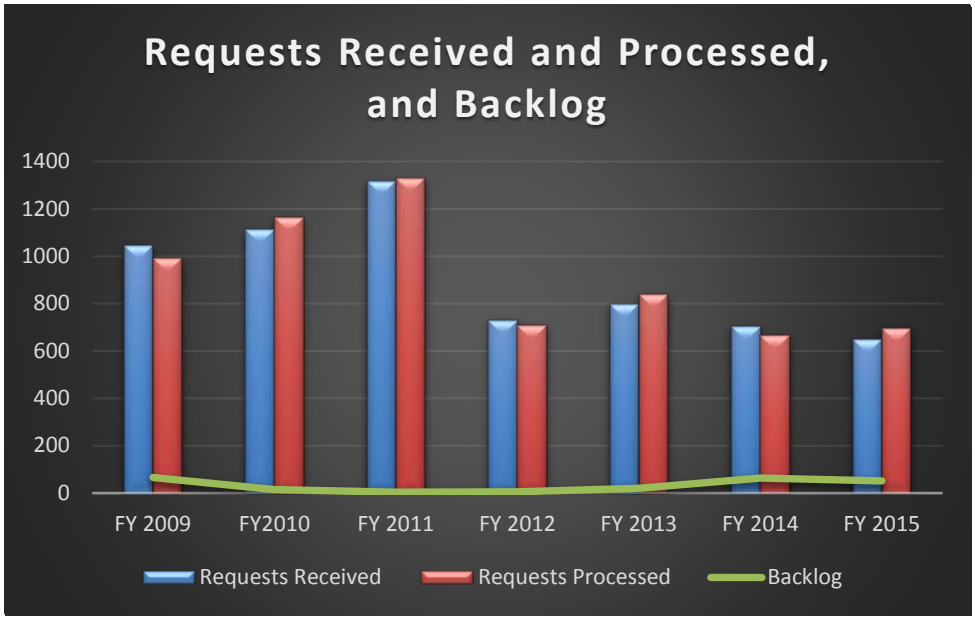
The structure of the FOIA branch of the Privacy Office largely reflects the office's various roles and responsibilities. It is led by the Deputy Chief FOIA Officer who oversees the:

- Senior Director of FOIA operations, responsible for helping to manage and oversee the office's operation;
- Director of Disclosure, responsible for ensuring that requests for records are appropriately processed, and as the Department's FOIA Public Liaison, responsible for assisting with resolving disputes;
- Director of FOIA Policy and Training, responsible for preparing the annual Chief FOIA Officer Report, preparing responses to Government Accountability Office (GAO) reports, providing ad hoc internal training and writing policy memos;
- Director of Compliance and Oversight, responsible for collecting, compiling and analyzing monthly FOIA reports from DHS components, preparing the DHS Annual FOIA Report, and tracking significant FOIA activity through weekly and daily reporting;
- Director of FOIA Appeals and Litigation, responsible for managing the administration of the Privacy Office appeals process and assisting OGC in litigation involving the Privacy Office; and
- Director of FOIA Technology, responsible for operations of the department-wide FOIA processing and tracking system and other FOIA-related information technology projects.

Privacy Office FOIA Process

The Privacy Office processes requests for records from the Privacy Office; Office of the Secretary; Chief of Staff; Military Advisor; United States Citizenship and Immigration Services (USCIS) Ombudsman; Public Affairs; Legislative Affairs; Domestic Nuclear Detection Office; Executive Secretariat; and Health Affairs. Prior to FY 2009, the Privacy Office also processed requests for records from the Office of Intergovernmental Affairs. Beginning in FY 2013, DHS Annual FOIA Reports show that the Privacy Office also processed requests for records from the Management Directorate; the Office of Policy; and OGC. The FY 2015 Annual FOIA Report reflects that the Privacy Office also processed records for the Office of Operations Coordination. More recently, the Privacy Office has processed records for the Office for Civil Rights and Civil Liberties (CRCL), according to staff.

