



DEPARTMENT OF DEFENSE

AGENCY CHIEF FREEDOM OF INFORMATION

ACT OFFICER REPORT

FOR 2014

Preparation of this study/report cost the
Department of Defense approximately \$40,000 for the 2014 Fiscal Year.

DIRECTOR OF ADMINISTRATION
AND MANAGEMENT

**2014 Department of Defense (DoD)
Chief Freedom of Information Act (FOIA) Officer's
Report to the Department of Justice**

Executive Summary

DoD Leadership continues to be dedicated to the success of the Department's FOIA programs throughout its 32 components located around the world. The Chief of the Freedom of Information Division (FOID), who is responsible for policy and execution of the DoD FOIA program, meets regularly with the DoD Chief FOIA Officer, the Director of Administration and Management (DA&M), to ensure continued awareness and to engage in discussions about continued emphasis on training, backlog reduction, closure of the Agency's ten oldest requests, consultations and appeals, and to ensure that the DoD FOIA community has the resources needed to keep the FOIA programs running efficiently to meet the President's Open Government goals. Despite budget constraints, the commitment of leadership was evident, with 72% of DoD Components reporting their FOIA professionals attended training and more than half of the components indicating that they conducted training for their own personnel. Components continued efforts to foster a more transparent environment by posting information to their websites and engaging in practices that reduced the need for requesters to seek information utilizing the FOIA.

Over 50% of DoD Components reduced their backlog of initial FOIA requests and DoD closed all of its ten oldest consultations and appeals and seven out of ten of its oldest initial requests. Ninety-five percent of requests that fell within the category of "Simple" were processed within 20 working days; 82% of requests that fell within the "Complex" category were processed within 100 working days; and 90% of all DoD FOIA requests were closed within 100 working days of receipt.

On behalf of the DA&M, the Defense Freedom of Information and Policy Office (DFOIPO), an office within FOID, oversees all FOIA policy matters within the DoD. The Office of the Deputy Chief Management Officer (DCMO) leads and integrates enterprise-wide performance improvement and business operations and is tasked with leading the DoD Open Government Team. This report encompasses the execution of efforts by DFOIPO, DCMO and these 32 DoD Components:

Air Force	Department of the Air Force
AFRICOM	U.S. Africa Command
ASBCA	Armed Services Board of Contract Appeals
ARMY	Department of the Army
CENTCOM	U.S. Central Command
DCAA	Defense Contract Audit Agency
DCMA	Defense Contract Management Agency

DeCA	Defense Commissary Agency
DFAS	Defense Finance and Accounting Service
DHA	Defense Health Agency
DIA	Defense Intelligence Agency
DISA	Defense Information Systems Agency
DLA	Defense Logistics Agency
DoDEA	Department of Defense Education Activity
DoD IG	Department of Defense Inspector General
DSS	Defense Security Service
DTIC	Defense Technical Information Center
DTRA	Defense Threat Reduction Agency
EUCOM	U.S. European Command
JPRA	Joint Personnel Recovery Agency
NAVY	Department of the Navy
NGA	National Geospatial-Intelligence Agency
NGB	National Guard Bureau
NORTHCOM	U.S. Northern Command
NRO	National Reconnaissance Office
NSA	National Security Agency
OSD/JS	Office of the Secretary of Defense/Joint Staff
PACOM	U.S. Pacific Command
SOCOM	U.S. Special Operations Command
SOUTHCOM	U.S. Southern Command
STRATCOM	U.S. Strategic Command
TRANSCOM	U.S. Transportation Command

**2014 Department of Defense (DoD)
Chief Freedom of Information Act (FOIA) Officer's
Report to the Department of Justice**

Table of Contents

Section	Page
I. <u>Steps Taken to Apply the Presumption of Openness</u>	5
II. <u>Steps Taken to Ensure that Your Agency has an Effective System in Place for Responding to Requests</u>	11
III. <u>Steps Taken to Increase Proactive Disclosures</u>	15
IV. <u>Steps Taken to Greater Utilize Technology</u>	22
V. <u>Steps to Improve Timeliness in Responding to Requests and Reducing Backlogs</u>	24
VI. <u>Spotlight on Success</u>	27

**Department of Defense
Agency Chief Freedom of Information Act Officer's Report
to the Department of Justice**

**Michael L. Rhodes
Chief FOIA Officer
Director of Administration and Management
Office of the Secretary of Defense**

Section I: Steps Taken to Apply the Presumption of Openness

FOIA Training:

The DoD remained committed to operating its FOIA programs with the “Presumption of Openness” across its 32 components, as leadership demonstrated that keeping the FOIA community trained and fully engaged in conducting training are top priorities. Seventy-two percent of DoD FOIA professionals and attorneys attended FOIA training.

Over the past year, DoD FOIA professionals and attorneys attended FOIA training sponsored by the DoD, the Department of Justice (DOJ), and the American Society of Access Professionals. Additionally, over half of the DoD Components conducted their own training. Components conducting their own FOIA training were Air Force, Army, CENTCOM, DCMA, DHA, DIA, DoDIG, DSS, DTRA, Navy, NGA; NGB, NORTHCOM, NSA, and OSD/JS.

Although DoD reported last year that it would capitalize on the success of its training conferences implemented at no-cost training facilities, budget restrictions altered that training approach. However, recognizing that training is essential and a priority, DoD increased its efforts to train via the virtual environment within Defense Connect Online (DCO).

Use of DCO allowed the presenter and participants worldwide to participate in training while at their desks. Training slides were uploaded and available to every participant; the presenter presented the material from his/her desk; and every participant had the opportunity to ask questions and engage in dialog during the training session. DoD conducted four training sessions via DCO. These DCO sessions were recorded, and made available on-demand, online for any member of the DoD FOIA community. All DCO training sessions were open to questions throughout. FOIA topics included the following:

1. FOIA 101, a 3-hour training session on the basics of FOIA processing, addressing almost all aspects of the FOIA, with the exception of the exemptions;
2. Exemption 4, a 1.5 hour training session
3. Exemption 5, a 1.5 hour training session
4. Exemptions 6 & 7(C), a 1.5 hour training session

Most significantly, DoD implemented FOIA Chats on DCO and held six such sessions during this reporting period. The chats were led by the Chief of FOID, Will Kammer, and the

Chief of DFOIPO, Jim Hogan, where the hosts addressed the community about FOIA-related current events and invited the community to tune in to get FOIA questions and concerns answered. Because DoD FOIA officers are located in multiple time zones worldwide, these chats were scheduled at different times in an effort to make them convenient for everyone.

Approximately 200 participants were in attendance at each DCO FOIA training and chat session and participants joined the training/chats from across the continental U.S. and from FOIA offices located in Japan, Korea, Germany, Qatar, England and Afghanistan, to name a few.

