

How to Conduct A Privacy Audit

Bruce J. Bakis
in collaboration with Julie Smith McEwen, CIPP/G, CISSP

Presentation for the 2007 New York State Cyber Security
Conference

June 6, 2007

Presentation Overview

- **Section 1: Privacy overview**
 - What is privacy: Key definitions
 - Why is it important to protect privacy?
 - How is privacy different from security?
- **Section 2: Privacy audit criteria**
 - What the privacy audit does
 - Components of effective privacy programs
- **Section 3: Sample audit approach**
- **Section 4: Lessons learned**
 - Privacy Principles
 - Privacy-related policies and procedures
 - Identifying Personally Identifiable Information (PII)
 - Data flow mapping
 - PII risk levels
 - Privacy incident categories

Overview (cont.)

- **Common privacy mistakes: Collection and use of PII**
- **Common privacy mistakes: Notices and privacy impact assessment**
- **Common privacy mistakes: Operational privacy issues**
- **Section 5: Conclusion**



Section 1: Privacy Overview

What is Privacy: Key Definitions

- **Personally Identifiable Information (PII)**
 - Information that directly or indirectly identifies an individual
 - Examples include name, address, date and place of birth, Social Security Number, biometric identifiers (e.g., photo, fingerprint)
- **Privacy**
 - Ability of an individual to exercise control over the collection, use, and dissemination of PII
- **Confidentiality**
 - Assurance that PII is not disclosed to unauthorized entities (people and systems).

Why Is It Important to Protect Privacy?

- **Privacy is a core value of our society**
- **Potential consequences for not adequately protecting privacy in the government include:**
 - **Reduced mission effectiveness for government organizations**
 - **Negative impact upon individuals whose PII is collected and used; examples include:**
 - **Identity theft**
 - **Embarrassment**
 - **Loss of credibility, confidence, and trust in government organizations from covered individuals, the public, and stakeholders**

Identity Theft Statistics

- Since January 2005, over 153 million data records have been compromised¹
- The government sector has more identity theft-related data breaches than any other sector (25% of all cases)²
- Victims of identity theft spend an average of 330 hours and \$4,000 in lost wages to repair the damage³

¹www.privacyrights.org/ar/ChronDataBreaches.htm

²Symantec Internet Security Threat Report, Trends for July-December 06, Volume XI, March 2007

³Identity Theft Resource Center, Identity Theft, The Aftermath, 2004

Privacy Incident Response Statistics*

- **Almost 30% of all reported data breaches originate with external partners, consultants, outsourcers, or contractors**
- **Recovery costs per data breach incident average \$4.8M**
- **Even after privacy incidents are discovered, many organizations have not identified a clear cross-organizational owner for breach recovery**

***2006 Annual Study: Cost of a Data Breach, Ponemon Institute**

Examples of Federal Government Privacy Incidents*

Date	Organization	Type of Breach	Number of Records
February 2006	Agriculture	Exposed Social Security Number (SSN) and tax ID numbers in FOIA request.	350,000
May 2006	Veterans Affairs	Data on stolen laptop included names, SSNs, dates of birth, phone numbers, and addresses of all American veterans who were discharged since 1975.	28,600,000
June 2006	U.S. Navy	Civilian web site contained files with PII of Navy members and dependents including names, birth dates, and SSNs.	30,000
June 2006	Government Accountability Office	Data from audit reports on Defense Department travel vouchers were inadvertently posted online, including names, SSNs, and addresses.	1,000
May 2007	Transportation Security Administration	A computer hard drive containing SSNs, bank data and payroll for TSA employees was reported missing.	100,000

