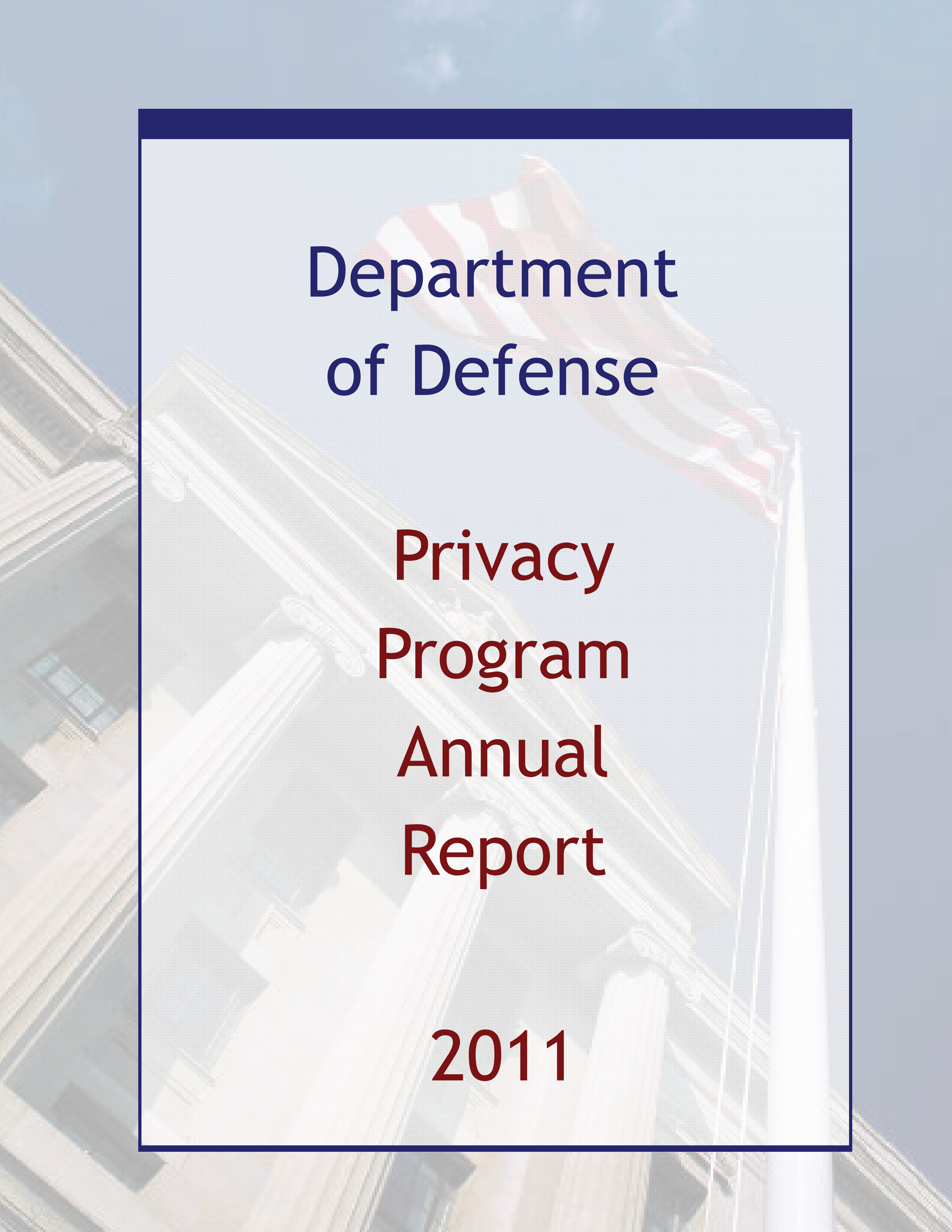


Department of Defense

Privacy Program Annual Report

2011

Published by the

Defense Privacy and Civil Liberties Office
2011

http://dpclo.defense.gov

TABLE OF CONTENTS

TABLE OF CONTENTS

Message from our Senior Official for Privacy

The Defense Privacy and Civil Liberties Office compiled this first-ever summary report to provide Department of Defense (DoD) leadership and the public with an informative review of our privacy program. This report outlines our daily activities and highlights a selection of our most significant accomplishments to date.

The Department's commitment to privacy has a 36-year history. We strive daily to protect the privacy of DoD personnel as well as the privacy of those individuals whose information we maintain. When DoD is requested or required to share information within the Department or with another Federal agency, we seek to ensure that safeguards are in place to protect that information at every step.

With constant changes in technology and in society's evolving expectations of privacy, our challenges never cease. Identity theft is a recurring problem frequently resulting from the breach of personally identifiable information. The news is also full of stories related to inappropriate disclosures of information through social media. These are issues that we monitor closely in order to improve our service to DoD and the wider community.

We frequently partner with technology experts to design better systems for storing, sharing, and retrieving important information on individuals. We constantly examine how new technologies and new policies impact the security of personally identifiable information and other privacy-related matters.

We are grateful for the opportunity to serve the DoD community and the public by protecting the privacy of every individual who has entrusted us with their information. To learn more about our program, please visit http://dpclo.defense.gov.

Michael L. Rhodes

Defense Privacy & Civil Liberties Office
1901 South Bell Street, Suite 920
Arlington, VA 22202-4512

Published 2011
Arlington, VA
http://dpclo.defense.gov

This page intentionally left blank.

DoD Privacy Program History and Purpose

The Department of Defense (DoD) Privacy Program is headquartered within the Defense Privacy and Civil Liberties Office (DPCLO). Our mission is to implement the DoD Privacy Program through advice, monitoring, official reporting, and training.

History and Who We Are

Our program was founded in 1975, after passage of the Privacy Act of 1974 (5 U.S.C. 552a, as amended). The Privacy Act arose out of two powerful currents within the United States during the 1960s and 1970s: Government abuse of records held on its citizens and the dawn of the automation age. By passing the Privacy Act in 1974, Congress recognized Federal agencies' need to collect and maintain information on citizens, and, at the same time, provided citizens with a way to access their personal records maintained by Federal agencies.

Image courtesy of the Library of Congress.

To fulfill its mission, DoD has an ongoing need to collect and maintain information on various persons. The DoD Privacy Program ensures that citizens' personal privacy is protected with respect to the records that DoD maintains.