Despite limited resources DFOIPO, in partnership with the Defense Privacy and Civil Liberties office, was able to host a National Capital Region (NCR) FOIA/PA Training Workshop at the NGA Facility in Springfield, VA. Over 150 FOIA professionals and attorneys in the NCR attended this 3-day workshop. The following were among the topics addressed:

FOIA Best Practices	FOIA – Post Milner Decision
FOIA Exemption 4	Identifying Intelligence Equities
FOIA Exemption 5	Investigative Records
FOIA Exemption 6 and 7C	Litigation Considerations/Attorney Concerns
FOIA/PA Interface	Utilization of Technology

In alignment with the President’s direction that agencies should act “in a spirit of cooperation” remembering that we are “servants of the public”, DFOIPO worked to ensure that the FOIA community gained the necessary skills to work well with the public by maintaining its partnership with the DoD and Army Alternative Dispute Resolution Offices and continuing to train FOIA professionals in the area of conflict resolution/customer relations. These professionals gained skills in relating to customers; understanding conflict; interest-based problem solving; understanding self and others; communications; and overcoming impasse.

FOIA professionals also attended training sponsored by the Office of the Director of National Intelligence and the Department of Energy, where they learned how to better identify intelligence information, formerly restricted data and restricted data within documents requested..

DoD Components were heavily engaged in conducting FOIA training; some of the training conducted:

- Air Force conducted mandatory computer-based training for Air Force FOIA professionals, consisting of FOIA exemptions, the Privacy Act, and FOIA processing. Additionally, FOIA/Privacy teleconferences were frequently held focusing on Air Force implementation requirements, and improving FOIA/Privacy processing.
- Army conducted internal training programs for FOIA professionals focusing on the tenets of the FOIA and FOIA request processing.
- CENTCOM provided quarterly FOIA training for subject matter experts and to Joint Task Force personnel to address unique challenges, applying exemptions, clarifying policy, and to address FOIA topics of interest.

- At DCMA, annual FOIA training was provided to the legal staff, as well as mandatory weekly FOIA question and answer sessions for FOIA staff.
- DHA provided monthly training for new employees covering FOIA topics and Records Management.
- DoDIG conducted basic FOIA training at “All Hands” meetings for various DoDIG Components and DoD GAO liaisons.
- DTRA had a number of training initiatives, including online FOIA/PA training; classroom training for Acquisition/Finance/Logistics and Security personnel; the Administration’s guidelines to senior leadership; and roundtable discussions discussing issues such as search and review processes and transparency.
- Navy held a break-out session at the DoD NCR FOIA/PA Training Workshop to update its FOIA professionals and attorneys on Navy-specific FOIA matters. Additionally, the United States Marine Corps (USMC) provided training to its Inspector General community and a briefing for USMC Plans, Policies & Operations staff.
- FOIA/PA training for new employees was provided by NGA.
- The comprehensive internal “Guard Knowledge Online” website was used by NGB to provide FOIA reference tools and training presentations to its FOIA professionals.
- At NORTHCOM, online FOIA training was provided to all new employees and one-on-one training was provided to staff action officers tasked with responding to FOIA requests. All training included a FOIA overview, summary of the exemptions, and an emphasis on the presumption of openness.
- A 3-day internal FOIA training session was provided for NSA FOIA employees covering the history of FOIA, application of FOIA exemptions, expedited treatment, fees and fee categories, initial processing (including tasking searches), reviewing documents, using the FOIA database, processing contracts, and documents containing equities of other agencies. Furthermore, the NSA FOIA Officer did the following:
 - Briefed the NSA workforce on the protection and release of information under the FOIA;
 - Briefed 30 Operations Security (OPSEC) course instructors on the FOIA; OPSEC managers on the link between FOIA and OPSEC;
 - Briefed 70 employees from the Business Acquisitions community on the FOIA and search and review requirements;
 - Developed modules discussing FOIA requirements and the impact of proper records management on FOIA for use at the NSA’s mandatory annual Records Management Awareness Training, to include the handling of protected information and how FOIA reviews for declassification and release are performed;

- Briefed NSA Senior Leadership on FOIA responsibilities.
- OSD/JS conducted mandatory training for the FOIA on seven occasions during the reporting period, on topics such as Records Management, database documentation, and changes to FOIA processing. Additionally, six training sessions were provided to subject matter experts within OSD/JS.

Fifteen out of 32 DoD Components reported that 100% of their FOIA workforce attended training; eight of the 32 reported that 70 to 99% of their employees attended training; three reported that 40 to 59% attended training; and six reported that less than 10% of their FOIA employees received training during the reporting period.

By continuing to utilize the robust capabilities of DCO, to include recording the trainings, DoD is ensuring that FOIA training is available to 100% of the DoD FOIA community, 24 hours a day, 365 days out of the year, and in any part of the world FOIA professionals and attorneys might find themselves situated. Furthermore, DoD will host an NCR FOIA Training Workshop at the Mark Center in Alexandria, VA in June, and will continue to offer training in the area of Conflict Resolution/Customer Relations. DoD is looking to develop modules to supplement the anticipated DOJ online training modules that will be available in the near future. DoD Components expressed their intent to continue the extensive training programs already in place; continue to take advantage of DoD-sponsored training opportunities; use newly acquired funding to take greater advantage of training opportunities outside of their duty areas; request funding; initiate an in-house training requirement; and include a training requirement within their employees' performance plans.

Outreach:

To demonstrate the DoD's commitment to engaging in dialog with the requester community, FOID leadership visited the National Security Archive to discuss processes in general, and to address specific challenges faced with some of the documents of interest to the National Security Archive. The Archive asked questions on specific cases about which they were concerned. This visit proved to be very beneficial for FOID, since it gave the Archive the opportunity to explain what additional information would be useful to them and perhaps other members of the public, and on how FOID could better categorize information in its FOIA Library.

Sixty-one percent of the DoD Components reported that they regularly engaged in dialog with the FOIA requester community via telephone, email, in-person and during meetings, to inform requesters of the types of documents held within the component; to clarify requests, to keep them updated on the status of their requests; to assist with determining fee categories; and to gain a better understanding of the records the requester is seeking.

Discretionary Disclosures:

Discretionary release reviews have become standard practice in most DoD FOIA offices. Fifty-five percent of the DoD Components reported that they have formal processes in place to