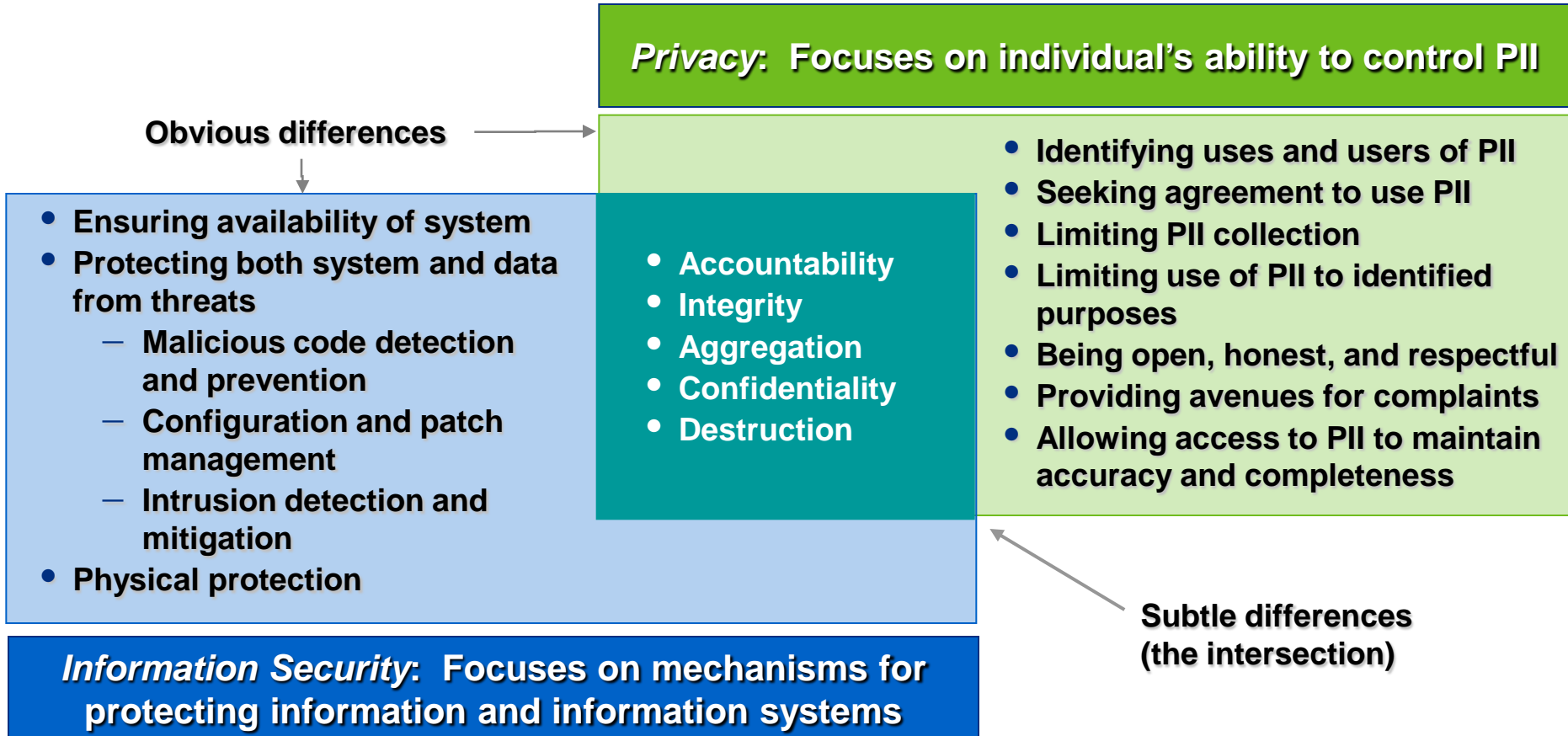
*Source: Privacy Rights Clearinghouse, <http://www.privacyrights.org/ar/ChronDataBreaches.htm>