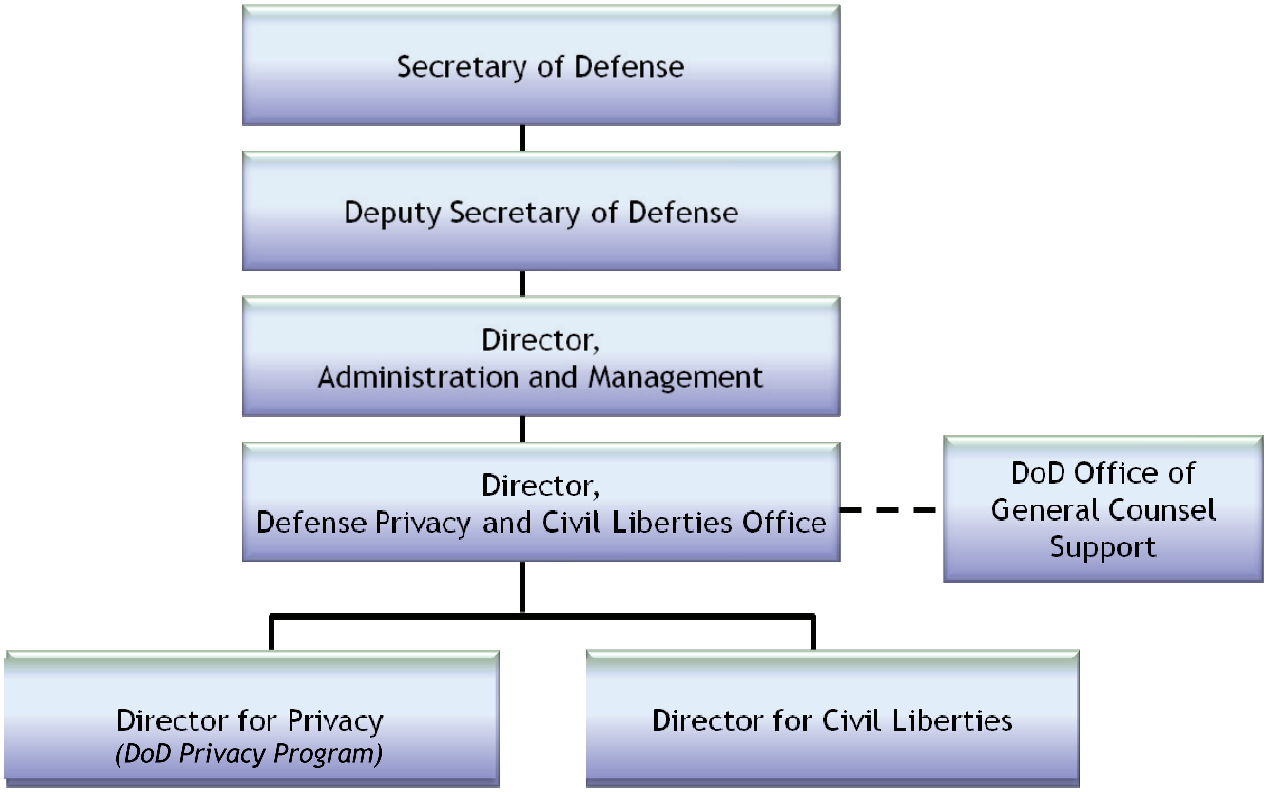

Secretary of Defense
Deputy Secretary of Defense
Director, Administration and Management
Director, Defense Privacy and Civil Liberties Office
DoD Office of General Counsel Support
Director for Privacy (DoD Privacy Program)
Director for Civil Liberties

Figure 1. Organizational Chart. Position of the DoD Privacy Program within the Department of Defense.

How do we communicate with the "front lines" of the privacy program?

DoD is an exceptionally large Federal agency. Managing privacy for DoD involves not only programmatic leadership and guidance, but committed Component-level support.

DoD Components operate privacy programs at the Component level, staffed by privacy officers and support staff. These DoD Component personnel provide the day-to-day, on-the-ground privacy program support for their respective Components.

DoD privacy officers guide and train their Component personnel; advise leadership whenever privacy protection can be improved; compile reports on privacy breaches and compliance; and often support collateral duties regarding information sharing and other issues related to privacy.

Certain DoD Components are represented on the Defense Privacy Board, some as voting members, others as participants. The Board meets monthly to discuss current issues and hot topics, share innovations and best practices, and ensure continued excellence within the Defense Privacy Program.

DoD was the first Federal agency to establish a privacy program, and was commended by Congress in the early 1980s for its proactive approach to privacy protection. Our program has enjoyed significant stability in its 36 years of operation, being led by only four Directors.

We provide program guidance to all DoD Components represented on the Defense Privacy Board *(see page 10)*, which is chaired by the Senior Agency Official for Privacy. The Board's Executive Secretary is the DoD Director for Privacy.

What We Do

While our role within DoD continues to evolve, our program's mission is consistent—to provide a comprehensive framework which regulates how and when DoD collects, maintains, uses, or disseminates personal information on individuals. We focus on balancing the information requirements and needs of DoD with the privacy interests and concerns of the individual.

In discharging DoD Privacy Program responsibilities, we perform multiple functions. We:

- Develop policy, provide program oversight, and serve as the DoD focal point for Defense privacy matters.

- Provide day-to-day policy guidance and assistance to DoD Components in the implementation and execution of their privacy programs.

- Review new and existing DoD policies which impact the personal privacy of individuals.

- Review, coordinate, and submit for publication in the Federal Register, Privacy Act system of records notices (SORNs) and Privacy Act rulemaking by DoD Components.

- Develop and coordinate Privacy Act computer matching agreements between DoD Components and other Federal and state agencies.

- Develop and coordinate memoranda of understanding for computer matching among DoD Components.

- Provide administrative and operational support to the Defense Privacy Board and the Defense Data Integrity Board.

For more information

About our office,
please visit our website
http://dpclo.defense.gov/

We continue to grow and improve our services every year while remaining true to our core principles of privacy protection. The following section provides examples of our endeavors to protect individual privacy.

Program Activities

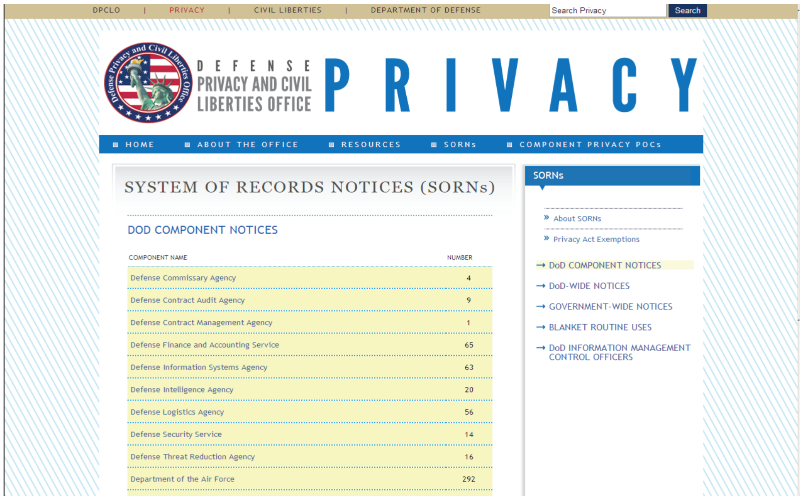
Like many Federal agencies, we have a responsibility to report to our agency's senior leadership, Congress, and others on certain issues and events. The Privacy Act and related policy documents require DoD to report on systems of records maintained by DoD, breaches of personally identifiable information (PII), Federal information security, and more. What follows are explanations of the reporting that we conduct for DoD, the requiring authorities (i.e., legislation), and notes about how we have improved and continue to improve reports and processes.