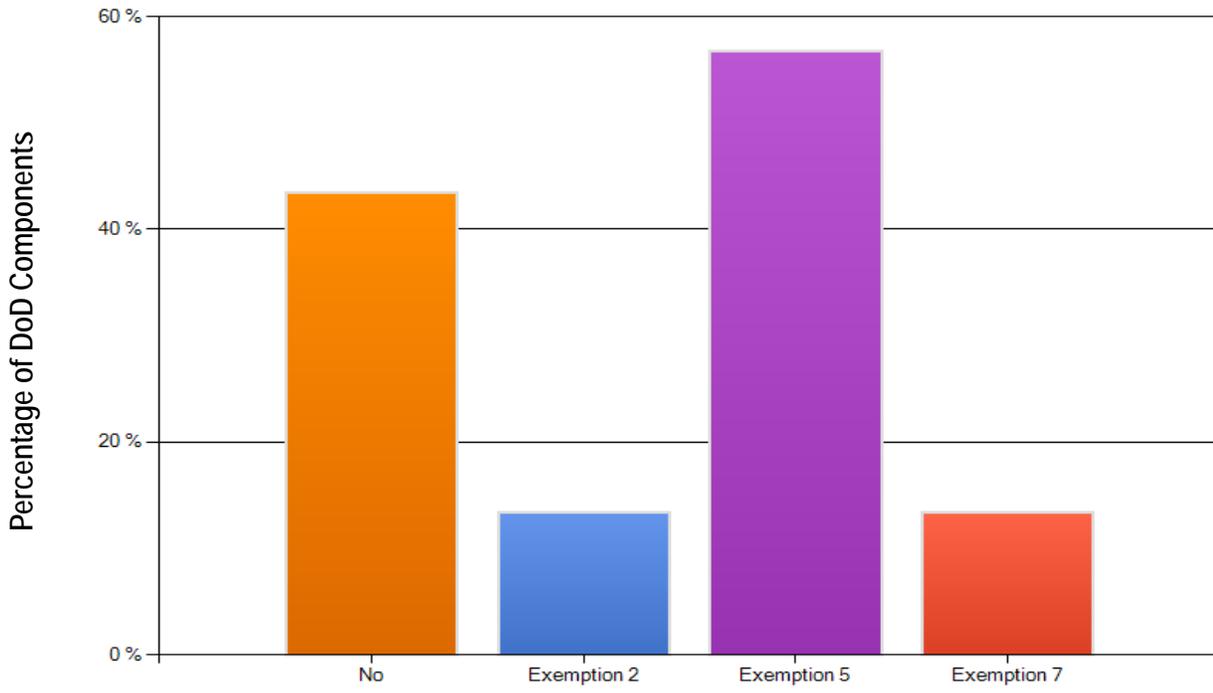
review records for discretionary release. Below are processes in place at the Military Departments:

- Air Force has procedures in place for reviewing all cases before accepting the application of exemptions 2 (internal personnel rules and practices), 5 (privileged information), 7D and 7E (law enforcement information), or 9 (geological and geophysical information). These procedures include a line-by-line review by local Judge Advocates (JAs) to ensure the Attorney General's guidelines are implemented, and include a clear statement of foreseeable harm, in writing, if these exemptions are used.
- Army FOIA processing procedures include an initial review of responsive records by an Army Component's FOIA and legal personnel to make an objective analysis to determine if a discretionary release is feasible.
- When coordinating with subject matter experts (SME), Navy Initial Denial Authorities (IDA) require that a statement of anticipated harm be provided for any claims of exemptions which may be subject to a discretionary release. If, after review, the IDA does not believe that the anticipated harm justifies withholding, the SME is contacted for further coordination until the IDA and SME are in agreement on which information should be withheld under exemptions and which should be released under IDA discretion.

In evaluating FOIA responses for the opportunity of making discretionary releases, the other DoD Component FOIA offices employed a variety of practices including program offices providing harm analyses when claiming exemptions where discretion could be applied; FOIA attorneys assisting FOIA professionals and IDAs in identifying those instances where a discretionary release could be made; directing program offices to make additional reviews; and emphasizing the Attorney General's FOIA Memorandum encouraging discretionary releases with staff personnel.

Fifty-nine percent of DoD Component FOIA offices reported making discretionary releases of otherwise exempt information, while 41% indicated they did not. The exemptions that would have been applied to the discretionary releases were exemptions 2, 5, and parts of 7. As is evidenced in the following chart, most discretionary releases were made on records where exemption 5 of the FOIA could have been applied.

Did your Component make any discretionary releases of otherwise exempt information? If yes, please check the exemptions that would have been used.



Army reported that their activities often made discretionary releases of information under FOIA exemptions 2 and 5. They also reported, “For the past three years the Army has seen a change in the percentage of full grants and partial grants due to the change in the usage of exemptions 2 and 5 (partial grants have decreased to approximately 25% and full grants increased to about 71%); and the emphasis placed on the President’s and Attorney General memoranda on transparency through open government. Openness, discretionary releases, and timely responses to requesters are continuously emphasized.”

Examples of the types of information released as a matter of discretion throughout the components were drafts and supporting material related to final decisions; agency hiring information; material relating to internal discussions; counterintelligence activity reports; escape and recovery reports; records pertaining to hurricanes (Sandy, Andrew, Irene, and Katrina), wild fires, wind farms, situational reports, historical documents, and operating instructions.

While components were able to make discretionary disclosures of some information, documents originating with components engaged in intelligence activities mostly consist of classified information or information that falls under specific exemption 3 statutes and do not lend themselves to discretionary release.

Other Initiatives:

As required by DOJ, DoD solicited input from all 32 components for the quarterly FOIA reports, posted all such reports, and will continue the practice during 2014.

FOIA managers consistently engaged with subject matter experts/action officers to ensure they understood their responsibilities to reasonably segregate releasable from non-releasable information. Many components reported that the President and Attorney General's memoranda on transparency and discretionary disclosure of information were provided during training and given to FOIA personnel, component employees, record owners/reviewers, and to senior leadership.

For example, the CENTCOM Chief of Staff published policy and emphasized the President's direction to encourage and promote accountability through transparency in government to headquarters staff and to the combined joint area of operation. FOIA policy and guidelines, executive orders, and case law decisions affecting openness in government were posted to an internal online portal for all personnel to review. At DIA, the presumption of openness was emphasized during FOIA training to subject matter experts who conducted FOIA reviews of agency records for release. The Air Force continued to publish written guidance, service-wide, to legal and FOIA professionals, about the impact and presumption of disclosure called for in President Obama's policy memorandum, and about the application of specific FOIA exemptions under this policy. FOIA training at OSD/JS included a discussion on the Administration's Open Government initiatives and the potential role of the component in pre-emptively releasing applicable information. Training also included a discussion of the Attorney General's FOIA memorandum, which exemptions most specifically apply, as well as various techniques for affording discretion while still protecting sensitive information, particularly Personally Identifiable Information.

Section II: Steps Taken to Ensure that Your Agency has an Effective System in Place for Responding to Requests

Personnel:

Since the Office of Personnel Management established a job series for FOIA professionals, approximately 50% of DoD FOIA Components have converted their FOIA positions to the new Government Information Specialist series, 0306. Those who have not converted positions report that the action is pending in their Human Resource Offices or that they are working to convert positions during this calendar year. On behalf of the DoD Chief FOIA Officer, DFOIPO will continue to engage those components that have yet to convert their positions to 0306.

Processing Procedures:

Of the DoD Component FOIA offices receiving requests for expedited treatment, 98% of those offices adjudicated the requests in ten days or less. In fact, the overall average number of days to adjudicate expedited treatment requests was less than 5 days. Components who did not adjudicate within the required ten-day timeframe indicated “administrative oversight” and “a cumbersome approval process” as the reasons for the delays. These components indicated procedures are now in place to monitor timelines and streamline their processes that will assist in meeting deadlines in the future.

DoD took advantage of systems in place that are capable of moving large documents from one agency or component to another without overloading email boxes and without compromising security. The Safe Access File Exchange (SAFE) and the Intelink allows FOIA processors to upload documents currently on their computers, obtain a link to where the documents have been uploaded, and send the link to the appropriate reviewer at the component or agency in order to give them immediate access. SAFE is available for use throughout the federal government, while Intelink is available for use by a broad range of customers/stakeholders sharing a common purpose – Intelligence, National Defense, Homeland Security, Law Enforcement, and Diplomatic/Foreign Relations. These systems add significant ease to the referral and consultation processes and decrease the time involved working through these processes.

