# Privacy Horizons

Presented by

**Samuel P. Jenkins,**

**Director, Defense Privacy Office**

April 28, 2009

**Sponsored by: Booz Allen Hamilton**

# Defense Privacy Office
## Presentation Topics

- ✓ GAO Reports
- ✓ NIST Recommendations
- ✓ Compliance and Reporting
- ✓ Program Review
- ✓ Transparency
- ✓ Current DPO Issues and Privacy Concerns
  - Breaches
  - Social Security Number Reduction
  - Biometrics and Deoxyribonucleic Acid (DNA)
  - Access Controls for Systems

# GAO Reports

# Defense Privacy Office
## GAO Reports

*GAO-08-603*

***Privacy: Agencies Should Ensure That Designated Senior Officials Have Oversight of Key Functions***

***http://www.gao.gov/new.items/d08603.pdf***

*May 2008*

# Defense Privacy Office
## GAO Reports

***GAO-08-603 "Privacy: Agencies Should Ensure That Designated Senior Officials Have Oversight of Key Functions," May 2008***

**Purpose:**

1. To describe laws and guidance that set requirements for senior agency official for privacy (SAOP) within federal agencies
2. To describe the organizational structures used by agencies to address privacy requirements and assess whether SAOPs have oversight over key functions.

**Methodology:**

GAO analyzed the laws, related guidance, policies and procedures relating to key privacy functions at 12 agencies

| | | |
|---|---|---|
| Commerce | Justice | Transportation |
| Defense | Labor | Veterans Affairs |
| Health and Human Services | State | Social Security Administration |
| Homeland Security | Treasury | U.S. Agency for International Development |

# Defense Privacy Office
## GAO Reports

***GAO-08-603 "Privacy: Agencies Should Ensure That Designated Senior Officials Have Oversight of Key Functions," May 2008***

**Findings:**

There are six (6) broad categories of SAOP responsibilities as defined by federal laws and guidance

- Conducting PIAs
- Complying with the Privacy Act
- Reviewing and evaluating the privacy implications of agency policies, regulations and initiatives
- Producing reports on the status of privacy protections
- Ensuring that redress procedures are in place
- Ensuring that employees and contractors receive appropriate training

Agencies have varying organizational structures to address privacy responsibilities. Evolving requirements in law and guidance have resulted in fragmented assignment of privacy functions across organizational units.

Not all agencies have given their designated SAOP full oversight over all privacy related functions. This may lead to ineffective SAOPs.

# Defense Privacy Office
## GAO Reports

***GAO-08-603 "Privacy: Agencies Should Ensure That Designated Senior Officials Have Oversight of Key Functions," May 2008***

**Recommendation:**
In order to ensure SAOPs function effectively as central focal points for privacy management, the Attorney General and the Secretaries of Commerce, ***Defense***, Health and Human Services, Labor and Treasury should take steps to ensure that their SAOPs have oversight over all key privacy functions.

*Note: DoD provided written comments that did not state whether it agreed or disagreed with the GAO recommendation, however, the agency stated that its privacy management structures were adequate.*

# Defense Privacy Office
## GAO Reports

*GAO-08-536*

***Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information***

***http://www.gao.gov/new.items/d08536.pdf***

*May 2008*

# Defense Privacy Office
## GAO Reports

***GAO-08-536 "Alternatives Exist for Enhancing Protection of Personally Identifiable Information," May 2008***

**Methodology:**

GAO analyzed privacy laws and guidance (Privacy Act, E-Gov Act, Paperwork Reduction Act and OMB guidance), compared them with the Fair Information Practices, and obtained perspectives from federal agencies and an expert forum.

- They may not consistently protect personally identifiable information (PII) in all circumstances of its collection and use throughout the federal government and may not fully adhere to key privacy principles.

- Based on discussions with privacy experts, agency officials, and analysis of laws and related guidance, the GAO identified three major areas.

# Defense Privacy Office
## GAO Reports

***GAO-08-536 "Alternatives Exist for Enhancing Protection of Personally Identifiable Information," May 2008***

***1. Applying privacy protections consistently to all federal collection and use of personal information*.**

•The Privacy Act's definition of a "system of records" (any grouping of records containing personal information retrieved by individual identifier), which sets the scope of the Act's protections, does not always apply whenever personal information is obtained and processed by federal agencies.

•If agencies do not retrieve personal information by identifier, the Act's protections do not apply.

# Defense Privacy Office
## GAO Reports

***GAO-08-536 "Alternatives Exist for Enhancing Protection of Personally Identifiable Information," May 2008***

***2. Ensuring that collection and use of personally identifiable information is limited to a stated purpose.***

•According to the purpose specification, collection limitation, and use limitation principles, the collection of personal information should be limited, and its use should be limited to a specified purpose.

•Current laws and guidance impose only modest requirements for describing the purposes for collecting and using personal information and limiting how that information is collected and used.

•Agencies are not required to be specific in formulating purpose descriptions in their public notices.

# Defense Privacy Office
## GAO Reports

***GAO-08-536 "Alternatives Exist for Enhancing Protection of Personally Identifiable Information," May 2008***

***3. Establishing effective mechanisms for informing the public about privacy protections*.**

•According to the openness principle, the public should be informed about privacy polices and practices, and the accountability principle calls for those who control the collection or use of personal information to be held accountable for taking steps to ensure privacy protection.