Transparency

The relevant definitions of transparency are "to be easily recognized or detected" or "to be manifest or obvious." In 2009, President Obama issued a memorandum (*Transparency and Open Government*) requiring greater transparency in Federal government operations. DoD supports this effort in several ways through robust reporting requirements and by publishing information online and in the Federal Register. The following segments outline a few of our reporting requirements.

Systems of Records & System of Records Notices

A system of records (sometimes abbreviated as *SOR*) is a group of records, whatever the storage media (paper, electronic, etc.), under the control of a DoD Component from which personal information about an individual is retrieved by the name of the individual, or by some identifying number, symbol, or other particular that is assigned uniquely to that individual. Under the Privacy Act, any individual is entitled to see his or her information contained within a Federal system of records. Individuals can also request an amendment to their record(s) if the information is incorrect in any way. For example, if a military member's personnel


DPCLO | PRIVACY | CIVIL LIBERTIES | DEPARTMENT OF DEFENSE
Search Privacy
Search
Defense Privacy and Civil Liberties Office
DEFENSE PRIVACY AND CIVIL LIBERTIES OFFICE
PRIVACY
HOME
ABOUT THE OFFICE
RESOURCES
SORNs
COMPONENT PRIVACY POCs
SORNs
» About SORNs
» Privacy Act Exemptions
→ DoD COMPONENT NOTICES
→ DoD-WIDE NOTICES
→ GOVERNMENT-WIDE NOTICES
→ BLANKET ROUTINE USES
→ DoD INFORMATION MANAGEMENT CONTROL OFFICERS

SYSTEM OF RECORDS NOTICES (SORNs)

DOD COMPONENT NOTICES

COMPONENT NAME	NUMBER
Defense Commissary Agency	4
Defense Contract Audit Agency	9
Defense Contract Management Agency	1
Defense Finance and Accounting Service	65
Defense Information Systems Agency	63
Defense Intelligence Agency	20
Defense Logistics Agency	56
Defense Security Service	14
Defense Threat Reduction Agency	16
Department of the Air Force	292

To view DoD SORNs, visit our website at http://dpclo.defense.gov/privacy/SORNs/SORNs.html records are inaccurate, the individual has the right to request that the record be corrected.

How would an individual find out whether DoD maintains a record on himself? By consulting the SORNs published in the Federal Register.

For more information

About SORNs, please visit our website

The Privacy Act states that any system of records must have an accompanying SORN. Publishing the SORN in the Federal Register allows anyone in the public to learn about information that DoD maintains on various categories of individuals. A SORN includes the following details about a system of records:

- the system name and location
- categories of individuals covered by the system
- categories of records in the system
- authority for maintenance of the system
- purpose(s) for establishing the system
- routine uses of records maintained in the system
- policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system
- system manager(s) name and address
- notification procedure
- record access procedures
- contesting record procedures
- record source categories
- exemptions claimed for the system

Component level privacy program personnel are responsible for completing and publishing SORNs for every DoD system of records developed by a DoD Component. We help DoD Components complete and publish their SORNs.

Computer Matching Agreements

Computer matches involve two kinds of matching programs. The first are matches of records from Federal personnel or payroll systems. The second are matches related to Federal benefit programs to accomplish the following:

- determine eligibility for a Federal benefit,
- determine compliance with benefit program requirements, or
- recover improper payments or delinquent debts under a Federal benefit program.

For more information

To see examples of CMAs, visit our website

For example, let's say the Department of Veterans Affairs (VA) needs to confirm that a person is a member of the military in order to provide that person with access to the GI Bill and other benefits. The VA would need a computer matching agreement in order to access DoD military personnel records to confirm a service member's status.

We use a similar process whenever databases are linked within DoD. For example, if one DoD Component wants to access data in another DoD Component's database, we prepare a Memorandum of Understanding. A computer matching agreement is not necessary because the data is contained within the DoD community.

Accountability

The Federal government, including DoD, is ultimately accountable to the citizens of the United States. We are also accountable to Congress and the Office of Management and Budget (OMB)—two Federal government entities with which DoD maintains reporting relationships. The following segments of this report address specific pieces of legislation or privacy policies that require DoD to regularly report to Congress and OMB.

9/11 Commission Act of 2007

Formally known as *Public Law 110–53, Implementing Recommendations of the 9/11 Commission Act of 2007*, this legislation carries out recommendations made by the people appointed to examine the events of September 11, 2001. Among other things, the 9/11 Commission Act mandated that members of the intelligence community needed to improve their information-sharing practices. Because of the unique and very important nature of information sharing within the intelligence community, the 9/11 Commission Act created a different accountability process.

The Commission's recommendations have the potential to impact an individual's privacy and civil liberties. As a consequence, Section 803 of Public Law 110-53 requires that Federal agencies report periodically, but not less than quarterly, on progress regarding the Commission's recommendations. Section 803 also requires an accounting for DoD activities regarding privacy and civil liberties. Since DoD has had a long-standing privacy program, it was easy for us to adopt and accomplish these new accountability requirements.

For more information

Find our Section 803 reports online

These quarterly reports are designed to advise Congressional committees about:

- information on the number and types of reviews we undertake;
- the type of advice we provide and the response given to our advice;
- the number and nature of the complaints received by DoD for alleged violations; and
- a summary of the disposition of complaints, the reviews and inquiries conducted, and the impact of these activities.

Office of Management & Budget Memorandum 07-16

OMB provides guidance to all Federal agencies about a variety of activities. OMB is the office responsible for directing Federal agencies in implementing the Privacy Act.

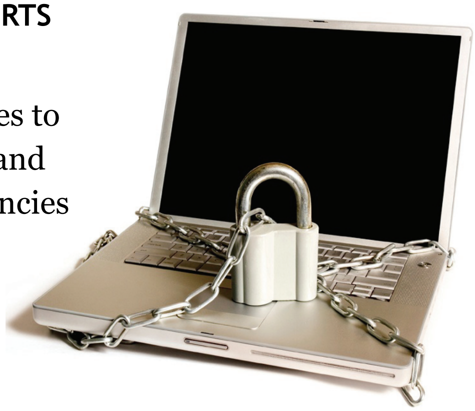
OMB published Memorandum 07-16 "*Safeguarding Against and Responding to the Breach of Personally Identifiable Information*" in 2007. This memo directs Federal agencies to protect PII and guard against breaches. Among other things, the memorandum directs Federal agencies to establish rules and procedures for notifying individuals whose information may have been breached in an incident. Those rules and procedures include a requirement that all breaches be reported to the United States Computer Emergency Readiness Team (US CERT) which is under the direction of the Department of Homeland Security.