Figure 2, Number of Requests Received and Processed, and Backlog, FY 2009 – FY 2015

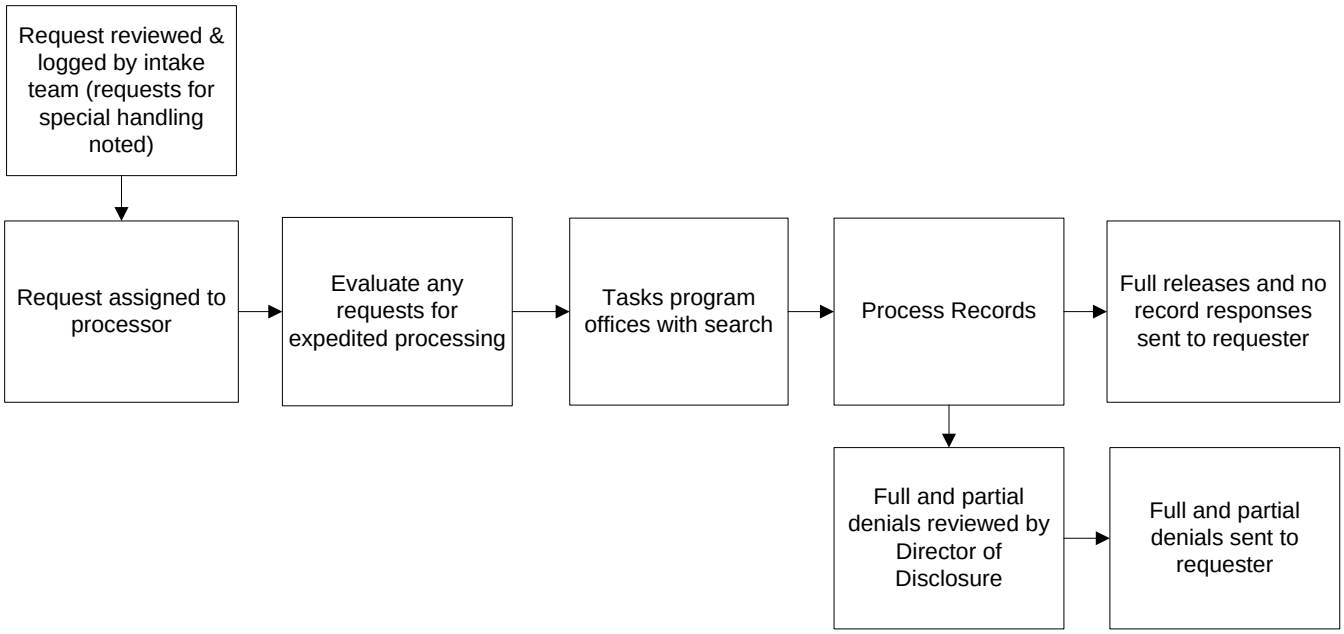


Between FY 2009 and FY 2015, the Privacy Office was responsible for an average of slightly less than one-half of one percent of the number of requests processed and received by all DHS components. Despite the increase in the number of offices and components for which the Privacy Office processes requests, the volume of requests received by the office dropped by about 45 percent between FY 2011 and FY 2012 from 1,317 requests to 730 requests. DHS Annual Reports show that between FY 2012 and FY 2015, the Privacy Office received an average of 721 requests per year and processed an average of 728 requests annually. These reports do not capture cases that the Privacy Office processes for other components; as discussed later in this report, the Privacy Office regularly enters into agreements to assist components with processing cases.

The Privacy Office's backlog accounts for a small portion of the overall DHS backlog: between FY 2009 and FY 2015, the Privacy Office accounted for less than one-half of one percent of DHS's backlog annually—ranging from 0.35 percent of the overall backlog in FY 2009 to 0.01 percent in FY 2011.

Each year between FY 2009 and FY 2015, the Privacy Office reported that its average processing time for complex requests was 78 working days, below the 127-working-day average processing time for complex requests across DHS.