•Public notices are a primary means of establishing accountability for privacy protections and giving individuals a measure of control over the use of their personal information.

•Yet concerns have been raised that Privacy Act notices may not serve this function well.

# Defense Privacy Office
## GAO Reports

***GAO-08-536 "Alternatives Exist for Enhancing Protection of Personally Identifiable Information," May 2008***

***Recommendations:***

Some of these issues—particularly those dealing with limitations on collection and use as well as mechanisms for informing the public—could be addressed by OMB through revisions or supplements to guidance.

- Unilateral actions by OMB would not have the benefit of public deliberations regarding how best to achieve an appropriate balance between the government's need to collect, process and share PII

and;

- The rights of individuals to know about such collections and be assured that they are only for limited purposes and uses.

# Defense Privacy Office
## GAO Reports

***GAO-08-536 "Alternatives Exist for Enhancing Protection of Personally Identifiable Information," May 2008***

**Recommendations (cont):**

A better approach is to amend applicable laws, such as the Privacy Act and the E-Government Act:

- Revise scope of the laws to cover all PII collected, used, and maintained by the federal government
- Set requirements to ensure that the collection and use of PII is limited to a stated purpose
- Establish additional mechanisms for informing the public about privacy protections by revising requirements for the structure and publication of public notices

# Defense Privacy Office

## Fair Information Practices

***GAO-08-536 report "Alternatives Exist for Enhancing Protection of Personally Identifiable Information" May 2008 provides a representation of Fair Information Practices.***

| The Fair Information Practices<br>*Source: Organization for Economic Cooperation and Development.* | |
|---|---|
| **Principle** | **Description** |
| **Collection limitation** | The collection of personal information should be limited, should be obtained by lawful and fair means, and, where appropriate, with the knowledge or consent of the individual. |
| **Data quality** | Personal information should be relevant to the purpose for which it is collected, and should be accurate, complete, and current as needed for that purpose. |
| **Purpose specification** | The purposes for the collection of personal information should be disclosed before collection and upon any change to that purpose, and its use should be limited to those purposes and compatible purposes. |
| **Use limitation** | Personal information should not be disclosed or otherwise used for other than a specified purpose without consent of the individual or legal authority. |

# Defense Privacy Office

## Fair Information Practices (FIPS)

***GAO-08-536 report "Alternatives Exist for Enhancing Protection of Personally Identifiable Information" May 2008 provides a representation of Fair Information Practices.***

| **The Fair Information Practices**<br>*Source: Organization for Economic Cooperation and Development.* | |
|---|---|
| **Principle** | **Description** |
| **Security safeguards** | Personal information should be protected with reasonable security safeguards against risks such as loss or unauthorized access, destruction, use, modification, or disclosure. |
| **Openness** | The public should be informed about privacy policies and practices, and individuals should have ready means of learning about the use of personal information. |
| **Individual participation** | Individuals should have the following rights: to know about the collection of personal information, to access that information, to request correction, and to challenge the denial of those rights. |
| **Accountability** | Individuals controlling the collection or use of personal information should be accountable for taking steps to ensure the implementation of these principles. |

# Defense Privacy Office

**GAO-08-536 "Alternatives Exist for Enhancing Protection of Personally Identifiable Information," May 2008**

## Key Memoranda for Privacy

| Date | Report | Title | Content |
|---|---|---|---|
| 5/22/2006 | M-06-15 | Safeguarding Personally Identifiable Information | Requires the Senior Official for Privacy at each agency to conduct a review of agency policies and processes, and take corrective action as appropriate, to ensure adequate safeguards to prevent the intentional or negligent misuse of, or unauthorized access to, personally identifiable information. |
| 6/23/2006 | M-06-16 | Protection of Sensitive Agency Information | CIO/NII responsibility. |
| 7/12/2006 | M-06-19 | Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments | Privacy responsibility required policy on reporting PII incidences to the United States-Computer Emergency response Team (US-CERT) within 1 hour of discovery of the incident. Requirement incorporated in DoD 5400.11-R, DoD Privacy Program |

# Defense Privacy Office

**GAO-08-536 "Alternatives Exist for Enhancing Protection of Personally Identifiable Information," May 2008**

## Key Memoranda for Privacy (continued)

| Date | Report | Title | Content |
|---|---|---|---|
| 5/22/2007 | M-07-16 | Safeguarding against and Responding to the Breach of Personally Identifiable Information | Requires agencies to develop a policy for handling breaches of personally identifiable information as well as policies concerning the responsibilities of individuals authorized to access such information. |
| 01/18/2008 | M-08-09 | New FISMA Privacy Reporting Requirements | 2008 privacy reporting requirements. |
| 7/14/2008 | M-08-21 | FY 2008 Reporting Instructions for FISMA and Agency Privacy Management | Instructions for reflecting the overall status of agency's Information Security and Privacy Program |

# Defense Privacy Office

## National Institute of Standards and Technology (NIST) Recommendations

# Defense Privacy Office

## NIST released Special Publication 800-122 (Draft) *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*

This document is intended to assist Federal agencies in protecting the confidentiality of PII

- Provides practical, context-based guidance for identifying PII and determining what level of protection is appropriate for each instance of PII
- Suggests safeguards that may offer appropriate levels of protection for PII
- Provides recommendations for developing response plans for breaches involving PII

# Defense Privacy Office

**NIST Special Publication 800-122 (Draft)** ***Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)***
(continued)

- Outlines factors for determining the PII confidentiality impact level to determine if additional protections should be implemented

- PII confidentiality impact level (low, moderate, or high) indicates the potential harm that could result to individuals and/or the organization if the PII were inappropriately accessed, used, or disclosed

# Defense Privacy Office

## From the Executive Summary:

Breaches of personally identifiable information (PII) has increased dramatically over the past few years and have resulted in a loss of millions of records. Breaches of PII are hazardous to both individuals and organizations.