Another notable mandate in the memorandum, is that agencies should reduce the use of social security numbers (SSNs). We included a special section later in this report to specifically discuss reduction of SSN use. In that section, we highlight the steps that some DoD Components have taken to successfully reduce the collection and use of SSNs in systems of records. One of our goals in reducing SSN use is to limit the number of individual SSNs that may be compromised in a given breach of PII.

We track breaches of PII weekly. Reports are initiated at the DoD Component level, reported to US CERT within one hour of their occurrence, and then reported up through the Component to us in the Defense Privacy Program. DoD Components send written notifications to impacted individuals if the breach has placed any individual(s) at significant risk of harm.

Reporting breaches from the Components up to the program staff also helps us track breaches over time to understand the causes. By understanding how breaches occur, we can develop targeted training to address and mitigate these threats to the DoD community.

Federal Information Security Management Act Reports



In 2002, Congress passed the Federal Information Security Management Act (FISMA) which requires all Federal agencies to improve the ways in which they secure Federal information and information systems. Each year, DoD and other Federal agencies collectively report to Congress and OMB on our progress.

An annual OMB memorandum provides reporting instructions for Federal agencies which include a section outlining each agency's privacy management program. DPCLO completes the Senior Agency Official for Privacy's portion of the annual FISMA report. The final DoD FISMA report is compiled by the DoD Chief Information Officer (CIO) and includes sections from the CIO and Inspector General.

Collaborative Activities

Protecting privacy is not a one-stop-shop issue. It involves working within DoD across Component privacy programs and with the information technology community, General Counsel, Public Affairs, and others, depending on the issue. We frequently collaborate with other Federal agencies to understand the state of the art (i.e., "what's the latest and greatest in privacy?") and to resolve issues as they arise related to the DoD community.

Several key roles support the DoD Privacy Program at all times (see table on the following page). Each role has one main function—executive, strategic, or operational. The highest privacy leadership role in DoD is the Senior Agency Official for Privacy. The person in this appointed role is ultimately responsible for the executive-level leadership of the DoD Privacy Program.

Component Senior Officials for Privacy

Component Senior Officials for Privacy (CSOPs) are appointed officials who provide high-level visibility and strategic direction for the Component privacy programs. Component Senior Officials for Privacy meet quarterly to discuss and strategize solutions for big picture privacy issues within DoD.

Component Privacy Officers

Each DoD Component has a designated privacy officer. This person has a management role and day-to-day oversight for his or her Component's privacy-related activities. Often, these officers are also responsible for associated duties such as responding to Freedom of Information Act requests or addressing Civil Liberties complaints. Certain DoD Components have representatives on the Defense Privacy Board (DPB). See the following segment for information regarding the requirements for representation.

Defense Privacy Board

The DPB provides a two-way communications forum in which DoD Components receive information from DoD Privacy Program leadership and, simultaneously, provide feedback about challenges experienced in the field.

The Board, which meets monthly, is composed of representatives from specific DoD Components—those whose mission requires them to manage a significant amount of PII or those whose mission involves critical use of PII. The DPB Chair is our Senior Agency Official for Privacy. The Board's Executive Secretary is our Director for Privacy.

Function	Role	Communication Mechanism
Executive	Senior Agency Official for Privacy	Formal reports to Congress and OMB
Strategic	Component Senior Officials for Privacy	CSOP Forum
Operational	Component privacy officers Subject Matter Experts Functional Proponents	Defense Privacy Board Defense Integrity Board

Defense Data Integrity Board

The Defense Data Integrity Board was established to review and approve Computer Matching Agreements. The Board, composed of representatives from the DoD Components, operates virtually, in a collaborative online work environment with the use of electronic signatures. The Board is activated only when approval for a Computer Matching Agreement is required. Representatives on this Board are not necessarily the same as those on the DPB.

Adaptability

The DoD Privacy Program is constantly evolving to meet the demands of new and unique circumstances and emerging technologies. The tragic event of the Fort Hood shooting in November 2009, was one recent situation that pushed us to re-examine how best to protect DoD personnel while simultaneously preserving privacy protections.

An independent review of the incident at Fort Hood resulted in numerous recommendations aimed at monitoring behaviors and actions of members of the DoD community. Among the guidance were recommendations to collect and use information associated with how military members exercise their First and Second Amendment rights outlined in the U.S. Constitution. First Amendment rights include the freedoms of religion, speech, press, assembly, and to petition the Government for a redress of grievances. The Second Amendment provides the right to bear arms.

The DoD Privacy Program played a key role in developing a DoD-wide policy for the possession and registration of firearms on military installations. In these deliberations, we ensured no infringement upon the right to bear arms.

Our program continues to work with installation access entities across DoD. Collaborating helps us to ensure that portable electronic scanning devices are only employed to collect and use PII for authorized purposes, thus ensuring protections for individual privacy across all DoD installations.

Accomplishments

The following section highlights a selection of our program's significant accomplishments in recent years.

Training from the Defense Privacy Program

Training is an important element in any compliance program. Our leadership recognized the need for training opportunities related to DoD Privacy Program requirements. We developed a suite of training courses designed to inform and educate members of our DoD community, including those who work with SORNs, Component privacy officers, and members of the DoD workforce.

We now run several training workshops over the course of the year. Our portfolio of training opportunities includes a variety of topics. While our training program is still nascent, our workshops are garnering very positive feedback and increasing interest. We expect to grow our class sizes and our portfolio over the coming years.

System of Records Notice Workshops

The Privacy Act requires a SORN for each system in which a person's record is retrieved by a unique identifier, e.g., name, SSN, etc. Our personnel work with DoD Components each year to ensure that their SORNs are up-to-date. We manage a total of approximately 1,300 SORNs at any given time. Each SORN is published in the Federal Register, informing the public of the following:

1) which DoD Component and system manager maintains the system of records,
2) what categories of information are maintained in the system of records, and
3) how a person can access any information about himself or herself that may be maintained in the system of records.

The SORN development process can be rather daunting to newcomers and seasoned professionals alike. Completing the process requires attention to detail and ensuring compliance with Federal regulations. To demystify the SORNs process, in 2010, we began conducting a highly successful in-person quarterly training program for personnel who want to learn more. Our training program shows new hires and seasoned DoD personnel how to ensure their Component's SORN(s) are up-to-date and compliant with all Federal requirements. To date, we have held four SORN workshops, successfully training 53 DoD personnel (military, civilian, and contractors) who develop and submit SORNs.