Fifty-seven percent of the components reported that they have taken steps to make handling consultations and referrals even more efficient. Some examples are as follows:

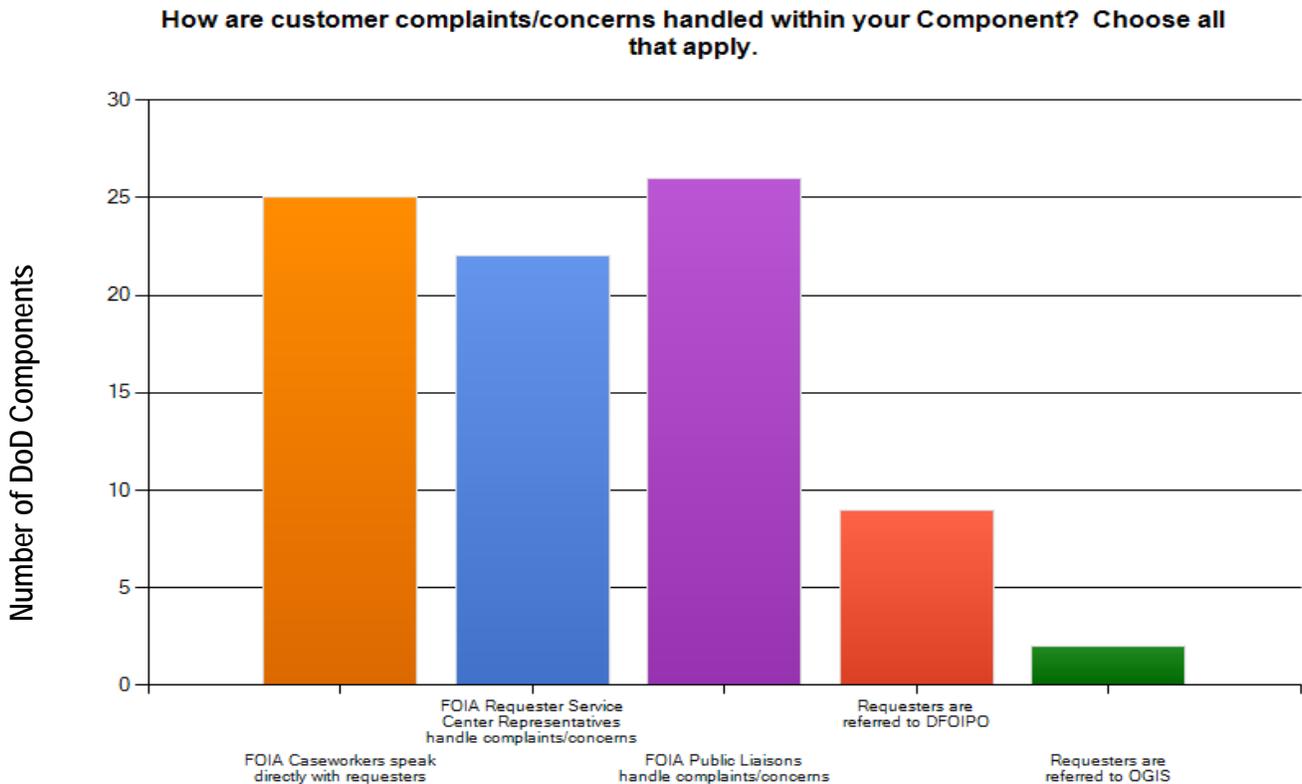
- The U.S. Army Human Resources Command (HRC) established an agreement with the U.S. Army Recruiting Command and Cadet Command on handling individual deceased personnel files and other specific types of requests. Because of their expertise, HRC acts as consultant for these commands, thereby reducing the processing time for requests.
- NSA developed quick "informal" consultation processes which allow an agency to send a request and portion of the responsive document to NSA so that it may quickly determine whether a formal consultation is required. This has hastened the consultation process and allowed other agencies to close their requests more quickly. Additionally, NSA does not require a formal consultation memorandum for extremely simple consultations (of distribution information, for example), and will provide a final response by email rather than a signed memorandum.
- DCMA established a Memorandum of Understanding with the Army in an effort to ensure consistency, efficiency and full compliance with the FOIA. The DCMA FOIA Officer works with the Army to make modifications to this agreement, when necessary.
- In order to make the consultation and referral processes faster, PACOM met regularly with local service component commands, with which they have shared equities.

- DISA engaged with FOIA Officers in the intelligence community to establish a process for handling certain DISA information.

Requester Services:

One hundred percent of DoD Components use email or other electronic means to communicate with requesters, when feasible. FOID fully encourages FOIA officers to dialog with FOIA requesters about the types of documents held within the component; to clarify requests; to keep them updated on the status of their requests; to assist with determining fee categories; to gain a better understanding of the records the requester is seeking, and other matters as they arise. On their FOIA websites, components encourage FOIA requesters to direct concerns, first, to the FOIA Requester Service Center, and then to the FOIA Public Liaison of the component. While DoD is fully committed to handling complaints and concerns expressed by FOIA requesters, DoD refers requesters to the Office of Government Information Services (OGIS) in instances where DoD has exhausted all means/resources/options to resolve the issues of the requester.

Components identified how complaints/concerns were handled within their component and the chart below indicates that the majority of complaints/concerns were handled at the DoD Component level. Sixty percent of the components reported that employees have taken Conflict Resolution/Customer Service training offered by DoD or OGIS.



DFOIPO is finalizing its internal FOIA site within Intelink which will serve as a one-stop shopping location where components will have FOIA tools at their fingertips. The site will make available letter samples, training materials, policy and internal processes, and will provide the capability for FOIA professionals within DoD to chat and share knowledge about various cases they are processing. DoD is optimistic that use of these resources will enable information into the hands of the FOIA processors faster, which could ultimately make FOIA processing faster and more efficient.

Also, DoD Component FOIA Offices are executing a range of practices to ensure that their FOIA systems operate efficiently and effectively.

- The Air Force FOIA Public Liaison conducted regular bi-weekly FOIA/Privacy teleconferences with Air Force FOIA/Privacy professionals to discuss current FOIA trends, workload, and available resources and training. In addition, Air Force conducted backlog reduction reviews with Air Force Components which did not meet backlog reduction goals. These reviews consisted of discussions about attainable goals outlined in written improvement plans which are monitored by the Air Force FOIA Office on a monthly basis. The monthly reviews provided insight on fundamental process improvements, ways to reduce processing time, and ways to improve record searches and tasking. All backlog reduction plans were approved by Air Force Component unit commanders. The Air Force FOIA Public Liaison conducted FOIA training via DCO for Air Force FOIA professionals that focused on the proper use of the Air Force electronic FOIA tracking system and the proper application of exemptions. Throughout the fiscal year, Air Force FOIA promoted the DoD FOIA 101 training by making it electronically available on the Air Force internal shared site for Air Force FOIA professionals. The Air Force FOIA Public Liaison also produced a monthly FOIA metrics report and briefing to the Air Force senior leaders. Emphasis on performance metrics produced a greater focus on timely, accurate and complete search, review, and responses for the decentralized program. Air Force senior leaders routinely expressed support for the FOIA program and the openness objectives, in particular.
- NRO held weekly case management reviews, which included status updates on open FOIA cases and discussed how to improve the processing of existing and future requests. These weekly reviews provided a forum for discussion of both case-specific and broader policy and procedural issues. NRO routinely discussed matters perceived as impediments to case processing, discussed and debated best practices, and examined current procedures to look for opportunities for improved efficiency.
- Air Force, Army, CENTCOM, DTRA, Navy, NGA, OSD/JS, and SOCOM implemented new tracking systems/databases, enhanced existing systems/databases or trained their personnel on accurate data entry within their systems/databases.
- DIA, DoDIG and NGA reviewed processes to improve efficiency and, in some instances, to insure proper alignment within the organization; DHA and NSA updated standard operating procedures to ensure process alignment with DoD and DOJ requirements and to improve process efficiency.