Individual harm may include identity theft, embarrassment or blackmail. Organizational harms may include a loss of public trust, legal liability or high costs to handle the breach.

**NIST Draft Guide to Protecting the Confidentiality of (PII) (1/09)**

# Defense Privacy Office

## The NIST Guide states that:

"To effectively protect PII, organizations should implement the following recommendations:

**IDENTIFY** all PII residing in their environment. PII Includes (but not limited to):

**Name** (full name, maiden name, mother's maiden name, or alias)

**Personal identifying numbers** (SSN; passport, drivers license Taxpayer ID, financial account or credit card numbers)

**Address information** (Street or email address)

**Personal characteristics** (Photo image, fingerprints, handwriting, or other biometric image or template data (retina scans, voice signatures, facial geometry)

# Defense Privacy Office

Treatment of PII is distinct from other types of data because it needs to be not only *protected*, but also *collected, maintained, and disseminated* in accordance with Federal law.

| **Fair Information Practices or Privacy Principles**<br>*These are based on the common elements or privacy principles of several international reports and guidelines.* | |
|---|---|
| **Notice/Awareness** | There must be no personal data record keeping systems whose very existence is kept secret. |
| **Choice/Consent** | There must be a way for an individual to find out what information is in their file and how it is being used. |
| **Access/Participation** | There must be a way for an individual to correct information in his or her record. |
| **Integrity/Security** | Any organization creating, maintaining, using or dissemination personally identifiable information must ensure the reliability of the data for its intended use and must take precautions to prevent misuse. |
| **Enforcement/Redress** | There must be a way for an individual to prevent personal information obtained for one purpose from being used for another purpose without his or her consent. |

# Defense Privacy Office

## Security Objectives

**CONFIDENTIALITY**

"Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…"

**INTEGRITY**

"Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…" A loss of *integrity* is the unauthorized modification or destruction of information.

**AVAILABILITY**

"Ensuring timely and reliable access to and use of information…" A loss of *availability* is the disruption of access to or use of information or an information system.

# Defense Privacy Office

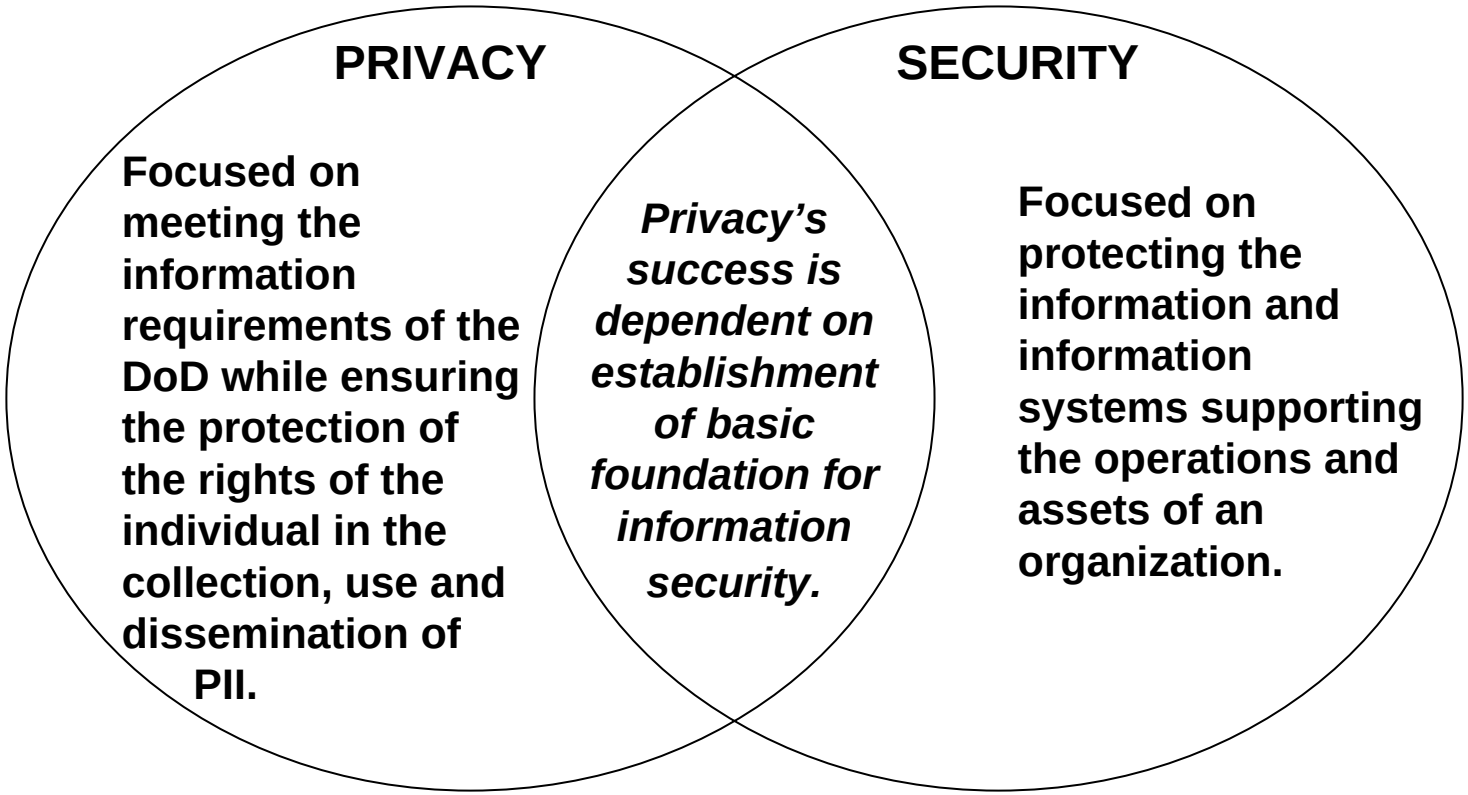
## NIST recommends and encourages close coordination with STAKEHOLDERS to include:

- Privacy Officers
- Chief Information Officers
- Contractors
- Executive Leadership
- Front Line Staff
- Information Security Officers
- General Counsel
- Service members
- Recipients of your services
- Other government agencies

**NIST Draft Guide to Protecting the Confidentiality of (PII) (1/09)**

# Defense Privacy Office

## Privacy – Security Interface




NIST Draft Guide to Protecting the Confidentiality of (PII) (1/09)

# Defense Privacy Office

**Close coordination among privacy officers, chief information officers, information security officers, and legal counsel are essential when addressing PII issues.**

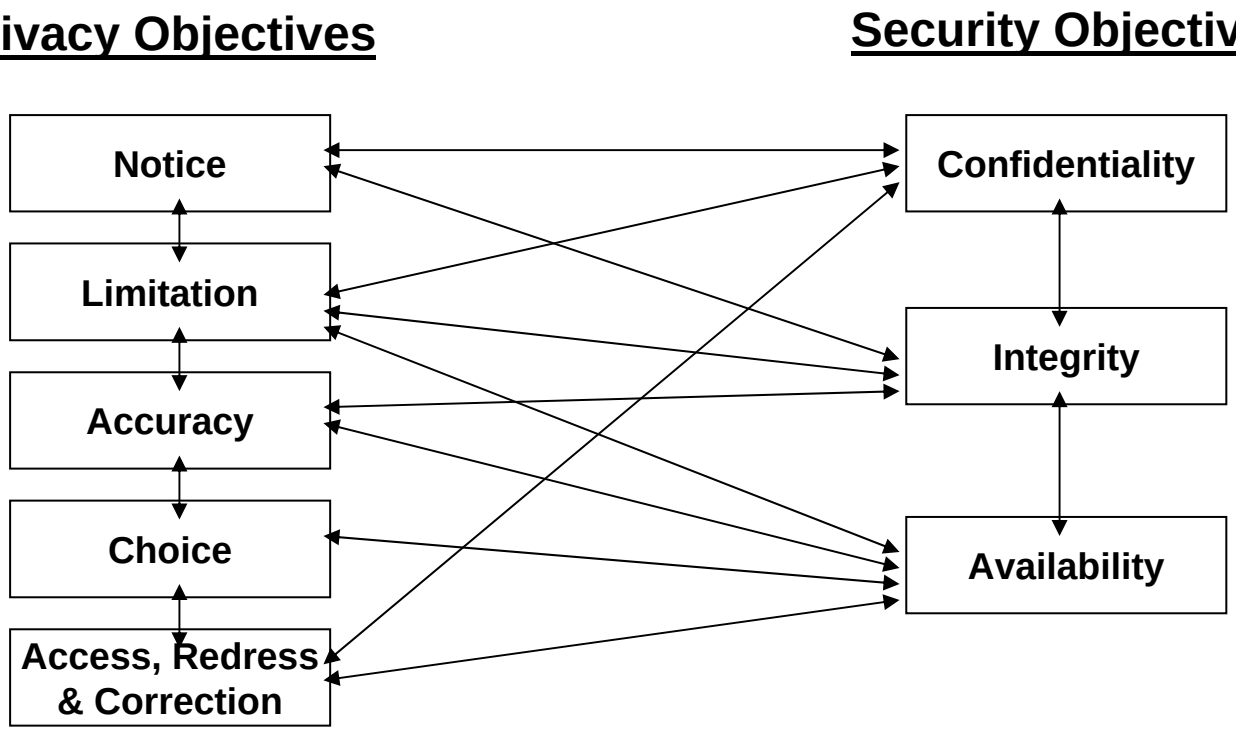
Protecting the confidentiality of PII requires knowledge of information systems, information security, privacy, and legal requirements.

Decisions regarding the applicability of a particular law, regulation, or other mandate should be made in consultation with an organization's legal counsel and privacy officer because relevant laws, regulations, and other mandates are often complex and change over time.

Additionally, new policies often require the implementation of technical security controls to enforce the policies. Close coordination of the relevant experts helps to prevent PII breaches by ensuring proper interpretation and implementation of requirements.