Privacy Act Essentials

In August 2011, we piloted a training series covering the basics of the Privacy Act. The course was designed to supplement training that Components provide to the DoD workforce. The series includes four in-person classes addressing the history of the Privacy Act; Agency requirements and individual rights under the Act; disclosures of PII and associated exceptions under the Act; and Privacy Act exemptions from disclosures. The series targets DoD employees (military, civilian, and contractor).

The first series, held in late summer 2011, was so successful that we hosted a second series within a month. Twenty-seven personnel participated in the two series, generating significant interest in upcoming courses.

Privacy Officer Professionalization Program

In October 2011, we initiated a training program to create a cadre of DoD privacy professionals by providing baseline privacy program implementation knowledge, building a rich culture of privacy across DoD, and developing train-the-trainer skills that will assist privacy officers in disseminating privacy training within their Components. The multi-day, intensive training course was profoundly successful.

By the final day, the inaugural class of 10 Component privacy officers were energized and excited to return to their offices and share with their personnel everything they had learned. This course also piqued interest in additional training courses provided by us and our counterparts in the DoD Civil Liberties Program.

Looking Forward

The DoD Privacy Program is growing its suite of training opportunities with a goal of eventually offering workshops on breach management, Privacy Act exemptions, and contract requirements. Our vision is that by increasing awareness and understanding via training, DoD will be better equipped to proactively protect the privacy of all DoD personnel.

Raising Awareness

Protecting PII

Beginning in mid-2011, we launched an awareness campaign focused on enhancing protection of PII. Our initiative was designed to remind DoD personnel to think about privacy protection within their daily work.

The first big step in the initiative involved collaborating with DoD InfoNet services. InfoNet provides important information to DoD personnel throughout facilities within the National Capital Region. InfoNet informational kiosks display brief messages informing personnel about everything from upcoming events to reminders about operational security.

We decided to capitalize on this resource by completing four informational campaigns via InfoNet, each of which related to the protection of PII. The various campaigns garnered positive attention and feedback. Content from the InfoNet campaigns continues to be adapted to other purposes, including tools to aid Component privacy officers in their daily work.

Cell Phone Scam Notification

Late in 2009, law enforcement personnel notified us that an identity theft ring had recently been disrupted. While this theft ring did not specifically target military personnel, many people affiliated with DoD were victimized in their scam, including some high level officers and retirees. The scam involved fraudulently opening cellular phone accounts in the names of the victims, and then charging the accounts with bills from a pay-per-minute phone line tied to the criminals' bank accounts.

As the fraud was discovered, the wireless providers shut down the accounts and did not hold the victims accountable for the charges. Since the victims were not being held accountable, the cellular companies did not plan to notify the victims.

Although the harm from this particular scam was likely minimal, the DoD Privacy Program determined that we had a duty to inform the affected DoD personnel. The original scam included SSNs and it was our belief that the potential for further harm from other scams warranted a notification effort.

In conjunction with investigators and the Defense Manpower Data Center (DMDC), a list of DoD affiliated victims was compiled and letters were mailed to nearly 500 military, civilian, and contractor personnel, alerting them of the risk to their identity. Notified individuals were encouraged to place alerts on their credit reports, provided with identity theft mitigation pamphlets, and given contact numbers to receive more information. In some cases, victims with additional knowledge related to this scam, or potentially related schemes, were put in touch with investigators to aid in the investigation.

Looking Forward

Awareness of situations that may compromise the protection of individual privacy is an important part of protecting the overall privacy of individuals. Whenever situations arise that may impact DoD personnel (military, contractor, or civilian), we and DoD

DoD Privacy Program Issuance Review Process

The privacy program actively participates in the DoD issuance process. We receive, review, and comment on DoD issuances with respect to privacy and/or civil liberties matters.

In 2011, the DoD Privacy Program recognized a need to expand the reach of its review process. Beginning in the spring of 2011, we began reviewing all DoD-wide issuances. Every issuance released by DoD is now reviewed by our staff; we reviewed an average of forty issuances each month throughout 2011.

Component privacy personnel will work together to bring that information to the attention of impacted personnel.

We continue to raise awareness through various programs implemented throughout the Department over the course of each year. We will continue to develop new and innovative ways to bring privacy information to the DoD workforce. Our InfoNet campaigns will continue into 2012. We also anticipate developing materials for use by and within DoD Components, hosting events, and continuing to improve the content on our website.

Policy and Program Oversight

Policy Review

The Department of Defense, like many Federal agencies, periodically releases policy Directives, Memoranda, Instructions, and Manuals, which are collectively referred to as issuances. These issuances provide guidance to DoD personnel in various ways, depending on the type of issuance (directive, instruction, etc.). Some issuances outline program roles and responsibilities (e.g., those for the DoD Privacy Program). Other issuances, such as manuals or regulations, provide "how to" guidance which is used to implement a specific program.

Privacy Issuance Revisions

Through most of 2011, the DoD Privacy Program worked to reissue our Directive (*DoDD 5400.11 "DoD Privacy Program"*) and revise our current Regulation into a Manual (*DoD 5400.11-R "Department of Defense Privacy Program"*).

We completely revised our Manual to ensure that our program continues to meet all Federal laws and rules which govern the safeguarding and handling of PII. The Manual was rewritten with an increased focus on privacy principles and to provide guidance for keeping up with technology and its future evolution. We expect final approval of the Directive and Manual in early 2012.

For more information

About DoD issuances, click here

Looking Forward

Sound policies lead to stable and effective programs. We will always look for opportunities to improve and enhance DoD policies regarding privacy.

DoD Components—Making an Impact

DoD Components provide the daily on-the-ground support activities that implement the DoD Privacy Program. Privacy officers and their teams work tirelessly to protect the privacy of individuals while furthering the DoD mission. These dedicated teams often develop innovations that benefit their Component and, eventually, benefit the entire privacy program by becoming best practices. The pages that follow contain just a few of this year's Component accomplishments.

Defense Media Activity—Identity Protection

The Defense Media Activity (DMA) was using a system to identify and track photographers working for DMA. The system included more PII than was necessary, posing a risk to the photographers, i.e., possible identity theft. We worked with DMA to change the way their system tracked and identified photographers to improve protection for individuals.

What DMA did about it

DMA created a new identification schema to enroll new photographers. The system was adjusted to identify photographers by assigning a random identification (ID) number. The new ID number is now issued to every new photographer who enrolls in any DMA system. The process also includes steps for updating existing photographer information in the DMA database.