Figure 3, Privacy Office FOIA Request Process



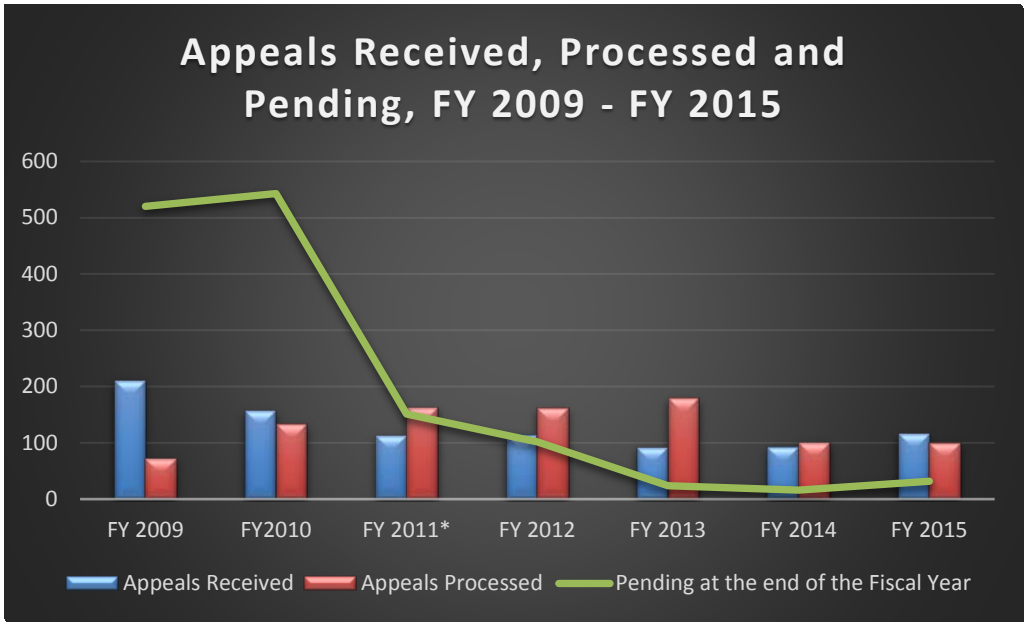
An intake team logs incoming requests to the Privacy Office, ensures requests are perfected and notes any special handling requests such as requests for expedited processing. The Director of Disclosure assigns requests for processing. The processors acknowledge requests; task program offices with searches; follow up on overdue searches; process records; and prepare responses to requesters. Full releases and no records responses are sent directly to the requester; in cases of full or partial withholding, the Director of Disclosure reviews redactions and responses.

Appeals

The Privacy Office assumed responsibility for managing the administration of the appeals that the office receives on behalf of OGC for headquarters offices and some smaller components in FY 2011; prior to the Privacy Office assuming this responsibility, TSA Office of the General Counsel was delegated the authority to manage and issue decisions for appeals that were logged with DHS OGC.[5]

[5]The Privacy Office administratively closed an unknown number of appeals in FY 2011 after auditing open appeal files, processing 164 appeals, and adjusting its numbers accordingly; it ended that fiscal year with 151 pending appeals.

Figure 4, Number of Appeals Received, Processed and Pending, FY 2009 – FY 2015



The number of appeals OGC received from FY 2011 to FY 2015 was fairly steady— ranging from 92 appeals in FY 2013 to 116 appeals in FY 2015 with an average of 106 appeals received each year. During the same period, OGC reported processing an average of 141 appeals each year. OGC reported having 32 appeals pending at the end of FY 2015, accounting for about 7 percent of the 431 appeals reported pending across DHS at that time.

The Privacy Office logs appeals into the FOIA processing and tracking system, ensures that there is a complete administrative file and sends it to a USCG Administrative Law Judge (ALJ). The ALJ program processes appeals for several smaller components including Headquarters Offices; the Office of Biometric Identity Management (OBIM); Privacy; Office of Intelligence and Analysis; CRCL: and the National Protection and Programs Directorate. ALJ charges about $70 per hour to review FOIA appeals; the average cost per case is $200, according to the Privacy Office Director of FOIA Appeals and Litigation. If the request needs further processing, the director completes the work.

Chief FOIA Officer Responsibilities

As described above, DHS has delegated statutory responsibilities to the Chief Privacy Officer for FOIA implementation, oversight and customer service. Although, the DHS Privacy Officer is designated to be Chief FOIA Officer, the name of the office does not reflect the offices' two missions under the Privacy Officer's purview. Renaming the office to reflect its dual mission would greatly improve internal and external understanding of the office's key role in providing access to records and protecting personal privacy.