# Defense Privacy Office

**Some privacy objectives are only partially supported by the security objectives or are fully independent of the security objectives.**




NIST Draft Guide to Protecting the Confidentiality of (PII) (1/09)

# Defense Privacy Office

## Putting It Into Action

- Chart the flow of PII both inside and leaving your organization.
- Identify points of exit.
- Inventory and categorize PII identified in your flowchart.
- Share your flowchart with the CIO and other stakeholders.
- Update the flowchart annually.
- Crosswalk information technology, privacy and information assurance policies.
- Create a decision flowchart to assess the risk level of PII.
- Build privacy in during the early stages of the system development life cycle.
- Train, train, train …
- Stay on top of the latest technology trends.

# Defense Privacy Office

*Current DPO Issues*

*and Privacy Concerns*

# Defense Privacy Office

## Breach Reporting

**Office of Management and Budget (OMB) Defines a Breach as:**

**"A loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic."**

**DoD Breach Policy requires a Breach report be made:**

**To US-CERT[1] within one hour of discovering that a breach of PII has occurred;**

**To the Senior DoD Component Official for Privacy within 24 hours;**

**To the Defense Privacy Office within 48 Hours for use in further reporting.**

[1] United States Computer Emergency Readiness Team at www.us-cert.gov.

# Defense Privacy Office

## Breach Reporting

**The Breach report to the Senior Component Official for Privacy must include:**

- **The component or organization involved;**
- **Specific dates, number and type of individuals involved;**
- **Facts and circumstances surrounding the loss, theft or compromise;**
- **Brief descriptions of actions taken;**
- **Status of notification of affected individuals;**
- **Remedial actions that have or will be taken to prevent similar incidents in the future.**

DoD 5400.11-R, May 14, 2007

# Defense Privacy Office

## Breach Reporting

### Notification of Individuals in Breaches

**Notification to individuals must be made as soon as possible, but no later than 10 working days after the loss, theft or compromise is discovered and the identity of the individuals is ascertained.**

**It is also noted that "…agencies should bear in mind that notification of a breach when there is little or no risk of harm to the individual might create unnecessary concern and confusion."**

# Defense Privacy Office

## Notification of Individuals in Breaches

Five Factor Risk Assessment Model

| | |
|---|---|
| **Nature of the Data Elements Breached** | The nature is a key factor. A database with SSN and Birthdates may be riskier than the loss of a database with just names, depending on content. |
| **Number of Individuals Affected** | The number affected may dictate the method you use for notification. |
| **Likelihood the Information is Accessible and Usable** | Consider the likelihood Personally Identifiable Information will be or has been used by unauthorized individuals. |
| **Likelihood the Breach May Lead to Harm** | Consider broad reach of potential harm; Likelihood may depend on the manner of the actual or suspected breach and type(s) of data involved. |
| **Ability of the Agency to Mitigate the Risk of Harm** | The risk of harm will depend on how the agency is able to mitigate further compromise of the system (s) affected. Monitoring systems for misuse and patterns of suspicious behaviors. |

# Defense Privacy Office

*Social Security Number Reduction*

# Defense Privacy Office

## Social Security Number (SSN) Reduction

**The reduction of the use of the SSN was required by OMB M-07-16.**

**This effort has been approached as a part of DoD's effort to create a 'Culture of Security'**

**DoD Policy – DTM dated 28 MAR 08:**

- **http://www.dtic.mil/whs/directives/corres/pdf/pr080328ssn.pdf**

**The DoD Instruction is currently in the SD-106 process for formal coordination.**

# Defense Privacy Office

## Reducing Dependence on SSNs

**Must have positive authority for use.**

**Reduction/elimination is not meant to cause failure of business processes.**

**No direct funding to support.**

**Expect changes to coincide with system lifecycles.**

**Plan for elimination doesn’t mean it has to go away this minute.**

# Thinking Through the Challenge

**During the SSN reduction evaluation phase, users should be looking to improve security and protection for SSNs they have in their systems.**

**Documentation of completed reviews should show that users have really looked for alternatives to use of SSNs.**

**It is unacceptable to simply say it can't be done.**

# Defense Privacy Office

## It's Not Only About SSNs

**SSNs are high profile, but not the only threat.**

**Have to think about all PII and only collect what is REALLY needed. *Business as usual is unacceptable*.**

**This is about protecting ourselves and the organization and reducing the liability for both.**

# Defense Privacy Office

## The DoD SSN Reduction Plan

### Acceptable Uses of the Social Security number:

| | |
|---|---|
| 1. Geneva Convention Serial Number | 7. Federal Taxpayer Identification Number |
| 2. Law Enforcement, National Security, Credentialing | 8. Computer Matching |
| 3. Security Clearance Investigation or Verification | 9. Foreign Travel |
| 4. Interaction with financial Institutions | 10. Noncombatant Evacuation Operations (NEOs) |
| 5. Confirmation of Employment Eligibility | 11. Legacy Systems Interface |
| 6. Administration of Federal Worker's Compensation | 12. Other Cases. (Justification of use requires specific documentation) |

# Defense Privacy Office

*Biometrics and DNA*

# Defense Privacy Office

## Biometrics

**The use of biometrics creates a unique identifier that can be electronically stored, retrieved, and compared with other information collected on an individual to aid decision-making and to facilitate individual information sharing in accordance with applicable laws and policies. Common scenarios include the following:**

- **Credentials acceptable for use to grant base and systems access.**
- **Information to identify a specific individual; to determine if the person is cleared for a meeting.**
- **To determine if an individual participated in criminal activity since their last periodic investigation.**