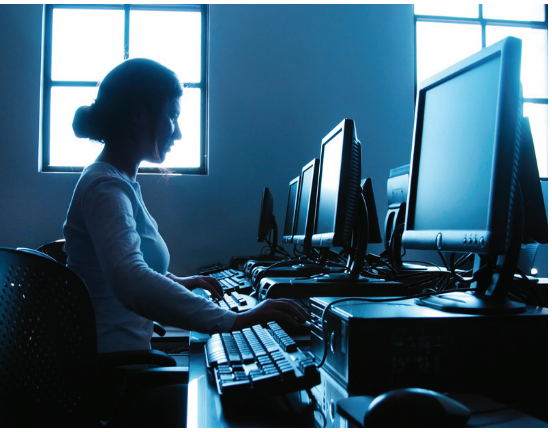
Impact

The new identification system significantly improved protection of PII without disrupting the DMA mission.

Defense Manpower Data Center—IT Application Flaws

A military member entered a DMDC web application, but rather than receiving his own record, he saw another military member's record. The military member who saw the wrong record immediately reported the breach to DMDC.

DMDC contacted the service member whose record was exposed. The development team then worked extensively with both Service members to understand and record the exact chain of events leading to the breach.



DMDC discovered a "threading issue" in a computer program which arose when developers added new code to old code without verifying that the coding sets worked together. This was such an unusual event and the chance of the wrong record being pulled was one in millions, but it was a good lesson for all future development.

What DMDC did about it

The developer team involved in finding the problem provided a training session for DMDC developers (approx. 100) on what happened, how they found it, and how to complete future development testing and review.

Impact

The training session opened the door to a better dialog among Information Technology (IT) personnel and the privacy policy staff. Their interactive session generated a great exchange of questions, ideas, and solutions. The dialog also made developers much more aware of PII issues in the development of new applications. While metrics are difficult to measure, DMDC has a strong record of very few breaches, especially for the number of people handling PII and the development of so many applications that provide PII data.

Defense Manpower Data Center—Protecting PII

DMDC is the largest holder of PII data in DoD. As such, the agency strives to create a culture of privacy and "*Make DMDC #1 in the Protection of PII*".

What DMDC did about it

One DMDC initiative supporting this goal was to organize their own Privacy Board. The DMDC Privacy Board is composed of representatives from multiple divisions and from each contracted company working for DMDC. This provided different points of view on privacy issues. It also allowed the Board to write "how to" documents that worked best for the users because the technical staff and the users all had input.

The Board members were also tasked with taking any challenges they discussed back to their respective division or company so that at subsequent meetings, the representatives could present proposals for solutions and innovations to address the issues.

Impact

Innovations and ideas shared among the Board's technical and policy members have resulted in on-going collaboration which continues to benefit the privacy program.

National Geospatial-Intelligence Agency—Improving Contracts

The National Geospatial-Intelligence Agency (NGA) Privacy Program Office was faced with the challenge of enforcing privacy training requirements, SORN and Privacy Impact Assessment documentation compliance, and breach accountability, specifically related to the contractor workforce. Recent privacy awareness training statistics showed only 44% of NGA contractors had completed the mandatory privacy awareness training. Because no incentives existed to motivate contractors to adhere to these requirements, NGA had to find a way to incentivize contractors to comply with existing Federal statutes and requirements as well as agency policies.

What NGA did about it

NGA drafted specific privacy-related language to be incorporated in acquisition contracts. The areas covered by the language include:

- a requirement to complete mandatory annual privacy awareness training,
- ensuring that SORNs and Privacy Impact Assessments are published when a contractor is operating systems of records on behalf of NGA, and
- actions related to mitigating breaches committed by contractors.

Contractor non-compliance with any or all of these requirements may result in a negative impact on the contractor's award fee and/or past performance evaluations.

Impact

Since implementing this standard contract language and making continued efforts to raise awareness, privacy breaches by contractors were non-existent from March through September of 2011. This may be an indicator of successfully increasing privacy awareness and enhancing proactive efforts to securely maintain and handle PII. Other indicators of success include the cooperation of NGA's Acquisitions Directorate in standardizing this language in each contract in order to stress contractor responsibilities at NGA.

National Guard Bureau—Breach Management

National Guard Bureau (NGB) leadership was concerned that 1) breaches were not being reported in a timely manner, 2) staff were unaware of the reporting requirements, and 3) NGB was not fully prepared to deal with a significant breach of PII.

What NGB did about it

In the fall of 2010, NGB issued a PII Incident Response Handling policy. The policy established a quarterly PII Core Management Group whose members serve as part of the PII Incident Response Team when a significant PII breach occurs.

The PII Core Management Group is led by the Privacy Office. The group includes members from the Chief Counsel, Public Affairs, Legislative Liaison, Contracting, Security, Personnel, Intelligence, Communications, and others as deemed appropriate.

Impact

After training members of the PII Core Management Group, NGB received several ideas to improve privacy protection. They have vastly improved the awareness of PII protection and implemented ideas from the group such as removal of SSNs on retirement certificates, and training and education to other staff members (by members of the group). NGB is working on several other ideas which include reporting quarterly metrics on PII breaches, screen savers emphasizing PII awareness/protection, a video message on the importance of privacy protection, and posters to be placed in work centers to emphasize PII awareness/protection. The NGB cross-office group develops and collaboratively implements innovative ideas, something that their small privacy office would otherwise not have the resources to do.

NGB leadership has been impressed at the ability of their group to form as an Incident Response Team to prepare recommendations for leadership to respond to PII breaches, thereby reducing the workload of all incident response residing with the privacy office.

These narratives are just a few examples of the work being conducted across DoD to protect privacy. The next section highlights a particular aspect of privacy protection—SSN use reduction.

Special Interest—Social Security Number Protection

Every legal resident in the United States is issued an SSN. Over the years, the SSN has become a ubiquitous identifier, linked to personnel files, financial accounts, medical records, and more. Our pervasive use has made the SSN a vulnerability for millions of Americans. Unnecessary use of the SSN leads to a significant risk of exposure to identity theft. Recognizing this inherent danger, DoD began an expansive review of all uses of the SSN in systems, with a mandate to remove the number wherever possible.

For more information

See DoD's
SSN use reduction plan

As DoD policies evolve, we expect to see a significant reduction in the use of SSNs on forms and in databases throughout DoD. Components have already taken steps to reduce SSN use—the following are just a few examples of our successes to date.

Defense Privacy Program—SSN Redaction from the Congressional Record

The lists of military officers nominated for promotion are reported to the US Senate for confirmation. Because confirming military officers is part of the Senate's official duties, lists of all confirmed officers are published in the Congressional Record. These lists, for a time, included the officers' full SSNs. Beginning in 1996, DoD only provided the last four digits of the SSN.