Examples of State/Local Government Privacy Incidents*

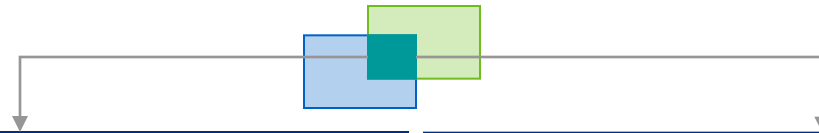
Date	Organization	Type of Breach	Number of Records
January 2006	State of Rhode Island web site	Hackers obtained credit card information in conjunction with names and addresses.	4,117
March 2006	California State Employment Development Division	Computer glitch sends state Employment Development Division 1099 tax forms containing Social Security Numbers and income information to wrong addresses.	64,000
March 2006	Georgia Technology Authority	Hacker exploited security flaw to gain access to information including SSNs and bank account details of state pensioners.	573,000
January 2007	Kansas City, Missouri	26 IRS computer tapes containing taxpayer information were reported missing after they were delivered to City Hall. They potentially contain taxpayers' names, SSNs, bank account numbers, or employer information.	Unknown
May 2007	Maryland Dept. of Natural Resources (DNR)	Miniature data storage device containing names and SSNs of current and retired DNR employees was reported missing.	1,433

*Source: Privacy Rights Clearinghouse, <http://www.privacyrights.org/ar/ChronDataBreaches.htm>

Privacy vs. Information Security



Privacy vs. Information Security (Concluded)



	Information Security	Privacy
Accountability	<ul style="list-style-type: none"> Focuses on tracking an individual's actions and manipulation of information 	<ul style="list-style-type: none"> Focuses on tracking the trail of PII disclosure
Integrity	<ul style="list-style-type: none"> Protects against the corruption of data by authorized or unauthorized individuals 	<ul style="list-style-type: none"> Seeks to ensure that inaccurate PII is not used to make an inappropriate decision about a person
Aggregation	<ul style="list-style-type: none"> Focuses on determining the sensitivity of derived and aggregated data so that appropriate access guidance can be defined 	<ul style="list-style-type: none"> Dictates that aggregation or derivation of new PII should not be allowed if the new information is neither authorized by law nor necessary to fulfill a stated purpose
Confidentiality	<ul style="list-style-type: none"> Focuses on processes and mechanisms (e.g., authenticators) that prevent unauthorized access 	<ul style="list-style-type: none"> Focuses on ensuring that PII is only disclosed for a purpose consistent with the reason it was collected
Destruction	<ul style="list-style-type: none"> Focuses on ensuring that information cannot be recovered once deleted 	<ul style="list-style-type: none"> Addresses the need for the complete elimination of collected information once it has served its purpose



Section 2: Privacy Audit Criteria

What the Privacy Audit Does

- **Periodically determines degree of compliance with:**
 - **Applicable privacy laws and regulations**
 - **Required privacy practices—Privacy Rules of Behavior which consist of principles, policies and practices**

Value of Privacy Audit

- **Measures privacy effectiveness**
- **Demonstrates compliance**
- **Reveals gaps between required and actual privacy management, operational and technical controls**
- **Provides basis for privacy remediation and improvement plan**
- **Enhances effectiveness and completeness of security assessment process by addressing privacy-specific criteria**

Fair Information Practices

■ Overview

- Widely-accepted standards for collecting, using, and safeguarding personal information
- Implemented by Privacy Act of 1974
- Recognized throughout many parts of the world
- Supports an open and accountable policy