- DHA and STRATCOM identified specific subject matter experts to routinely review documents in their areas of expertise. This resulted in thorough reviews and analysis of what could be released without compromising security. Also, this lessened the need to return packages to program offices to question recommendations and has improved accountability and turn-around time on requests.
- Senior management at DFAS evaluated the FOIA system of internal controls in effect during fiscal year 2013, in accordance with guidance from Office of Management and Budget (OMB) Circular No. A-123, “Management’s Responsibility for Internal Control,” December 21, 2004. The objectives of the system of internal controls are to provide reasonable assurance of “effectiveness and efficiency of operations and compliance with applicable laws and regulations.” Findings after the evaluation of the FOIA program revealed no material weaknesses in either internal controls or administrative controls and that the internal controls are adequate and allow for all FOIA program requirements to be achieved. DFAS developed a FOIA quality metric to measure the quality of FOIA responses and timeliness on tasks. Additionally, DFAS created a FOIA business cycle, which reflects the number of FOIA requests, appeals, and over-aged FOIA requests, which assists with a better understanding of trends. This will assist in forecasting resource and workload requirements and provide high visibility as the charts are briefed to leadership on a monthly basis.
- NGB provided monthly briefings to leadership regarding FOIA backlog and received assistance from National Guardsmen, who assisted the FOIA office with redactions on large and/or complex FOIA requests.

Section III: Steps Taken to Increase Proactive Disclosures

Posting Material:

The system in place at DoD to identify records for proactive disclosures is run by the DoD Open Government Team. This team continues to maintain the DoD Open Government website (<http://www.defense.gov/open>) to provide the latest information on transparency efforts as well as opportunities to collaborate and participate in the Department's activities. Inquiries from the public are answered within 72 hours.

DoD continues to implement Open Government principles with an expanded focus on Open Data as defined in OMB Memo M-13-13, Open Data Policy – Managing Information as an Asset.

In accordance with M-13-13, DoD developed an Open Data website (<http://www.defense.gov/data>) to not only point to the datasets posted to data.gov, but also to accomplish the following:

- Direct the public to additional resources such as the Web Application Programming Interface (Web API) resources (<http://www.defense.gov/developer>) with which interested

parties can produce third-party applications using mobile or other Web 2.0 technologies. Currently, DoD hosts eight web APIs for developers to utilize.

- Solicit input from the public on what kinds of data resources would be most valuable to be made available through data.gov and receive feedback on the priority of effort that DoD should undertake in order to make that data available.
- Showcase DoD's Mobile Application Gallery (<http://www.defense.gov/developer/appsgallery.aspx>) which gives links to some of the premier applications developed by DoD for mobile devices such as smartphones and tablets.

Those customers making requests for Open Data assets that match FOIA guidelines (i.e. are more one-time requests for information rather than a type of data that would be of interest to a larger slice of the public on an ongoing basis), are directed to the FOIA website for OSD/JS and instructed on how to make a FOIA request.

The Open Government Team increased the number of raw datasets posted to data.gov by 66% during 2013. Examples of datasets, data extraction tools, and Web APIs published during 2013 include:

- US Army Corps of Engineers Lock Performance Monitoring System Web API
- OSD/JS FOIA request logs for 2000-2012
- Authorized and funded Army construction in Afghanistan for fiscal year 2010
- Armed Services Board of Contract Appeals Published Decisions - 2012

Also, the US Army Natick Soldier Research, Development, and Engineering Center sponsored DoD's first "hackathon" using open data to produce several mobile applications for providing combat ration nutrition information to deployed troops. Approximately \$6,000 in prizes was awarded to three of twelve submissions through the website Challenge.gov. More information on the submissions and winning entries is at <http://combatfeedinghack.challengepost.com/>.

DoD Component FOIA Offices reported the following:

- Air Force used its web-based application to track, process, and post FOIA releases, as well as records proactively disclosed, to its Reading Room, <http://www.foia.af.mil/reading/index.asp>. Air Force posted FOIA Annual reports, contracts, aircraft accident reports, historical reports, mission reports, government purchase card holders, radar reports, FOIA logs, investigation reports, organizational charts, phone books/directories, audit reports, FOIA training material, policy, guidance, flight operations, unit history, historical honors, mechanical reports, congressional travel, and factsheets.

- Army FOIA personnel reviewed unclassified, non-sensitive, FOIA requests, without privacy implications, and of potential interest to the public, for posting on websites and to the Army Reading Room. This included documents released multiple times to FOIA requesters; likely to become the subject of future requests; documents released to the media; of interest to public interest groups; and documents pertaining to subjects on the Army's hot topic list of significant FOIA issues, such as information concerning Private Bradley Manning Court Martial. These Army postings are located at the following link: https://www.rmda.army.mil/foia/FOIA_ReadingRoom/index.aspx.
- Navy FOIA personnel coordinated with Navy Public Affairs offices to identify subjects of potential public interest. Once identified, records custodians and subject matter experts were consulted to determine what records might exist and whether any portions of these records would be releasable. Community-wide announcements were disseminated to advise all Navy FOIA personnel of major matters which may warrant proactive disclosure.
- ASBCA began posting, on its website at www.asbca.mil, all decisions and dismissal orders related to matters on its docket. Previously, ASBCA only posted decisions or dismissal orders that contained significant legal analysis likely to be of interest to government contracts law practitioners.
- DHA required contractors to provide releasable versions of contracts so that their FOIA Office could proactively post them to the DHA FOIA Reading Room site at the following link: <http://www.tricare.mil/tma/privacy/FOIAReadingRoom/readingroom.aspx>. Additionally, DHA posted frequently requested information online. DHA underwent an extensive process of converting online material to ensure Section 508 compliance, so that the information would be more readily available to a broader segment of the public.
- DIA made proactive disclosures through the Public Affairs Office and routinely posted updates at www.dia.mil. When appropriate, DIA routinely posted these updates to its official social media presences on Facebook, Twitter, and YouTube. DIA posted news articles about DIA-sponsored or DIA-attended events, to include the following:
 - Stories about efforts to help the community;
 - Articles detailing DIA's contributions to historical events, to include information on the anniversary of the capture of Saddam Hussein;
 - Congressional speeches and testimonies, including transcripts of DIA Director, Lieutenant General Flynn's speech at the 4th Annual Intelligence and National Security Alliance Achievement Awards and his statement before the Senate Armed Services Committee on the Annual Threat Assessment;
 - Videos of senior leadership messages to the workforce and public, including a message from the DIA Director on intelligence and national security.