What we did about it

While the practice of publishing officers' full SSNs was discontinued more than a decade ago, older copies of the Congressional Record still contained the full SSNs of previously confirmed officers. The ready availability of these historical records through searchable internet repositories and bound volume holdings made these listings vulnerable to identity thieves.

We requested that the Government Printing Office redact all SSNs, in whole or part, published in the Congressional Record. After ensuring that new printings of the record would have SSNs redacted, we contacted online repositories such as The Library of Congress, LexisNexis, and Westlaw and asked them to redact the electronic copies which they offered through their online services.

Impact

All known and discovered sources for the Congressional Record online were contacted, and all sources took action to eliminate SSNs from their holdings. Redacting this information from easily-accessed public records has helped protect thousands of active duty and retired personnel from potential dangers resulting from this unnecessary public dissemination of personal information.

National Geospatial-Intelligence Agency—New Instruction

Like many government agencies, NGA's Privacy Program Office was challenged with reducing the unnecessary collection, use, and dissemination of SSNs. NGA complies with Federal statutes and regulations with regard to protecting PII and SSNs; however, they recognized that their requirement for employees to input their full SSN on certain NGA forms and templates, may not have been a privacy "best practice."

What NGA did about it

In keeping with their mission to mitigate and prevent privacy breaches, NGA took steps to drastically reduce the collection and exposure of SSNs on all NGA forms, Privacy Act systems of records, and other documents. In accordance with OMB and DoD guidance, NGA took the additional step of reducing the collection, use, and dissemination of PII and SSNs by updating an Instruction for all agency employees to only require the last four digits of the SSN or an alternate identifier, such as employee ID number.

NGA Instruction 1401.1, *Elimination of Unnecessary Personally Identifiable Information (PII) and Social Security Numbers (SSNs)* instructs all employees to only provide the last four digits of the SSN on all NGA forms even in cases where the form requests the entire number. Further guidance suggests that employees use their employee ID numbers wherever possible.

The NGA Privacy Program Office, at the request of the NGA CIO, also compiled a comprehensive list of all agency-wide forms requiring the SSN and forms that are internal to each directorate. They used this list to approximate the number of potential incidents that could arise from the circulation of these forms and take actions to protect the PII contained in them. They drafted and disseminated a "Privacy Best Practices" document to key NGA offices in an attempt to enhance the protection of SSNs and PII through a change in internal processes.

NGA realized the need to disseminate the new guidance quickly and in as broad a forum as possible. To accomplish this, they sent NI 1401.1 to the Office of International Policy (OIP) for expedited publishing and posting to the OIP website. Furthermore, the NGA Chief Operations Officer posted an agency-wide notice on their main Internet and Intranet website, informing NGA employees of the policy update. Lastly, they also published the notice in NGA's weekly newsletter, *In the Know*, to complete their privacy program office's aggressive communications campaign.

Impact

NGA employee feedback was positive. NGA forms now have a lower yield of SSNs being collected, used, and disseminated throughout the agency. Supervisors and employees continue to contact the NGA Privacy Program Office in an effort to improve internal processes and reduce the collection of SSNs. Continued success will be predicated upon more robust metrics indicating the same reduction in SSN use, and ideally showing an acceleration of the trend.

Department of the Navy—IT System Updates

Like other DoD Components, the Department of the Navy is working toward reducing SSN use. Reducing the number of Department of the Navy IT systems that collect SSNs was difficult due to a number of factors including:

- the cost of system reprogramming,
- overcoming a culture and history of continued SSN use,
- interfaces with IT systems outside the Navy that rely on the SSN,
- the absence of authority to use the DoD ID number as a substitute identifier, and
- administrative workload required to conduct reviews and justifications.

Regardless, the Navy was committed to finding a solution to reduce the collection and use of SSNs in Navy systems.

What Navy did about it

They applied lessons learned from their first SSN reduction efforts involving official Navy forms. First, they implemented a data call with step by step instructions to complete IT system reviews. In that data call, they included a justification memo—a statement of the need for continuing to collect the SSN. The Navy then implemented programmatic changes to the DoD Information Technology Portfolio Repository.

These changes encouraged Navy program managers to complete required reviews for all systems that collect the SSN. Each system that would continue to use the SSN posted a signed justification memo (electronic) to the DoD Information Technology Portfolio Repository. In tandem with all of these changes, the Navy increased awareness through email and a Department of the Navy IT magazine article.

Impact

The Navy completed reviews verifying that they reduced the total number of systems collecting SSN. In the process, they increased their accuracy related to the collection of PII and SSNs, and reduced SSN collection in IT systems by 25% across the organization.

What's on the horizon?

Over the last fifty years, technology has evolved at an exponential pace, changing the ways in which we communicate and altering how we conduct our daily business. With the advent of social media and expansion of portable technology, we must continuously reexamine our understanding of privacy, its boundaries, and best approaches to protecting it. We foresee DoD focusing its attention and resources on the following issues and content areas over the next several years.

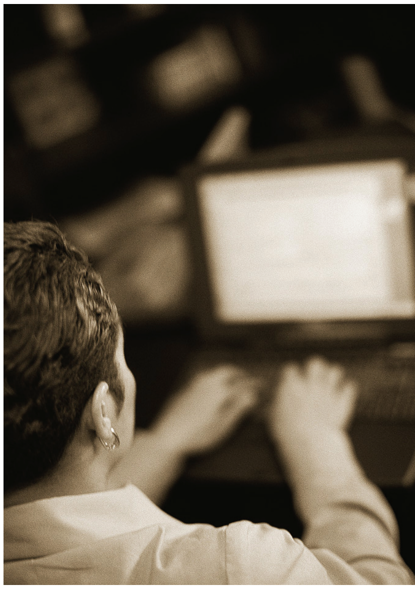
Reducing SSN Use

As DoD continues to pursue a path towards reducing its dependence on the SSN, many important milestones lie in our future. First and foremost, the Department is progressing in its effort to replace the SSN on ID cards. The SSN is slowly being replaced with a new DoD ID number. While this process will take several years to complete, the proliferation of this new identifier will better enable our internal systems and processes to replace the SSN as well.

In addition, a temporary plan is in place to review all systems that are currently collecting the SSN. This temporary plan is slated to become a permanent requirement once the associated draft Instruction is reviewed and signed. The plan mandates that all DoD systems which collect the SSN will be reviewed over the next 2 years to ensure that the collection of the SSN is relevant, necessary, and authorized. This review process is already under way. Reports on the first reviews are due in the first quarter of 2012.

Telework

President Obama signed *Public Law 111-292, Telework Enhancement Act of 2010* in December 2010. The Act intends to make the Federal workforce more flexible, while still requiring adequate protections for systems and information used by teleworkers.