■ Practices

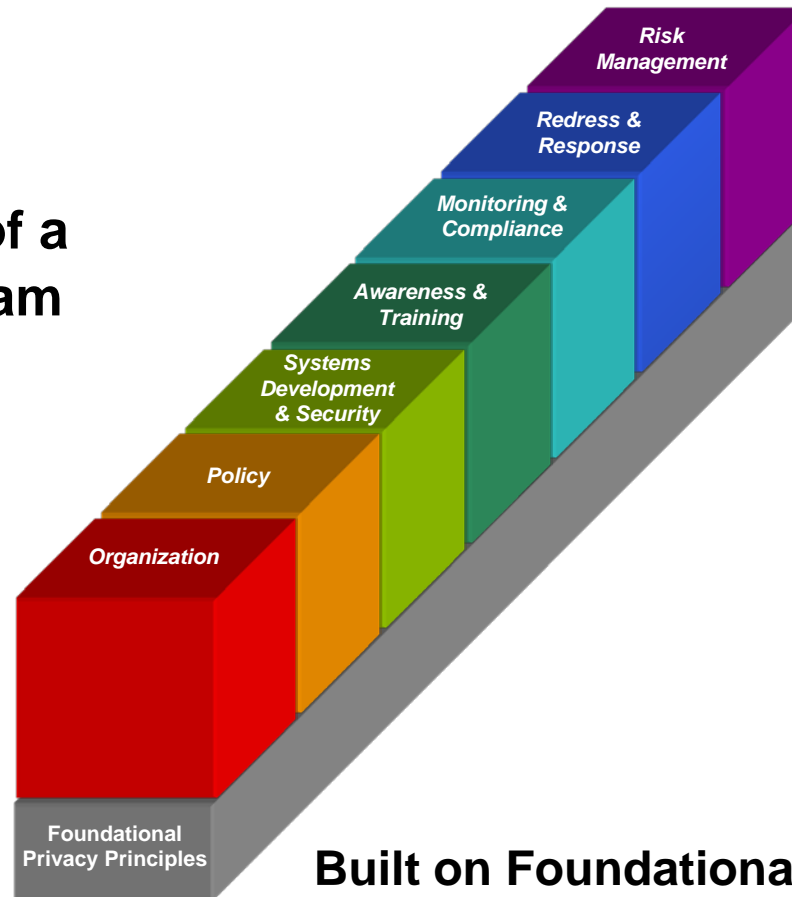
- Notice/Awareness
- Choice/Consent
- Access/Participation
- Integrity/Security
- Enforcement/Redress
- Limitation

Main Privacy Program Objectives

- **Establish high-standard privacy protection**
 - **Comply with the letter and the spirit of privacy laws and regulations**
 - **Facilitate appropriate sharing of PII**
 - **Reduce threats to PII including identity theft and insider threat**
- **Improve audit posture**

Effective Privacy Program

Components of a Privacy Program



Built on Foundational Privacy Principles

Effective Privacy Programs

Components

Foundational Privacy Principles	Fundamental tenets that guide a privacy program
Organization	People/processes responsible for assessing privacy risks and developing and implementing plans to manage risks
Policy	Privacy rules and ways to adhere to them
Systems Development & Security	Administrative, physical, and technical safeguards that control privacy risks, including PIAs and system engineering
Awareness & Training	Programs to make an organization and the public aware of the organization's privacy policy and practices
Monitoring & Compliance	Programs to monitor adherence to privacy rules of behavior and to applicable laws and regulations
Redress & Response	Systems and processes to respond, if needed, to privacy issues and incidents
Risk Management	Tools and techniques to support privacy risk management