The Chief Privacy Officer relies on the FOIA branch of the Privacy Office to carry out FOIA responsibilities. FOIA proscribes several actions that agency Chief FOIA Officers must take to support agency implementation of the law. The Chief FOIA Officer is required to

- support efficient and appropriate compliance with FOIA and make recommendations as necessary to improve implementation;
- provide oversight of FOIA operations by monitoring implementation and reporting to the Attorney General as required;
- support customer service by taking certain steps to improve public understanding of FOIA and by designating one or more FOIA Public Liaisons; and
- offer training to FOIA staff.

The findings of this report evaluate the Privacy Office's compliance with the responsibilities of the agency Chief FOIA Officer.

Finding 1: DHS Privacy Office Supports Efficient FOIA Implementation

The Chief FOIA Officer is responsible for supporting efficient and appropriate compliance with FOIA and making recommendations as may be necessary to improve implementation of the FOIA. DHS meets these responsibilities though its provision of policy guidance and targeted services and assistance for components. We observed a lack of consistency in components' awareness of and adherence to DHS FOIA policy and recommend that the Privacy Office adopt practices to address these deficiencies by adopting a standard procedure and method for issuing guidance.

Under the law the Chief FOIA Officer has specific responsibilities for ensuring that agencies implement FOIA, including responsibility for efficient and appropriate compliance and providing recommendations to the head of the agency for improving implementation.[6] The FOIA Improvement Act of 2016, which was enacted on June 30, 2016, also gives the Chief FOIA Officer responsibility for offering FOIA training to staff.[7]

[6] 5 U.S.C. §§ 552(i)(2)(A) and 552(i)(2)(C).
[7] 5 U.S.C. § 552(i)(2)(F).

The Privacy Office supports compliance by providing components with assistance processing cases. During our review, staff informed us that the Privacy Office was wrapping up an all-hands-on-deck project to close 14,435 cases from the backlog of OBIM; the Privacy Office spent a month and a half processing the backlogged requests. We observed a similar agreement during our FOIA compliance assessment of CBP: during FY 2015, CBP entered into an agreement with the Privacy Office to process cases pending from FY 2013. Under the agreement, CBP paid the Privacy Office $284,998.50 to process between 8,000 and 9,000 cases; two contractors and six members of the Privacy Office staff completed the work. Our CBP assessment report notes that this agreement was a key to CBP's success in reducing its backlog and improving timeliness of its responses to requesters.

The Privacy Office has also made a substantial investment in technology to improve FOIA processes and coordination across DHS. In 2012, the Privacy Office obtained unused licenses from USCG for a proprietary FOIA tracking and processing system. The Privacy Office used the licenses to launch a department-wide FOIA system. When the system launched, it had 40 users from four DHS components; at the time of our review the department-wide system had 266 users from all but four components (CBP, USCIS, USSS, and Federal Law Enforcement Training Centers).

To encourage components to adopt the system, the Privacy Office covered all costs for components using the system through FY 2016. Prior to FY 2017, the components participating in the system agreed to a cost-sharing model based on the number of system users. The shared costs include the contract, security, server space, and the salary of the Director of FOIA Technology, who acts as the system administrator and provides components with technical assistance. The annual per-user cost for components for FY 2017 is about $2,400, based on 216 system users at the time the agreement was made. As users are added to the system, the Director of FOIA Technology expects the per-user cost to decrease.

The department-wide system has several benefits for the components on the system and DHS headquarters, according to the Director of FOIA Technology, including that DHS can leverage its buying power to keep costs down and to make upgrades requested by DHS components a priority for the vendor. In addition to making it easy for the component to extract information for annual FOIA reports, the department-wide system also has reporting tools that management can use to track employee performance and identify emerging bottlenecks. The department-wide system also helps ensure that the component has a complete administrative record should the case be appealed or go into litigation; if the component has processed all of the responsive records using the department-wide system, the FOIA staff can also automatically generate the basis of a Vaughn index, which is usually a time-consuming and labor-intensive process.[8]

We reviewed four DHS components that use the department-wide FOIA system ICE, TSA, FEMA and USCG. The Privacy Office provides a day-long basic training to new users on how to use the