Being able to work remotely can allow the Federal workforce to be productive under conditions that would otherwise result in work stoppage. It can provide resource savings in some situations. Telework is also environmentally friendly, and can even improve employee recruitment and retention. For all its benefits, however, telework presents us with some challenges.

Remote work stations represent opportunities for privacy breaches. Improper use of records, for example, or working on sensitive files on non-government issued equipment are both potential problems. Likewise, downloading or transferring sensitive information onto personal computers represents a vulnerability. If those personal pieces of equipment are compromised in any way—hacked, stolen, etc.—the sensitive information on that equipment may also be compromised.

In a 'work anywhere' world, DoD must continue to be vigilant about protecting data, information devices, and systems that could adversely impact individuals' privacy.

Cloud Computing

Cloud computing offers organizations some flexibility and cost savings that traditional, government-purchased and government-maintained servers did not. The "cloud" provides software and data storage, among other services, over the Internet from and to 3rd-party-managed environments.

In a work environment, the software and data needed to do your job are accessed via a "remote-in" or "thin client" that allows you to connect to your files via the Internet. The thin client essentially generates a copy of your desktop on a remote device (laptop, PDA, etc.). Any work conducted on that remote device is saved to the cloud or to your work computer. In this way, cloud computing has evolved into a very viable resource for Federal computing needs.

One of the most frequently asked questions with regard to cloud computing is "*Is it secure*?" On the surface, the cloud is no more or less secure than current DoD systems. Both are vulnerable to cyber attack. Any system owned and operated by DoD is subject to high security standards regardless of whether the system is cloud-based or running on a local server. Any vendor operating a system on behalf of DoD must be required to meet the same high information security standards DoD meets in its own systems. So, we foresee the conversation transitioning from "*How secure is the cloud?*" to "*How can we best use cloud computing to support the DoD mission*?" Cloud computing is cost-effective, safe, and provides opportunities for continuity of operations via telework.

The evolution of other technologies in the workplace—e.g., the ubiquity of laptops—brought about useful changes to the way we do business. We anticipate cloud computing will revolutionize our workforce as well. We look forward to ensuring the same quality of privacy protections within the cloud that we strive for with respect to protecting records in all other media.

Information Sharing

Information sharing is currently a hot topic. From national security operations to social media, everyone is looking for "the sweet spot"—sharing enough without sharing too much. In social media, sharing too much information can lead to embarrassment. In the pursuit of national security operations, sharing too much information can be illegal, but sharing too little can adversely impact our ability to deal with a threat. In two fields where the state of the art is constantly changing, it can be challenging to stay on top of issues and best practices.

Social Media

With the advent of social media, information sharing in our personal lives has grown exponentially. What does this have to do with the DoD mission? Sharing personal information or inappropriate information can create problems related to individual privacy or operational security, e.g., posting messages about deployment dates. As such, DoD is committed to staying abreast of the social media evolution and its impact on privacy and the DoD mission.

Find us on Facebook

The Department encourages units, offices, and other DoD entities to take advantage of the social media community of products. The DoD Social Media Hub provides information about DoD social media use and policies.

9/11 Commission Recommendations

Since September 11, 2001, information sharing has become an increasingly important topic of conversation within the defense and intelligence communities. These two communities bear a responsibility to protect the U.S. and its people from threats, while at the same time maintaining appropriate boundaries for individuals' privacy rights under the law. The 9/11 Commission recommended, among other things, that the defense and intelligence communities increase their information sharing in order to thwart future terrorist attacks. These communities are working toward that goal by creating an environment where information is shared as rapidly as possible, while simultaneously being mindful to maintain privacy protections.

For more information

On the 9/11 Commission Recommendations, view the report online

Our existing legislation provides consistently strong guidance that can be applied to evolutions in communication. We remain mindful and vigilant when it comes to putting that legislation into practice.

DEFINITIONS

Biometric data – information about an individual derived from their biology, e.g., finger prints, retina scans, voice signature, facial scans, etc.

Component – a Military Service, Agency, or Field Activity within DoD.

Computer Matching Agreement - a written accord that establishes the conditions, safeguards, and procedures under which a Federal organization agrees to disclose data where there is a computerized comparison of two or more automated system of records.

Privacy Act Statement - a document that explains why a Federal agency is collecting personal information, the purpose of the collection, and what could happen if you choose not to provide the requested information. The statements are required when the collected personal information (name, date of birth, SSN, etc.) will be entered into a Federal system of records. This applies to all collection methods, i.e., forms, personal or telephonic interview, etc.

Privacy Impact Assessment - an analysis of the collection, storage, protection, sharing, and management of PII in electronic information systems.

Personally Identifiable Information - any details about an individual that can be used to distinguish or trace a person's identity. A few examples include SSN, date of birth, address, biometric data, or financial information.

System of Records - a group of records under the control of a Federal government agency from which personal information about an individual is retrieved by the name of the individual, or by an identifying number, symbol, or other unique identifier.

System of Records Notice - a description of any Privacy Act system of records. SORNs generally describe the 'who, what, where, and why' of a system and describe the processes for individuals to access or contest the information being held on them in that system. SORNs are required to be published in the Federal Register for a period of public comment before the system data collection (paper-based or electronic) is started.

Abbreviations and Acronyms

CIO	Chief Information Officer
CSOP	Component Senior Official for Privacy
DMA	Defense Media Activity
DMDC	Defense Manpower Data Center
DoD	Department of Defense
DPCLO	Defense Privacy and Civil Liberties Office
ID	Identification
IT	Information Technology
MOU	Memorandum of Understanding
NGA	National Geospatial-Intelligence Agency
NGB	National Guard Bureau
OIP	Office of International Policy
OMB	Office of Management & Budget
PII	Personally Identifiable Information
SORN	System of Records Notice
SSN	Social Security Number
US CERT	United States Computer Emergency Readiness Team

Web links used within this document

9/11 Commission Report	http://www.9-11commission.gov/report/index.htm
Computer Matching Agreements	http://dpclo.defense.gov/privacy/Res_And_Pub/reports.html
DoD Directives (Issuances)	http://www.dtic.mil/whs/directives/
Defense Privacy and Civil Liberties Office (DoD Privacy Program Headquarters)	http://dpclo.defense.gov/
DoD SSN Use Reduction Plan	http://www.dodig.mil/fo/privacy/PDFs/pr080328ssn_28Mar08_DrChu.pdf
DoD Social Media Hub	http://www.defense.gov/socialmedia/
DoD Systems of Records Notices	http://dpclo.defense.gov/privacy/SORNs/SORNs.html
Public Law 110-53, Section 803 Reports	http://dpclo.defense.gov/privacy/Res_And_Pub/reports.html

2011 Annual Report

Defense Privacy Program

Defense Privacy and Civil Liberties Office

http://dpclo.defense.gov/Privacy