

TESTIMONY OF ALINA M. SEMO

DIRECTOR, OFFICE OF GOVERNMENT INFORMATION SERVICES

**SUBCOMMITTEE ON OVERSIGHT, MANAGEMENT AND
ACCOUNTABILITY**

HOUSE COMMITTEE ON HOMELAND SECURITY

October 17, 2019

**“The Public’s Right to Know:
FOIA at the Department of Homeland Security”**

Good afternoon Chairwoman Torres Small, Ranking Member Crenshaw and members of the Subcommittee. I am Alina Semo, and I was appointed as the Director of the Office of Government Information (OGIS) by the Archivist of the United States, David Ferriero, as of November 2016.

Thank you for the opportunity to appear before you to discuss OGIS’s review of the administration of the Freedom of Information Act (FOIA) by the Department of Homeland Security (DHS).

As the Federal FOIA Ombudsman, OGIS offers a range of services to help anyone through the FOIA process. My staff of nine helps to resolve Federal FOIA disputes; educates stakeholders about the FOIA process; reviews agency FOIA policies, procedures and compliance; and identifies procedures and methods for improving compliance. All of our work is conducted through the lens of advocating for neither the requester nor the agency, but rather for the FOIA process itself.

Earlier this month, we celebrated our 10th anniversary. While we have offered dispute resolution services since 2009, our compliance program is still young—we conducted our first agency assessment in November 2014 by reviewing one of the FOIA programs at our own agency, the National Archives and Records Administration (NARA). Earlier that year, before we even had our compliance program up and running, DHS approached OGIS to request that we review several DHS FOIA programs. We were able to turn our attention to particular DHS FOIA programs in 2015.

Today I will briefly discuss our compliance work generally, and focus more specifically on our assessments of seven FOIA programs at DHS that we conducted between September 2015 and February 2018. Additionally, I will discuss our December 2016 assessment of DHS’s compliance with the responsibilities for Chief FOIA Officers as mandated in the FOIA statute.

Our agency assessment program is just one piece of a robust FOIA compliance program that also includes assessing FOIA process issues; reviewing agency FOIA regulations; identifying and addressing government-wide compliance issues using responses to self-assessment questions; and managing the FOIA Advisory Committee, which I chair, and which brings together FOIA experts from inside and outside of government appointed by the Archivist of the United States to identify solutions to FOIA’s biggest challenges.

It is important to note that while we review compliance, we are not the “FOIA police,” and as I mentioned earlier, we advocate for the FOIA process to work as Congress intended. It is also important to note that the assessments we conduct are snapshots in time and our findings and recommendations may no longer apply—or have been addressed subsequently by each DHS component. We follow up with agencies 120 days after our assessments are published, and our follow-up track record shows that overall agencies have addressed approximately 98 percent of our recommendations.

Our assessments of agency FOIA programs are based on generally accepted government auditing standards (GAGAS) and offer agencies a holistic review of their FOIA programs. We rely on our staff’s knowledge of the FOIA process and on best practices to identify issues in the administration of FOIA and make tailored recommendations. Our compliance assessment process recognizes that there is no “one-size-fits-all” approach to administering FOIA—each agency’s records are unique and FOIA processes are as diverse as agency missions. Nevertheless, we have observed that successful FOIA programs share three general characteristics: they manage their resources appropriately; they use technology effectively; and they communicate well with requesters.

The seven DHS FOIA programs my team reviewed, in the order of our assessment reports, were at (1) [Federal Emergency Management Agency](#) (FEMA)—September 18, 2015; (2) [United States Coast Guard](#) (Coast Guard)—September 25, 2015; (3) [Transportation Security Administration](#) (TSA)—January 11, 2016; (4) [Customs and Border Protection](#) (CBP)—March 9, 2016; (5) [United States Secret Service](#) (USSS)—July 27, 2016; (6) [Immigration and Customs Enforcement](#)

(ICE)—October 18, 2016; and (7) [U.S. Citizenship and Immigration Services \(USCIS\)](#)—February 9, 2018.