[8] A Vaughn index is a document that agencies prepare in FOIA litigation and must: (1) identify each document withheld; (2) state the statutory exemption claimed; and (3) explain how disclosure would damage the interests protected by the claimed exemption.

department-wide system; components can also ask the Privacy Office to provide training on how to use the system as needed. The Director of Information Technology also acts as a help desk for components, regularly helping troubleshoot and resolve issues; if the Director of Information Technology cannot address the issue, he escalates it to the vendor. The Director of Information Technology has also written a handbook that addresses common issues components have with the system. Our assessment reports show a wide variety in components' use of the department-wide system and their technical expertise in the system's capabilities.

- USCG used the department-wide system only as a tracking tool, with contractors in the headquarters office logging into the system all requests submitted to nine districts and more than 1,200 units. USCG informed us that it originally intended to have all of the districts and units use the software to track and process requests; however, because USCG's workforce is so dispersed and personnel change frequently due to redeployments, the agency said it is not able to effectively train FOIA processors on how to use the software and decided against implementing it agency-wide. Because USCG did not use the system to process requests, we observed that the appeals officer frequently had to reach out to processors to complete the administrative record before the appeal could be reviewed.
- Our assessment report shows that FEMA struggled with using the department-wide system to process records in their native format and that weak record-keeping practices often meant that key documents were missing from administrative files. We also reported that FEMA had recently invested in a supplemental license for the department-wide system that would improve its ability to process requests for email records by automating de-duplication and shortening the time for FEMA to respond.
- Our assessment report on TSA's FOIA compliance documents that the component uses the department-wide system to track requests, review records and apply redactions. We noted that for some of the case files we reviewed, information about the use of exemptions that was logged into the system did not match with what was applied to the records. We also noted that TSA was not able to use the supplemental license for the department-wide system that would automate the de-duplication of records.
- Our report on FOIA compliance by ICE shows that the components used the department-wide system to make its process efficient. We noted that ICE used the system's reporting capabilities to monitor and reward employee productivity. We also noted that new ICE FOIA employees are trained by the Director and Deputy Director and on how to use the system.

Another component we reviewed, CBP, on its own used the proprietary FOIA processing and tracking system but did not participate in the department-wide system used by other DHS components. Prior to our assessment, CBP had moved to another processing and tracking tool, which, according to CBP, was better able to handle the large volume of requests it receives annually and helped substantially reduce the backlog in FY 2015. The other component we reviewed, USSS, uses the same proprietary FOIA processing and tracking system as DHS components on the department-wide system; however, USSS pays for its own contract and is on an older version of the system. Our assessment of USSS's FOIA

program noted severe limitations in USSS's ability to use its FOIA processing and tracking system due to issues with the USSS information technology infrastructure and security requirements.

Interviews with USSS FOIA officials and the Privacy Office Director of FOIA Technology indicate that USSS opted not to participate in the department-wide system because of concerns over the security of the component's Law Enforcement Sensitive information compiled for law enforcement purposes and concerning White House security and other related matters. The Director of FOIA Technology explained that users can only access records that have been uploaded by someone from the same component. He also explained that he is the only DHS employee outside of a particular component who might be able to access records, and that he could only access the records with the express permission of the user as a part of troubleshooting an issue with the department-wide systems operations.

The Privacy Office fulfills its other responsibility for recommending adjustments to agency practices, policies, personnel and funding as may be necessary to improve implementation by issuing DHS-wide FOIA policies. These policies are transmitted in both formal memorandums and informal emails. The Privacy Office generally issues policies and guidance to component FOIA Officers via an email list maintained by the Director of Disclosure. Component FOIA Officers are responsible for letting their FOIA staff know about the policy and for contacting the Privacy Office if the list needs updating. The Privacy Office has posted some of its policy and guidance memos online, but there is no public or internal repository of all DHS FOIA policy and guidance.

The Office of Information Policy (OIP) at the Department of Justice, which is responsible for issuing FOIA guidance government-wide, has a standard distribution procedure and template for its guidance. OIP includes, where applicable, a checklist of actions an agency must take to comply with the guidance. All OIP guidance is available on a public website. Adopting OIP's practices could greatly improve components' access to and awareness of DHS FOIA policy.