- DoDIG provided, on its website, a consolidated listing of investigative reports that included name, date, and title. Reports that were not FOUO or classified were made available to the public on the site. Information on how to file a FOIA request was provided for the remaining reports. The listing of these reports can be viewed at <http://www.dodig.mil/pubs/index.cfm>.
- The DTIC Open Government page provided the public with a broad range of scientific, technical, engineering and business related resources for academic research. This page serves to enhance efforts to improve the exchange of public information by providing easy access to scientific and technical resources as well as budgetary, social science, policy, and other resources available in the DTIC collection and through the DTIC Online integrated search at <http://www.dtic.mil/dtic/opengov/index.html>. The White House, in its Innovations Gallery, recognized DTIC's Open Government initiatives. Also, DTIC was a Government Computer News award winner "for notable IT accomplishments in advancing the work of agencies in serving the public."
- The DTRA Chief Information Office has a system in place for reviewing records for posting on the agency's external website. Currently, the DTRA FOIA and Public Affairs offices do not have Webmaster support. However, the FOIA office has a web content Manager who handles the submission/uploading of Privacy Impact Assessments. Also, DTRA created a Facebook page, along with accounts for Twitter and Flickr. These Social Network tools are maintained by the Chief, Public Affairs office.
- The NSA FOIA and Declassification Services Offices identified records appropriate for posting based on requester interest. These offices did not wait for there to be frequent requests, but based the decision to post information on the likelihood that others would have a significant interest in having access to the information. NSA added two new sections to the front page of its public website www.nsa.gov. With these new sections, the general public was able to see NSA information released in response to news reporting on the unauthorized disclosure of classified information. Examples included statements to the press, as well as public speeches, found at the following link: http://www.nsa.gov/publi_info/speeches_testimonies/index.shtml. The NSA FOIA and Declassification Services office reviewed, released, and posted 136 editions of the Cryptolog (4,400 pages), along with frequently asked questions about the history of the journal and the significance of the release. NSA posted 100 additional documents (249 pages) relating to the USS PUEBLO incident, *History Today* articles, an *NSA Technical Journal* article, Cryptologic History documents, NSA policies, and several miscellaneous documents, totaling over 1,000 pages.
 - The NSA Research Directorate posted the following new material on NSA.gov at <http://www.nsa.gov/research/index.shtml>: Science of Security contest winners; information about the NSA partnership with North Carolina State University; the 20th Anniversary issue of its quarterly publication, *The Next Wave*.
 - The NSA Information Assurance Directorate (IAD) published information on both the NSA web page, as well its web page at www.iad.gov.

- Examples of new information made available in 2013 by IAD were as follows:
 - NSA Mobility Program (Mobility Capability Package Version 2.3)
 - Campus Wi-Fi Capability Package - VPN Capability Package (Version 2.0)
 - National Information Assurance Partnership Approved Protection Profiles - Release of CGS Versions 1.0 and 1.1 onto both IAD.gov, and the SIA.mil sites
 - IAD unclassified 14 minute video "Confidence in Cyberspace" - IAD unclassified "Executive-level" cybersecurity guide
 - Host Based Security System Host Intrusion Prevention System Application Whitelisting Technical Implementation Guide
 - Hardening Network Infrastructure: Security Recommendations for System Accreditors
 - IAD's Top 10 Information Assurance Mitigation Strategies
 - Antivirus File Reputation Slicksheet - Control Admin Privileges
 - Limit Workstations to Workstation Communication
 - Take Advantage of Software Improvements
 - Segregate Networks and Functions
 - Spotting the Adversary with Windows Event Log Monitoring
 - Reducing the Effectiveness of Pass the Hash
 - Building Web Applications-Security Recommendations for Developers
 - Security Tips for Personally Managed Apple iPhones and iPads
- OSD/JS continued to post every FOIA release not containing any privacy implications in its FOIA Library. Significantly, this was lauded as a “Best Practice” in the Center for Effective Government’s (formerly OMB Watch) published report. OSD/JS also began posting documents released under the DoD Mandatory Declassification Review Program. These documents reside within this component’s Special Collection Library at the following link <http://www.dod.mil/pubs/foi/specialCollections/MDR/>.

Making Posted Material More Useful:

DoD Component FOIA offices continued to update websites in an effort to make them more user friendly and adapted the practice of using social media to announce major updates and the proactive disclosure of information likely to be of significant interest to the public. Army announced the release of information concerning Private Bradley Manning; NSA, via press releases, announced its partnership with North Carolina State University and announced the start of the Science of Security Cybersecurity Paper Competition. On its website, NSA announced the anniversary issue of its publication “The Next Wave”. The NSA Research Directorate (RD) also participated in a recent *CBS 60 Minutes* segment and the film crew was given access to several locations within RD Headquarters offices. The day after the Navy Yard shooting, DoDIG announced the proactive posting of the report, “Navy Commercial Access Control System Did Not Effectively Mitigate Access Control Risks.” DHA announced the stand-up of their new agency.

DoD Components reported that they have faced the following challenges to posting information:

1. Lack of resources and reduced budgets.
2. Long wait times exist to have documents posted by the offices assigned this duty.

In spite of challenges, DoD Components are going beyond posting material to their websites:

- The Air Force FOIA Office continued to provide more information on its FOIA website, to include the latest guidance on Air Force FOIA policy and procedures, and additional information on how to locate records without submitting a FOIA request. The Air Force has a blog account to discuss issues surrounding specific program area concerns and provides updated information to the staff and public through more 'informal' channels. Air Force FOIA Office continued to monitor each FOIA Requester Service Center website to ensure it contains direct contact information for their local office such as email, postal address and phone numbers; links to the Air Force FOIA Public Liaison office; and a link to the main Air Force FOIA page. The main Air Force FOIA page includes direct contact information to the Air Force FOIA Public Liaison and a directory of all Air Force FOIA RSCs.
- Army reorganized the documents in its FOIA Reading Room into subject categories (e.g. Contracts, Criminal Investigation Records, Intelligence Documents, etc.) and upgraded the site's search capabilities. Users may now conduct an advanced search by the title, subject, keywords, document date, document number, originator, category and sub-category, and date ranges. Members of the public may submit feedback pertaining to the content or presentation of posted material may be submitted using the Army FOIA office e-mail address posted online.
- DCAA upgraded the agency's public website in fiscal year 13. Significant updates included DCAA Contract Audit Manual updates, Audit Program updates and open audit guidance updates. Other significant additions included: Incurred Cost Adequacy Checklist, updates to DCAA's Incurred Cost Electronic (ICE) Model, fiscal year 13 Active Contractor Listings and other relevant information about DCAA audits. DCAA estimates that the posting of this information relieves requesters from having to submit requests for this information. Prior to proactively posting the Active Contractor Listings and audit information, DCAA received approximately 25 requests yearly for such information. DCAA also created a Facebook page for recruitment and general information about the agency.
- The DeCA routinely utilized its public website, www.commissaries.com, as well as Facebook (facebook.com/yourcommissary) and Twitter (twitter.com/yourcommissary) to provide information to commissary patrons and to allow patrons to provide immediate feedback.
- In 2013, DIA enhanced the search capability on www.dia.mil by incorporating the USA.gov search engine. This tool automatically archives all website content and

social media posting on primary social media accounts, and provides detailed analytics that give insight into what visitors to www.dia.mil are seeking. DIA is currently evaluating how to transition www.dia.mil to a responsive design that will be optimized for mobile and desktop visitors. In 2014, these updates will be expanded to include notifications of when the website has been updated, to include postings within the FOIA Reading Room as well as the quarterly updates required by the Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002 (commonly known as the NoFEAR Act).