Section 3: Sample Audit Approach

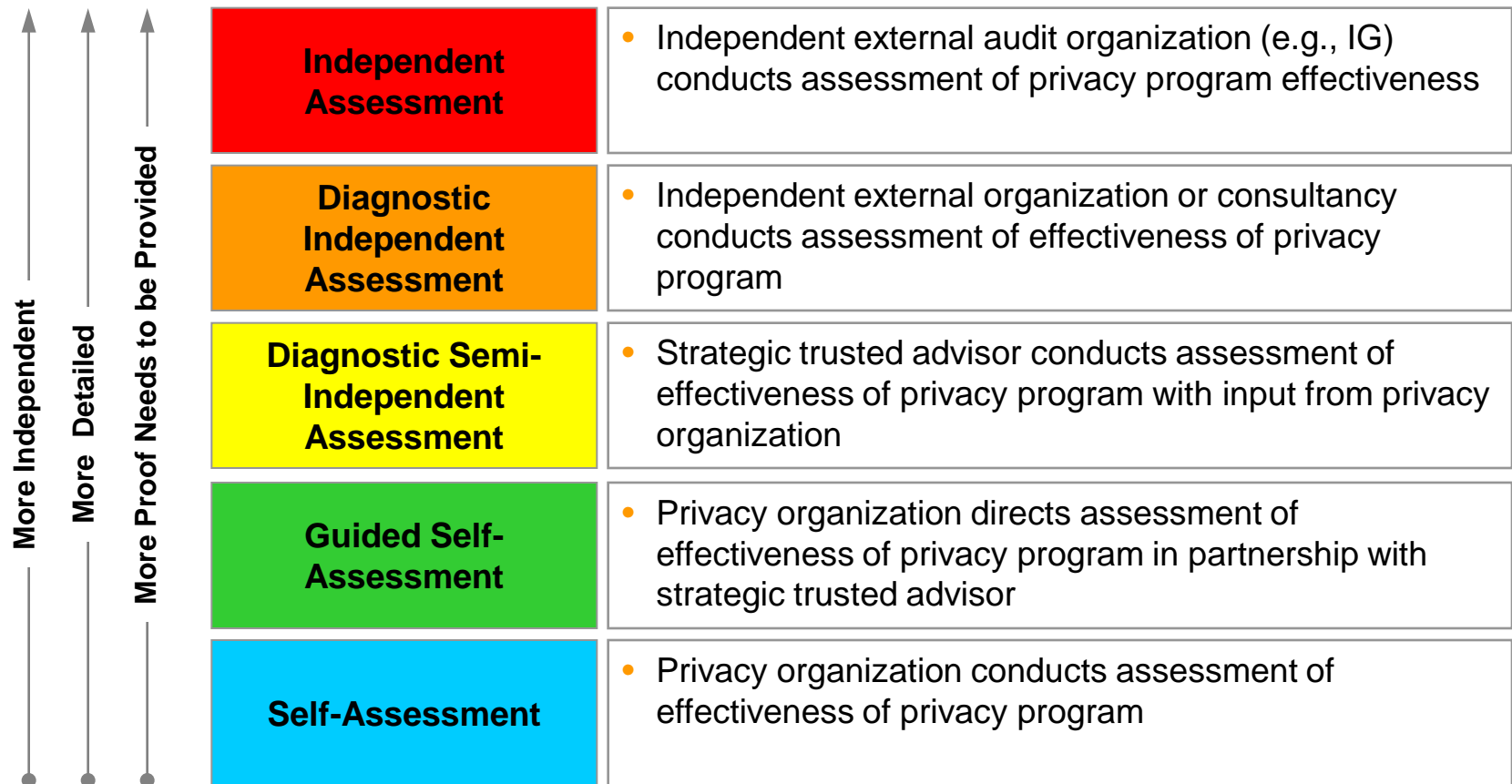
Sample Audit Approach: Steps in the Audit Process

■ Steps in the Privacy Audit

- Define scope of audit and approach
- Identity stakeholders and their responsibilities
- Complete Audit Plan
- Develop audit criteria
 - Used self-assessment criteria and results as starting point for developing audit criteria
- Conduct audit
 - Followed basic audit guidance and best practices – e.g., refer to *IS Standards, Guidelines and Procedures for Auditing and Control Professionals*, Section G31, Privacy at <http://www.isaca.org>
- Write Audit Report and discuss remediation steps

Levels of Privacy Assessment

- **Strategy: begin to move up the stack**



Self-Assessment Instrument Characteristics

- **Privacy-centric version of security self-assessment developed by the National Institute of Standards and Technology (NIST) as a tool to comply with Federal Information Security Management Act (FISMA) information security assessment requirements**
- **Assessment requirements stated as control objectives**
 - Management (including roles and responsibilities)
 - Operational (including processes)
 - Technical (including privacy-specific mechanisms, for example machine readable website privacy policies)
- **Focuses on objective measures rather than subjective criteria or narrative**
- **Control objectives based on**
 - Privacy principles, policies and practices
 - Applicable privacy laws and regulations

Determine Scope of Privacy Audit


- **Compliance with applicable privacy laws and regulations**
 - Freedom of information
 - Personal privacy protection
 - Open meetings
 - Other laws related to specific areas that contain privacy provisions (e.g., health care)
 - International privacy laws and directives
- **Web site**
- **Subjects whose PII is collected and used**
 - Government personnel and contractors only for internal personnel processes
 - Public

Determine Scope of Privacy Audit (cont.)