During our assessments of DHS components, we observed inconsistency in awareness of and adherence to DHS FOIA policies. For example, while we found that most components comply with DHS's "significant requests" policy, the USSS FOIA office does not appear to follow the part of the DHS Privacy Office's policy on "significant requests" that requires components to alert the Privacy Office 24 hours before it responds to significant requests.[9]

We also observed some inconsistencies with components' use of "still interested" letters to administratively close FOIA requests when requesters do not re-affirm their interest in the request within a specific time-frame. Guidance from DOJ requires that agencies provide requesters with at least 30 working days to respond and that agencies should limit the use of these letters.[10] The Privacy Office circulated this guidance to components and directed that components follow the policy, and report on the

[9] "Guidelines for Reporting on Significant FOIA Activity for Inclusion in the Cabinet Report to the White House, July 7, 2009,"accessed November 28, 2016, http://www.dhs.gov/sites/default/files/publications/priv_cfoiao_memo_cabinet_report_foia_guidelines_20090707.pdf.
[10] "OIP Releases New Guidance for Agency Still-interested Inquiries," last modified July 5, 2015, http://www.justice.gov/oip/blog/oip-releases-new-guidance-agency-still-interested-inquiries.

use of still interested letters. In our report on the FEMA FOIA program, we noted that FEMA had recently changed its practices to provide requesters with an appropriate amount of time to respond to a still interested inquiry; however, we later informed the DHS Chief FOIA Officer that FEMA was once again providing requesters with significantly less time to respond than required by the policy.[11] Our assessment reports on the FOIA programs at ICE, TSA, and USSS also included recommendations that the office use still interested letters in accordance with DOJ and DHS policy.

Finally, the Privacy Office also provides training materials to agency staff regarding their responsibilities under the FOIA, meeting its responsibility to "offer training to agency staff" as added by the FOIA Improvement Act of 2016. As previously described, the Privacy Office provides training to components on use of the department-wide FOIA tracking and processing system, and ad-hoc training on DHS FOIA policies. DHS's online learning system recently incorporated FOIA training modules released by DOJ in March 2015; this training is now required for all Privacy Office FOIA staff and optional for other DHS employees, and the Privacy Office notified component FOIA Officers of the availability of the training.

Recommendation: Adopting a standard procedure and method for issuing guidance, as OIP does in issuing government-wide FOIA policy, would improve DHS components' compliance with FOIA and adherence to DHS FOIA policy. We recommend that the DHS Chief FOIA Officer adopt these practices. When warranted, issues of non-compliance should be raised to higher levels, including to the Secretary's office. The Privacy Office should also issue additional recommendations or corrective actions as necessary to bring components into compliance with the law and DHS policy.

Finding 2: DHS Privacy Office Provides Oversight

The Chief FOIA Officer is responsible for monitoring the agency's FOIA performance and reporting on the agency's performance as required to the Attorney General. The Privacy Office maintains a robust reporting program that meets these requirements.

FOIA provides agency Chief FOIA Officers with responsibilities related to oversight of the agency's FOIA activities. In particular, Chief FOIA Officers are required to monitor implementation of the law, and review and report on the agency's FOIA performance to the Attorney General.[12] The FOIA Improvement Act of 2016 also requires that the Chief FOIA Officer act as the primary agency liaison for the Office of Information Policy (OIP) at DOJ and OGIS.[13]

The Privacy Office's reporting program monitors implementation and performance. Components report monthly on key performance statistics, including the number of requests and appeals received and

[11] Letter to DHS Chief Privacy Officer, September 15, 2015, accessed November 29, 2016, https://ogis.archives.gov/Assets/Letter+to+Karen+Neuman+re+FEMA+Stll+Interested-web.pdf?method=1.
[12] 5 U.S.C. §§ 552(i)(2)(B) and 552(i)(2)(D).
[13] 5 U.S.C. § 552(i)(2)(G).

processed, the 10 oldest pending requests and appeals, and the age of requests in the component's backlog. The monthly reports also include information about records posted to agency FOIA reading rooms and other significant proactive disclosures.