# Defense Privacy Office

## Biometrics

**The government sector was and continues to be the driving force behind the use of Identity Management (IdM).**

**Banks, e-commerce, the transportation industry, and communications companies are examples of industry leaders being the first to explore identity management concepts beginning around the year 2000. The US Government didn't actively engage until after 9-11 by enacting Homeland Security Presidential Directive 12 (HSPD-12) in 2001, for example.**

**HSPD-12 is a federal mandate that requires a common, interoperable, and rapidly electronically-verifiable credential (e.g., a smart card with Public Key Infrastructure (PKI) certificates) for physical and logical access to federally-controlled Standards (FIPS) 201 for Personal Identity Verification (PIV) requires both a contact (e.g., integrated circuit chip) and contactless interface. The DoD's Common Access Card (CAC) implementation preceded the HSPD-12 directive and is not yet 100% compliant.**

# Defense Privacy Office

## Biometrics

**The collection of biometrics does not violate the Privacy Act or infringe upon the rights of any individual. The Act provides US persons with rights of access, amendment or correction, and accounting.**

**The Privacy Act provides for a balancing of interests of the DoD's need for collection, use, and dissemination of information about individuals, balanced against the privacy interests of those individuals.**

**Biometric data files are routinely collected from DoD employees, military members and others for the purposes of controlling access to DoD facilities and networks. Biometric data files compiled for access purposes are stored separate and apart from those collected as a result of military operations.**

# Defense Privacy Office

## Biometrics

### Biometrics is not something new and unproven.

**Biometric modalities like face, voice, and gait have always been used for human identification. There are other notable early examples, however.**

**European explorer Joao de Barros recorded the first known example of fingerprinting, which is a form of biometrics, in China during the 14th century. Chinese merchants used ink to take children's fingerprints for identification purposes.**

**In 1890, Alphonse Bertillon, a Parisian police officer studied body mechanics and measurements to help identify criminals.**

**The U.S. Army began using fingerprints in 1905. Two years later the U.S. Navy started, and was joined the next year by the Marine Corps.**

# Defense Privacy Office

## Biometrics

**Biometrics are genetically unique to the individual but are not more private than other forms of identification like the Social Security Number. There is nothing inherently private about a biometric. We leave them wherever we go. Fingerprints are one example that we leave on anything we touch.**

**The concept of privacy is more compelling as the physiological features at issue become less readily apparent and more abstract (e.g., iris patterns, DNA).**

**The advent of new technology does not change the fact a person's biometrics are commonly used for identification, are held out to the public, and are readily accessible to others.**

# Defense Privacy Office

## Biometrics

**Biometric programs in use today nearly guarantee the true identity of individuals included within our databases. If a US person is identified or makes a claim of citizenship, that person's biometric data is quarantined and no longer made available for non-consensual use by DoD.**

**Biometric data contributes greatly toward the establishment and maintenance of peaceful, safe, and secure communities. The value and sensitivity of the information contained within these databases and their safeguarding is viewed as a serious responsibility. DoD conducts all of its biometric programs in strict accordance with existing US governmental and/or DoD policy and directives.**

# Defense Privacy Office

## Biometrics Best Practices

| Scope and Capabilities | |
|---|---|
| **Scope Limitation** | Biometric deployments should not be expanded to perform broader verification or identification-related functions than originally intended. |
| **Establishment of a Universal Unique Identifier** | Biometric information should not be used as a universal unique identifier. |
| **Limited Storage of Biometric Information** | Biometric information should only be stored for the specific purpose of usage in a biometric system, and should not be stored any longer than necessary |
| **Evaluation of Potential System Capabilities** | When determining the risks a specific system might pose to privacy, the system's *potential* capabilities should be assessed in addition to risks involved in its intended usage. |
| **Collection or Storage of Extraneous Information** | The non-biometric information collected for use in a biometric verification or identification system should be limited to the minimum necessary to make identification or verification possible. |
| **Storage of Original Biometric Data** | If consistent with basic system operations, biometric data in an identifiable state, such as a facial image, fingerprint, or vocal recording, should not be stored or used in a biometric system other than for the initial purposes of generating a template. |

# Defense Privacy Office

## Biometrics Best Practices

| Data Protection | |
|---|---|
| **Protection of Biometric Information** | Biometric information should be protected at all stages of its lifecycle, including storage, transmission, and matching. |
| **Protection of Post-Match Decisions** | Data transmissions resulting from biometric comparisons should be protected. |
| **Limited System Access** | Access to biometric system functions and data should be limited to certain personnel under certain conditions, with explicit controls on usage and export set in the system. |
| **Segregation of Biometric Information** | Biometric data should be stored separately from personal information such as name, address, and medical or financial data. |
| **System Termination** | A method should be established by which a system used to commit or facilitate privacy-invasive biometric matching, searches, or linking can be depopulated and dismantled. |

# Defense Privacy Office

## Biometrics Best Practices

| User Control of Personal Data | |
|---|---|
| **Ability to "Unenroll"** | Individuals should, where possible, have the right to control usage of their biometric information, and the ability to have it deleted, destroyed, or otherwise rendered unusable upon request |
| **Correction of and Access to Biometric-Related Information** | System operators should provide a method for individuals to correct, update, and view information stored in conjunction or association with biometric information. |
| **Anonymous Enrollment** | Depending on operational feasibility, biometric systems should be designed such that individuals can enroll with some degree of anonymity. |