- **Types of personnel who handle PII**
 - **Government staff and contractors working within organization**
 - **Other government organizations with whom PII is shared**
 - **Other organizations outside government with whom PII is shared, including commercial data providers**

Identify Stakeholders and Their Responsibilities

- **Sample stakeholders include:**
 - ***Privacy Officer:*** responsible for coordinating and conducting privacy self-assessments, reporting, and remediation planning and improvement
 - ***Security Officer:*** collaborates with Privacy Officer to include privacy-specific input to security reports
 - ***Chief Information Officer (CIO):*** responsible for compiling organization's security and privacy reports
 - ***Inspector General (IG) or other internal auditing organization:*** responsible for conducting independent security and privacy audits



Section 4: Lessons Learned

Lessons Learned Topics

- **Privacy Principles**
- **Privacy-related policies and procedures**
- **Identifying PII**
- **Data flow mapping**
- **PII risk levels**
- **Privacy incident categories**
- **Common privacy mistakes: Collection and use of PII**
- **Common privacy mistakes: Notices and privacy impact assessment**
- **Common privacy mistakes: Operational privacy issues**

Privacy Principles

- Typically based on
 - Fair Information Practices
 - Privacy-related laws
- For federal government examples, see:
 - Census Bureau
 - http://www.census.gov/privacy/files/data_protection/002822.html
 - IRS
 - <http://www.irs.gov/irm/part11/ch03s16.html>
 - Department of Homeland Security US-VISIT Program
 - http://www.dhs.gov/xtrvlsec/programs/editorial_0681.shtm
- Also see the list of Generally Accepted Privacy Principles developed by the American Institute of Certified Public Accountants (AICPA)
 - <http://www.aicpa.org>

Sample Topics Covered by Federal Government Privacy Principles

Census Bureau¹

- Necessity
- Openness
- Respectful treatment of respondents
- Confidentiality

IRS²

- Protecting taxpayer privacy is a public trust
- Collection limitation
- Use limitation
- Collect information directly; verify information for accuracy
- All employees share responsibility to protect privacy

US-VISIT³

- Responsibility and Accountability
- Privacy Awareness and Training
- Openness and Redress
- Identifying Purpose
- Informed Consent
- Limiting Collection, Use, Disclosure, and Retention
- Strict Confidentiality
- Data Integrity
- Individual Access
- Security

¹http://www.census.gov/privacy/files/data_protection/002822.html

²<http://www.irs.gov/irm/part11/ch03s16.html>

³http://www.dhs.gov/xtrvlsec/programs/editorial_0681.shtm

Privacy-Related Policies & Procedures

- **Privacy-related areas where specific policies and procedures should exist for a privacy program include:**
 - **Development of Privacy Impact Assessments (PIAs)**
 - PIA is an assessment of actual or potential impacts, including social and ethical, which a system may have on privacy and the ways in which any adverse impacts may be mitigated
 - Also serves as a public notice of a system's potential privacy impacts
 - **Development of System of Records Notices (SORNs)**
 - **Data (PII) retention**
 - **Redress**
 - **Consent**
 - **Access to PII**
 - **Data sharing agreements**
 - **Privacy incident response**

What is PII?

- **Information that could be considered PII, depending upon sensitivity and linkability to an individual, includes:**
 - **Name**
 - **Date of Birth**
 - **Social Security Number (or other number originated by a government that specifically identifies an individual)**
 - **Photographic Identifiers (e.g., photograph image, x-rays, and video)**
 - **Driver's License Number**
 - **Biometric Identifiers (e.g., fingerprint and voiceprint)**
 - **Mother's Maiden Name**
 - **Vehicle Identifiers (e.g., license plates)**
 - **Mailing Address**
 - **Phone Numbers (e.g., phone, fax, and cell)**
 - **Medical Records Numbers**
 - **Medical Notes**

What is PII? (cont.)