Components are expected to submit the monthly reports at the beginning of each month and regularly do so in a timely manner, according to the Privacy Office. Components submit the data to the Privacy Office in a PDF format; the Privacy Office manually enters the data from the reports into a spreadsheet so that they can analyze the data to identify potential issues, including increases in DHS's backlog. The Privacy Office also uses the monthly reports to create a progress report or scorecard that is sent to the component FOIA Officers.

The Privacy Office also has structures and systems in place to meet DHS's reporting requirements to the Attorney General. The Privacy Office provides components with guidance and assistance in collecting and reporting data for agency annual FOIA reports. The Privacy Office also provides DOJ with required quarterly performance data and collects data for and prepares Chief FOIA Officer reports on behalf of DHS.

Finding 3: DHS Privacy Office Supports Good Customer Service

The Chief FOIA Officer is responsible for improving public understanding of the interests protected under FOIA and designating FOIA Public Liaisons. The Privacy Office meets these responsibilities and leverages technology to provide components with tools that improve customer service.

FOIA requires that the Chief FOIA Officer take several steps to improve public understanding of FOIA, including by providing concise descriptions of the exemptions in the agency's handbook for requesters and annual reports, and providing an overview of certain general categories of agency records that are subject to exemptions. The FOIA Improvement Act of 2016 requires that the agency post its handbook for requesters online.[14]

Although we did not locate a copy of a handbook on the Privacy Office's FOIA page during our review of the Privacy Office's website, we note that the site includes concise descriptions of the exemptions and other material designed to help improve public understanding of the FOIA process. In addition to providing information on how to submit a FOIA request and links to resources, the Privacy Office's FOIA website also hosts the office's FOIA reading room containing frequently requested records from DHS components. Additionally, the website includes contact information for components' FOIA programs and information about the mediation services offered by OGIS.

The Privacy Office has also launched efforts to improve customer service department-wide using technology. The Privacy Office's website allows requesters to track the status of requests at any component participating in the department-wide FOIA processing and tracking system. The Director of FOIA Technology explained that components who do not use the department-wide system can

[14] 5 U.S.C. § 552(g)(3).

participate in the online check status feature by providing the Privacy Office with certain data about their requests. The website also features a mobile application that requesters can use to submit requests to any DHS component and check the status of their requests.

FOIA also requires Chief FOIA Officers to improve customer service by designating one or more FOIA Public Liaisons. The Privacy Office's Director of Disclosure acts as the office's FOIA Public Liaison. If a requester calls to discuss a case that is being processed by the Privacy Office, the Director of Disclosure alerts the processor working on the case that he or she needs to respond to the request. There is not a system to track requests or follow up on the resolution of complaints.

Components generally designate FOIA Public Liaisons to facilitate the resolution of disputes with requesters. The Privacy Office's website includes information about who holds this position at some components. In addition to responding for requests for assistance with requests processed by the Privacy Office, the Director of Disclosure fields a small number of requests for assistance with a component's FOIA process. These requests are directed to the appropriate component for response.

Scope and methodology[15]

OGIS Review Team Lead Kirsten Mitchell and Team member Amy Bennett assessed the compliance of the Privacy Office with requirements for agency Chief FOIA Officers. This report is the result of assessments of compliance at six DHS components; analysis of applicable data and documents including DHS FOIA regulations, the agency's FOIA website and other written material; and interviews with Privacy Office officials and staff. On October 12, 2016, we interviewed the Deputy Chief FOIA Officer, the Acting Senior Director FOIA Operations, the Director of Disclosure, the Director of FOIA Policy and Training, the Director of Compliance and Oversight (Acting), the Director of FOIA Technology, and the Director of FOIA Appeals and Litigation. Our findings rely on OGIS's Elements of an Effective FOIA Program, based on

- the FOIA statute;
- Office of Management and Budget Guidelines for Fees;
- Presidential Memorandums;
- Attorney General Memorandums;
- Guidance from the Department of Justice's Office of Information Policy, including DOJ's Guide to the Freedom of Information Act; and
- Inconsistencies and non-compliance observed during OGIS's mediation services.

[15] Please direct questions to OGIS at ogis@nara.gov or 202-741-5770.