# Defense Privacy Office

## Biometrics Best Practices

| Disclosure, Auditing, Accountability and Oversight | |
|---|---|
| **Third Party Accountability, Audit, and Oversight** | The operators of certain biometric systems, especially large-scale systems or those employed in the public sector, should be held accountable for system use. |
| **Full Disclosure of Audit Data** | Individuals should have access to data generated through third-party audits of biometric systems. |
| **System Purpose Disclosure** | The purposes for which a biometric system is being deployed should be fully disclosed. |
| **Enrollment Disclosure.** | Ample and clear disclosure should be provided when individuals are being enrolled in a biometric system |
| **Matching Disclosure.** | Ample and clear disclosure should be provided when individuals are in a location or environment where biometric matching (either 1:1 or 1:N) may be taking place without their explicit consent. |
| **Use of Biometric Information Disclosure** | Institutions should disclose the uses to which biometric data are to be put, both inside and outside a given biometric system. |

# Defense Privacy Office

## Biometrics Best Practices

| Disclosure, Auditing, Accountability and Oversight (continued) | |
|---|---|
| **Disclosure of Optional/Mandatory Enrollment** | Ample and clear disclosure should be provided indicating whether enrollment in a biometric system is mandatory or optional. |
| **Disclosure of Individuals and Entities Responsible for System Operation and Oversight** | As a precondition of biometric system operation, it should be clearly stated who is responsible for system operation, to whom questions or requests for information are addressed, and what recourse individuals have to resolve grievances |
| **Disclosure of Enrollment, Verification and Identification Processes** | Individuals should be informed of the process flow of enrollment, verification, and identification. This includes detailing the type of biometric and non-biometric information they will be asked to provide, the results of successful and unsuccessful positive verification, and the results of matches and non-matches in identification systems. |
| **Disclosure of Biometric Information Protection and System Protection** | Individuals should be informed of the protections used to secure biometric information, including encryption, private networks, secure facilities, administrative controls, and data segregation. |
| **Fallback Disclosure** | When available, fallback authentication processes should be available for individuals to review should they be unable or unwilling to enroll in a biometric system. |

# Defense Privacy Office

## Deoxyribonucleic Acid (DNA)

**The DNA Fingerprint Act of 2005 (Pub. L. 109-162) directed that agencies of the United States Government must take DNA samples from those arrested, facing charges, or convicted.**

**In general, samples are to be taken from those for whom fingerprints are taken.**

**This would generally be:**

**At the "arrest" phase of criminal processing.**

**Based on probable cause.**

# Defense Privacy Office

## DNA

**The DNA Fingerprint Act is implemented by the United States Attorney General who has directed the Department of Defense (DoD) to apply similar rules.**

- **Samples taken within DoD from known offenders or from crime scenes are forwarded for inclusion in a National DNA Index System (NDIS).**
- **DoD enters its samples into the database through the US Army Criminal Investigations Laboratory (Ft Gillem, GA).**
- **The database may by searched by various state and federal law enforcement personnel.**

# Defense Privacy Office

## DNA

**Prior to the DoD Fingerprint Act of 2005, samples from military members would only be entered into NDIS:**

**After conviction by a special or general courts-martial of "qualifying military offense (QMO)"**

**QMO: An offense that is punishable by a year or more in confinement**

**The DNA Fingerprint Act of 2005 significantly expands the prior law to a much earlier DNA sample collection in the criminal justice process.**

# DNA

**DoD is currently working with the Department of Justice to implement the DNA Fingerprint Act.**

**There are challenges because of differences between civilian criminal processing and the military justice system.**

- **The military justice system is run by commanders.**
- **It does not recognize traditional concepts of arrest.**

# Defense Privacy Office

## DNA

**Proposed DoD guidelines:**

**DNA would only be taken for those offenses:**

**For which DoD criminal investigators actually take fingerprints (this would generally be in arrests for the more serious cases);**

**For which an individual is charged with a crime, or**

**For which a Service member is ordered into pre-trial confinement.**

**In general, expungement could be requested by an individual when the offense did not result in a conviction.**

*Access Controls*

# Defense Privacy Office

## Homeland Security Presidential Directive 12 (HSPD 12)

HSPD 12, signed by the President on August 27, 2004 established the requirements:

- For a common identification standard for identification credentials issued by Federal departments and agencies
- To Federal employees and contractors (including contractor employees) for gaining physical access to Federally controlled facilities and,
- Logical access to Federally controlled information systems.

# Defense Privacy Office

## HSPD-12 explicitly states that:

"Protecting personal privacy" is a requirement of the personal identity verification (PIV) system.

- All departments and agencies shall implement the PIV system in accordance with the spirit and letter of all privacy controls specified in this standard.
- As well as those specified in Federal privacy laws and policies including but not limited to the E-Government Act of 2002 [E-Gov], the Privacy Act of 1974 [PRIVACY], and Office of Management and Budget (OMB) Memorandum M-03-22 [OMB322], as applicable.

# Defense Privacy Office

## HSPD-12 Control Objectives

Established control objectives for secure and reliable identification of Federal employees and contractors. Each agency's PIV implementation shall meet the four control objectives in Paragraph 3:

"Secure and reliable forms of identification" for purposes of this directive means identification that:

(a) is issued based on sound criteria for verifying an individual employee's identity;
(b) is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation;
(c) can be rapidly authenticated electronically; and
(d) is issued only by providers whose reliability has been established by an official accreditation process."