- DoDIG has a Twitter account that updates subscribers on the release of recent reports and links to a full copy of the report when a report is publicly available. Additionally, the agency produced a monthly IG newsletter that is sent to subscribers and advised the public of recently completed investigations and upcoming reports.
<http://www.dodig.mil/ELetter/eletter.cfm>
- NSA is going beyond posting in many ways:
 - The Information Assurance Development Mobility Program leadership regularly reviewed published materials (e.g., Capability Packages) and considers opportunities to further share information about the program's vision and strategy.
 - NSA consistently sought opportunities to make revisions to published materials in order to make them more useful to the community of people who regularly access the NSA public website.
 - The Mobility Program completed two revisions to the Mobility Capability Package (Enterprise Mobility Versions 2.2 (July 29, 2013) and 2.3 (November 4, 2013)). While intended primarily for industry and Government users, these significantly enhanced documents were made accessible by the public to promote communication, clarify security requirements, and enhance understanding about the Mobility Program's commitment to effective commercial solutions.
 - The NSA Associate Directorate for Human Resources Staffing Services Division found that social networking is an easy to use tool for NSA to market career opportunities and answer questions from potential candidates. This office partnered with Public Affairs to use its RSS feeds to filter new NSA news to the NSA Careers Link application and to post the latest news to NSA's Facebook, Twitter page and LinkedIn.
 - The NSA also has a public website and open phone lines which could be used to provide comments, recommendations, and concerns about the content. To ensure that information is relevant and timely to the general public, NSA reviewed the NSA.gov website and is in the process of updating the "Research" section of the site.

- EUCOM proactively shared information via blogs, news articles videos, Twitter, YouTube, Facebook, Flickr and Pinterest.

Section IV: Steps Taken to Greater Utilize Technology

Online tracking of FOIA requests

The majority of DoD Component FOIA offices do not have the capability to allow a FOIA requester to track FOIA requests online. Components that do have the ability to track FOIA requests online are Air Force, CENTCOM, Navy, OSD/JS, and TRANSCOM. The following is a summary of these capabilities:

- The Air Force and OSD/JS have an online portal that requires requesters to login, using their user identification and password. Once within the portal, the requester sees the case number, case description, received date, estimated date of completion, fees due and case status. The case status reads as *Received*, *Closed* or *In-progress*. At the site, requesters may also see the name and contact number of the assigned caseworker, in the event they need additional information about their request.
- CENTCOM has a webpage that provides the requester with the date of the request, the received date and the number in the queue. CENTCOM provides the requester a link to the webpage when providing the requester with an acknowledgement letter. The acknowledgement letter also provides a case number and a contact number for requesters to obtain additional information about their request.
- TRANSCOM has an interactive website, managed by its information technology team. The FOIA website has a “Request Status” link. Once requesters click on the link they get a list of FOIA requests that are *Open*, *Closed* or *In-process*. Beside each case is a link that contains comments about the case. If a requester decides to click on the comments, the requester will get status information as general as *Request Added*; *Request has been updated*; *Current status: OPEN*; or *Current status: CLOSED*. In some instances, the requester will get very detailed information, which could include information about interim responses made. To better illustrate, below are screen shots from the TRANSCOM status log.

Current FOIA Requests

FOIA Request ID	Date Received	Status	Estimated Response Date	Comments
14-13	2013-11-22	OPEN	2013-12-23	Read
14-12	2013-11-22	OPEN	2013-12-23	Read
14-11	2013-11-15	OPEN	2013-12-16	Read

Comments

FOIA Id: 12-78

Comment Date	Comment
2012-06-22	Request Added
2012-06-22	Tasked to the staff for records search
2012-08-02	Status to requester sent via 3-mail 2 Aug 12.
2012-08-29	Interim Response #1 sent via e-mail on 14 Aug 12
2012-09-04	Interim response #2 sent via e-mail 29 Aug 12.
2012-09-06	Interim response #3 in staff coordination.
2012-09-24	Interim response #3 sent 18 Sep 12 via e-mail to requester.
2012-10-26	Interim Response #4 in progress--voluminous responsive records being reviewed & redacted. Records being released through interim responses as they become available.
2012-11-27	Interim Response #4 sent electronically 20 Nov 12
2013-08-28	Request has been updated. Current status: IN PROCESS

While the remaining DoD Components do not have the capability for FOIA requesters to track the status of FOIA requests online, since 2006 all FOIA Requester Service Centers have been required to provide contact information so that FOIA requesters can obtain the status of their requests through either a telephone call or email. To assist in obtaining this information, FOIA officers provide acknowledgement letters with the case number, along with their contact information to requesters.

The Department of the Navy has decided to participate in the FOIAOnline portal, which will give their FOIA requesters the capability to track FOIA requests online.

Fifty-six percent of DoD Component FOIA offices reported they do not have plans to pursue online status tracking, with limited resources being the primary deterrent. Because some components have FOIA tracking systems on classified networks, a separate but identical unclassified system would have to be maintained to enable requester-oriented enhancements such as immediate online request status and the receiving of a FOIA request directly into a tracking system. Maintaining such a separate system on an unclassified network, along with a duplicate system on a classified network, and keeping both systems up-to-date, would be resource intensive. Some components report that the cost to implement an online capability in comparison to the relative small number of requests received would not be beneficial; these components already have processes in place that involve personal contact with the requesters. Some Components related that discussions with requesters revealed that, to a large extent, requesters prefer personal contact to the often generic information they receive through electronic online tracking mechanisms; and those with electronic tracking systems report that requesters who are able to see their request status at FOIA websites and online portals still take

advantage of the opportunity to call in to speak with assigned caseworkers for greater detail about the status of their requests.

Use of technology to facilitate processing of requests:

Sixty-seven percent of the DoD FOIA Components are implementing more advanced technology to facilitate overall FOIA efficiency. With the understanding that the management of records throughout the organization is key to faster and more efficient searches, FOIA offices are reporting that sound and, in some instances, improved Records Management practices are underway within their components. AFRICOM, CENTCOM, DeCA, DCMA, DoDIG, Navy, NSA, and STRATCOM reported that they are executing better searches because of the Records Management programs in place within their components. NSA reported Records Management enhancements that automate receiving, managing and shipping records. The automation effort enables users to create entries, track, and manage records from their desktops.