In assessing these seven FOIA programs, we surveyed nearly 500 FOIA professionals and reviewed a sampling of more than 1,500 FOIA requests that had been processed in the most recent fiscal year prior to each of our assessments. For example, we assessed the FOIA program at TSA which processed fewer than 1,000 requests in Fiscal Year 2014 and the government’s largest FOIA program at USCIS which processed 145,470 FOIA requests in Fiscal Year 2016.

I will discuss the three buckets of recommendations that I mentioned earlier—*management*, *technology* and *communication*—by providing examples from our seven assessments of DHS components.

Management

In reviewing an agency’s management of its FOIA program, we evaluate how a FOIA program is managing the resources it is given by the agency. Our assessments show the importance of strong management practices to the success of the program. For example, our assessment of CBP showed that support from leadership and a plan for addressing both the backlog and incoming requests enabled the FOIA program to drive down its backlog by 74 percent in FY 2015—from 34,307 requests to 9,024 requests.

At TSA, we recommended that it create standard operating procedures for the entire FOIA process and that FOIA managers monitor the number of cases closed and volume of pages reviewed by each processor, and set data-driven goals to reduce the backlog and increase timeliness. In response, the agency reported that establishing performance metrics for FOIA analysts and case closure goals for the office helped reduce its backlog in four months.

For USSS, we recommended that it create a formal data-driven backlog reduction plan and expand on the work the agency’s FOIA program was already engaged in to keep requests out of the backlog by using multi-track processing and focusing on responding to older requests.

Technology

We also review how well an agency is using the technology resources it has. At several DHS components, we observed that technology was not being used to its fullest potential to administer FOIA. For example, FEMA had technological tools

but the agency was not fully using the technology to improve FOIA tracking, processing, and proactive disclosure.

In 2016, we observed at TSA a duplication of effort because of a separate review of records containing Sensitive Security Information (SSI). The FOIA tracking and processing system did not communicate with the SSI tracking and processing system. We recommended that the FOIA office work with the SSI office to resolve the duplication and inefficiencies.

In 2016, we also recommended several actions aimed at getting different DHS components to collaborate more efficiently. For example, we recommended that ICE and USCIS explore electronic transmittal of misdirected FOIA requests which arrive at one agency but seek records at the other agency. We recommended that USSS discuss with USCIS a more efficient way to send requests it refers to USSS, possibly electronically.

Finally, in 2018, we recommended that USCIS weigh the costs and benefits of producing digitized version of Alien Files (A-Files) the official Government record that contains information regarding transactions involving individuals as they pass through the U.S. immigration and inspection process. A machine-readable version could enable use of computer-assisted review tools which, in turn, could speed the process. We also recommended that USCIS explore technologies to mark records as processed and enable the FOIA processor to easily access the previously processed version of the record, which could cut down on inefficiencies in a system in which an A-File is often requested several times by a requester and/or their lawyer—but reprocessed each time for each new FOIA request.

Communication

In reviewing FOIA case files, we look at most—but not all—of an agency's administrative record. We do not review the underlying records that have been requested and the exemptions applied to those records.

With regard to communication, we often find that more frequent and better communication with requesters in plain language goes far in helping requesters understand the FOIA process. As a result, our recommendations in this area have included providing requesters with additional information about certain records withholdings; updating and correcting FOIA websites and template letters; providing requesters with an estimated date of completion when they ask for one; and removing jargon and legalese in response letters.

Finally, in December 2016 we assessed whether the DHS Privacy Officer, who serves as the DHS Chief FOIA Officer, fulfills several specific statutory responsibilities.¹

FOIA defines 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.

While most of the 16 DHS directorates and components² are responsible for processing FOIA requests and appeals for their own records, policy and program oversight is centralized at DHS. In August 2011, the DHS Secretary delegated to the Chief Privacy Officer the responsibility to fulfill duties related to FOIA and Privacy Act programs across the entire Department,³ and in July 2019, the DHS Secretary designated the Chief Privacy Officer as the Chief FOIA Officer.⁴

In reviewing DHS Privacy Office's compliance with Chief FOIA Officer duties, we did not review FOIA case files as we did at the DHS component assessments 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.