# Defense Privacy Office

## Documentation

Write, publish, and maintain a clear and comprehensive document listing the types of information that will be collected (e.g., transactional information, personal information in identifiable form [IIF]).

- The purpose of collection, what information may be disclosed to whom during the life of the credential, how the information will be protected, and the complete set of uses of the credential and related information at the department or agency.
- PIV applicants shall be provided full disclosure of the intended uses of the PIV credential and the related privacy implications.

# Defense Privacy Office

## Technologies

Assure that the technologies used in the department or agency's implementation of the PIV system allow for continuous auditing of compliance with stated privacy policies and practices governing the collection, use, and distribution of information in the operation of the program.

- Utilize security controls described in NIST SP 800-53, Recommended Security Controls for Federal Information Systems, to accomplish privacy goals.
- Ensure that the technologies used do not erode privacy protections relating to the use, collection, and disclosure of information in identifiable form.
- Employ an electromagnetically opaque sleeve or other technology to protect against any unauthorized contactless access to information stored on a PIV credential.

# Defense Privacy Office

Assure that systems that contain IIF for the purpose of enabling the implementation of PIV are handled in full compliance with fair information practices as defined in privacy.

- Maintain appeals procedures for those who are denied a credential or whose credentials are revoked.
- Ensure that only personnel with a legitimate need for access to IIF in the PIV system are authorized to access the IIF, including but not limited to information and databases maintained for registration and credential issuance.
- Coordinate with appropriate department or agency officials to define consequences for violating privacy policies of the PIV system.

# Defense Privacy Office

**Concern:** The lack of uniform standards controlling the access to information and systems can lead to disparities and weaknesses, which could be exploited for malicious or other reasons.

- Analyze your information classification needs, and formulate an access control policy.
- Develop appropriate and uniform access control standards.
- Consider the sensitivity level of the data being processed by each business system and its appropriate level of access control.

# Defense Privacy Office

How Do We Get There?

# Compliance Reporting

# Defense Privacy Office

## Requirement for Privacy Compliance Reporting

- DoD 5400.11-R, C.8.,“Department of Defense Privacy Program Regulation”, May 14, 2007
- The Office of Management and Budget Circular A-130
- Section 803 of the “Implementing Recommendations of the 9/11 Commission Act of 2007”, Public Law 110 - 53, August 3, 2007.
- Federal Information Security Management Act (FISMA)

# Defense Privacy Office

## Compliance and Reporting

### Defense Privacy Office Quarterly Reports

- System/SORN & Exemption Reviews
- Privacy Act Statement (e)(3) Reviews
- Computer Matching Agreements
- Training Completion Reporting (*NEW 1st QTR CY 2009*)

# Defense Privacy Office

## Compliance and Reporting

### Defense Privacy Office Quarterly Reports

9/11 Commission Recommendations Section 803 Quarterly Report Requirement consists of:

- Number and Type of Reviews Undertaken
- Types of Advice Provided & Response Given
- Number, Nature and Disposition of Complaints

# Defense Privacy Office

## Compliance and Reporting

Federal Information Security Management Act (FISMA) FISMA Report

Must accurately reflect the overall status of program, without conflicting views of or unresolved differences from the Chief Information Officer (CIO), the Inspector General (IG), and the Senior Agency Official for Privacy (SAOP).

# Defense Privacy Office

## Compliance and Reporting

Federal Information Security Management Act (FISMA) goal:

The goal of FISMA is stronger agency and government-wide security information regarding an agency's information security program should be shared as it becomes available.

- This helps promote timely correction of weaknesses in the agency's information systems.

# Privacy Program Review

# Defense Privacy Office

## DoD Privacy Program review:

- DoDD 5400.11, “DoD Privacy Program”, May 8, 2007
- DoD 5400.11-R,“DoD Privacy Program”, May 14, 2007
- DoD Memorandum, “Safeguarding Against and Responding to The Breach of Personally Identifiable Information”, September 25, 2008.
- Office of Management and Budget Circular A-130
- Section 803 of “Implementing Recommendations of the 9/11 Commission Act of 2007”, Public Law 110 - 53, August 3, 2007.
- Federal Information Security Management Act (FISMA)

# Defense Privacy Office

Transparency

# Defense Privacy Office

## Transparency in Government

Transparency:  Something that can be seen through.

When we talk transparency in government, citizens must be able to see through its workings.

“(We must) work together to ensure the public trust and establish a system of transparency, public participation, and collaboration.  Openness will strengthen our democracy and promote efficiency and effectiveness in Government."  - *President Obama*

# Defense Privacy Office

## Transparency in Government

### On January 21, 2009, President Obama issued two key transparency memoranda

*A profound National commitment to ensuring an open government*

| | |
|---|---|
| Presidential Memorandum on the Freedom of Information Act | Directs the Attorney General to issue new guidelines for FOIA openness in 120 days. |
| Presidential Memorandum on Transparency and Open Government | Directs Chief Technology Officer, Director Office of Management and Budget and Administrator of General Services to produce an Open Government Directive within 120 days to implement the principles in the Memorandum.<br>–Government is Transparent<br>–Government is Participative<br>–Government is Collaborative |

# 2009 DoD Privacy Series Workshop

**Privacy Horizons**
**Presented by**
**Samuel P. Jenkins, Director, Defense Privacy Office**
**Sponsored by: Booz Allen Hamilton**

Thank You!

**My Question to YOU: Where Do We Go Next?**