CENTCOM reported the implementation of new *de-duplication software*, while DHA, DIA, NSA and OSD/JS are working to obtain this software for more efficient case processing. This software efficiently removes duplicate records from computer programs so that FOIA processors will only have to review a document for release once. This is extremely helpful when processing emails. As components begin to hear more about the success with the use of tools such as Intelink and SAFE, they are beginning to implement them within their processes to safely move documents for consultations and referrals. NRO is now using Intelink for document sharing and has obtained improved software for case management. Army has upgraded search capabilities within its database in order to improve search capabilities within the system and to implement greater accountability with regard to meeting deadlines.

Approximately ten percent of DoD's components are working to implement, upgrade or purchase FOIA databases to track case processing. Components reported the need for a tool that will assist with the processing of emails, especially in the areas of search and de-duplication. Components also see the need for a tool that would assist with the sorting of documents already processed under the FOIA.

Section V: Steps to Improve Timeliness in Responding to Requests and Reducing Backlogs

Simple Track Requests

DoD utilizes separate tracks for simple and complex FOIA requests and 87.5% of DoD Components reported that the average number of days to process simple FOIA requests was 20 working days or fewer. In fact, the overall average number of days for DoD to process its simple FOIA requests is 10 working days.

Backlogs and Ten Oldest Requests, Appeals and Consultations:

DoD received 68,014 FOIA requests during fiscal year 13 and processed 67,679 FOIA requests. In spite of funding shortfalls, hiring freezes, and government furloughs, the DoD FOIA

backlog only increased by 3.5 %; and DoD was able to make great strides in the closing of its ten oldest requests, appeals and backlogs.

Backlogs: Fifty percent of the 32 DoD Component FOIA offices either reduced their backlogs or maintained a backlog of zero. The DoD Components processing over 1000 requests reporting backlog reductions are:

- Army - from a backlog of 625 to 515 (18%);
- CENTCOM – from 205 to 177 (14%);
- DIA - from a backlog of 1132 to 809 (decreasing by 28.5%);
- DLA – from 23 to 1 (96%);
- Navy – from 1202 to 1163 (3%).

Components processing less than 1000 requests reporting backlog reductions are:

- NGA – from 73 to 51 (30%);
- DCMA – from 49 to 37 (24.5%);
- DTRA – from 39 to 30 (23%);
- DSS – from 8 to 5 (37.5%);
- NORTHCOM – from 16 to 11 (31%);
- EUCOM – from 37 to 35 (5%);
- DoDEA and JPRA – from 1 to 0.

Two components, ABSCA and DeCA, maintained a backlog of zero.

DoD reduced its backlog of appeals by 12.5 %, going from a backlog of 769 in fiscal year 12 to a backlog of 673 in fiscal year 13. Components with significant reductions include:

- DIA from 147 to 92 (decreasing by 37%);
- NSA – from 79 to 56 (29%);
- OSD/JS - from 354 to 302 (15%);
- DLA - from 4 to 0;
- DSS - from 1 to 0.

Ten Oldest Requests, Appeals and Consultations: DoD closed all of its ten oldest appeals and consultations and to date has closed eight of its ten oldest initial requests. .

Reasons for Backlogs and Ten Oldest Not Closed and Plans to Resolve:

While DoD decreased its backlog of FOIA appeals by 12.5%, the backlog of initial FOIA requests increased by 3.5%. Components reported that increases in backlogs of FOIA requests were due to an increase in the number of incoming requests, the effects of reductions in resources that included loss of staff, hiring freezes, and furloughs, and the increase in complexity of FOIA requests. NSA's dramatic increase in incoming FOIA requests (1809 in fiscal year 2012 and 4060 in fiscal year 2013) played a major role in both their increase in backlog and their inability to close two of the DoD ten oldest FOIA requests. With the requirement to address expedited treatment requests within 10 days and the need to log, assign case numbers and acknowledge receipt within, at least, 20 working days, NSA FOIA is facing a challenge that is far greater than ever expected.

DFOIPO recently visited NSA to consult with its FOIA leadership on the issues behind the increase in backlog and closing the final two of DoD's fiscal year 2012 ten oldest requests. NSA continues to receive a high volume of initial FOIA requests; since June 6, 2013, NSA has received 4989 FOIA requests, which is an average of 554 FOIA requests per month. As a comparison, in fiscal year 2012 NSA received an average of 151 FOIA requests per month. This is an increase of 267% in incoming FOIA requests. Given this dramatic increase in its workload, it is understandable that NSA is having difficulties in both backlog reduction and closing its oldest FOIA requests. Another contributing factor is the fact that some information concerning NSA's activities has been recently declassified. This has necessitated NSA to conduct new reviews of open FOIA cases that they were processing in addition to reprocessing a large amount of information that was subject to litigation. Because the litigation efforts take priority over the processing of initial FOIA requests, resources normally assigned to the processing of initial FOIA requests must be reassigned to litigation support.

DFOIPO is satisfied that NSA has properly allocated its available resources to focus on both its backlog and closing its oldest open requests. NSA has highly qualified FOIA analysts assigned to specific teams that focus on these two issues. Given there is no expectation that this high volume of FOIA requests will decrease anytime in the near future, without additional resources it will be very difficult for NSA FOIA to realistically deal with these two issues. Therefore, in an effort to resolve backlog issues, NSA FOIA has requested additional resources with a business case analysis. As for the two remaining FOIA requests from the fiscal year 2013 10 oldest, NSA reported that the two remaining requests are very complex, involving highly complicated classification matters. NSA anticipates providing the requesters with all releasable responsive NSA documents by the end of fiscal year 2014.

Other DoD Components reported, in order to resolve backlog issues, they will implement senior leadership involvement; process improvement efforts; overtime; monthly reviews to address challenges; and establishment of a team to focus solely on backlog issues.

Interim Responses:

Recognizing the importance of getting information into the hands of requesters as quickly as possible, 100% of the DoD Component FOIA offices have a system in place to provide interim responses to requesters. Less than 5% of the components have the ability to track the number or percentage of substantive interim responses provided to requesters on backlogged cases. Those able to track this data reported that substantive interim responses were made on 40 – 50% of their backlogged requests.

Use of FOIA’s Law Enforcement “Exclusions”

None of the DoD Component FOIA offices reported the use of law enforcement exclusions.

Spotlight on Success

Recognizing that quality training is essential to success in any FOIA program, DoD increased its efforts to train via the virtual environment within Defense Connect Online (DCO). The advantages of DCO training were as follows:

- Ability to reach the DoD FOIA community in great numbers, saving thousands of dollars in travel and conference fees, and minimized time away from duty stations.
- An online chat capability where participants can ask the briefer questions in real time.
- Allows participants to gain valuable information right at their desks.
- Training sessions are recorded, giving DoD personnel the opportunity for quality FOIA training 24 hours a day, 365 days per year.

DoD conducted a variety training sessions via DCO. These sessions were open to questions throughout and included the following:

- FOIA 101, a 3-hour training session on the basics of FOIA processing, addressing almost all aspects of the FOIA, with the exception of exemptions;
- Exemption 4, a 1.5 hour training session
- Exemption 5, a 1.5 hour training session
- Exemptions 6 & 7(C), a 1.5 hour training session
- FOIA Chat sessions, where the topics were varied, and often driven by participant questions.