¹ 5 U.S.C. § 552(j).

² At the time of our assessment, there were 16 DHS directorates and components. There are now 14 directorates and components, accessed October 4, 2019, <https://www.dhs.gov/operational-and-support-components>.

³ "Department of Homeland Security Delegation No. 13001," accessed October 2, 2019, https://www.dhs.gov/sites/default/files/publications/cpo-delegation-letter-for-foia-2011_0.pdf.

⁴ Department of Homeland Security Designation No. 00-13002," accessed October 9, 2019, <https://www.dhs.gov/publication/designation-chief-foia-officer>.

We found that the DHS Privacy Office met 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.

The DHS Privacy Office met its responsibility to provide oversight through its reporting program in which it monitored the status of component FOIA programs monthly and raised issues with component Chief FOIA Officers as necessary. The Privacy Office also prepared annual reports required by the statute.

In addition, the Privacy Office supported customer service by providing requesters with information on its FOIA webpage about how to make a FOIA request that furthers public understanding of FOIA. At the time of our assessment, the Privacy Office had a FOIA Public Liaison whose responsibility was to assist requesters and to resolve disputes. Additionally, the Privacy Office had launched information technology efforts that were intended to improve customer service across the Department.

During our assessments of individual DHS component agencies, we noted several instances in which the DHS Privacy Office provided valuable assistance to DHS component agencies. For example, the Privacy Office's assistance with processing requests was key to reducing CBP's backlog in FY 2015. During our assessments, however, we also observed a large variation in the use of the DHS-wide FOIA system's capabilities by participating component agencies and varying levels of success using technology to process requests by components that opted to not participate in the department-wide system.

As noted earlier, these assessments represent snapshots in time and our findings and recommendations may no longer apply.

Moreover, 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 component agencies comply with DHS's "significant requests" policy, the USSS FOIA office did not appear to follow 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.⁵

⁵ "Guidelines for Reporting on Significant FOIA Activity for Inclusion in the Cabinet Report to the White House, July 7, 2009," accessed October 2, 2019,

We recommended to the DHS Privacy Office that adopting a standard procedure and method for issuing guidance, similar to the way in which the U.S. Department of Justice's Office of Information Policy does in issuing government-wide FOIA policy, would improve DHS component agencies' compliance with FOIA and adherence to DHS FOIA policy. We recommended that the DHS Chief FOIA Officer adopt these practices, and, when warranted, issues of non-compliance should be raised to higher levels, including to the Secretary's office. Finally, we recommended that the DHS Privacy Office should also issue additional recommendations or corrective actions as necessary to bring component agencies into compliance with the law and DHS policy.

In response to our assessment of the DHS Privacy Office, the Department took several steps to ensure that its FOIA program operate more efficiently, including issuing a management directive directing components to comply with FOIA law and DHS policy.⁶ The DHS Privacy Office also committed to raising issues of non-compliance with component offices and when necessary, the Secretary's office, and issuing recommendations to components as necessary to ensure compliance with the law.

I hope the foregoing information regarding how OGIS conducts its agency assessments, and in particular our assessments of several DHS FOIA programs, has shed some light on how DHS works to administer FOIA. I appreciate the opportunity to appear before this Subcommittee. I look forward to answering any questions you may have.

http://www.dhs.gov/sites/default/files/publications/priv_cfoiao_memo_cabinet_report_foia_guidelines_20090707.pdf.

⁶ "Freedom of Information Act Compliance," Department of Homeland Security Directive Number 262-11, accessed October 15, 2019, <https://www.dhs.gov/sites/default/files/publications/Directive%20262-11%20Freedom%20of%20Information%20Act%20Compliance%20April%202017.pdf>.