- **Financial Account Information and/or Numbers (e.g., checking account number and PINs)**
- **Certificates (e.g., birth, death, and marriage)**
- **Legal Documents or Notes (e.g., divorce decree, criminal records, or other)**
- **Device Identifiers (e.g., pacemaker, hearing aid, or other)**
- **Web URLs**
- **E-mail Address**
- **Education Records**
- **Military Status and/or Records**
- **Employment Status and/or Records**
- **Foreign Activities and/or Interests**

Identifying PII

- **Finding where PII is collected, stored, and used can be challenging**
- **Policies and procedures should include a process for identifying PII; auditors should review that process to verify that it is appropriate**
- **How to find PII**
 - **Types of information that may contain PII include education records, financial transactions, medical history, and criminal or employment history**
 - **System inventory information can provide information on what types of PII are in systems**
 - **Risk management activities (e.g., privacy impact assessments) can also provide information on types of PII in systems**
 - **Automated discovery tools: Privacy Enhancing Technologies (PETs)**

Data Flow Mapping

- A data flow map provides a picture of the movement of PII (via push or pull) between different types of organizations for a specific type of activity or transaction.
- It can be used to assist with risk management privacy and data protection practices within and across organizations or activities.

Data Flow Mapping (cont.)

- **Data flow mapping should be able to answer the following questions:**
 - **What different types of entities handle PII in this activity?**
 - **What are the typical PII flows between different types of entities?**
 - **What PII does each type of entity transmit to each other type of entity?**
 - **What PII does each type of entity receive from each other type of entity?**
 - **To what extent is the PII of a given individual persistent across flows, i.e., how much of the data traffic is pass-through of the same PII?**
 - **What are the relevant contextual factors surrounding the PII flows, e.g., security, regulation/protection regimes, and purpose?**

Different Strategies for Assigning Risk Levels to PII

- **Sensitivity:** Each term viewed in isolation from other information
- **Contingent sensitivity:** Sensitivity of certain terms increased in the presence of other relevant information
 - E.g., complete mailing address, personal property and an identifying number (besides Social Security Number)
- **Hybrid sensitivity:** Contingent sensitivity without an identifying number (besides Social Security Number)

Sample PII Risk Levels

- **1 = Low risk of tangible or intangible harm if compromised**
 - E.g., middle name, postal code
- **2 = Moderate risk of tangible or intangible harm if compromised**
 - E.g., drivers license number, weight
- **3 = High risk of tangible harm if compromised**
 - E.g., Social Security Number (SSN)

Privacy Incident Categories

- **Privacy risk can be assessed as a combination of likelihood and impact**
- **Privacy incident categories can be developed from privacy risk identification based on the following factors:**
 - **The number of individuals affected, and/or the level of sensitivity of the PII**
 - **The level of perception that privacy is being intruded upon, and/or the likelihood of exposure**

Sample Privacy Incident Categories

Category	Risk Level	Definition
1	Low	<ul style="list-style-type: none"> ■ A very limited number of individuals' PII may be exposed, and/or ■ PII is of limited sensitivity such that the exposure would cause minimal distress or inconvenience, requiring few or no corrective actions on the part of the individual and/or the program ■ The perception that privacy is being intruded upon is limited, and/or mitigation factors in place make the likelihood of exposure minimal.
2	Medium	<ul style="list-style-type: none"> ■ Numerous individuals' PII may be exposed; and/or ■ PII is of sensitivity such that exposure would cause significant distress or inconvenience requiring some corrective actions on the part of the individual and/or the program ■ The perception that privacy is being intruded upon is likely, and/or there is a strong possibility that adverse events will occur if no additional corrective measures are taken.
3	High	<ul style="list-style-type: none"> ■ A very large number of individuals' PII may be exposed, and/or ■ The nature of the PII is of high sensitivity such that exposure would cause extreme distress (e.g., vulnerability to blackmail) or inconvenience (e.g., identity theft) requiring extensive corrective actions on the part of the individual and/or the program ■ The perception that privacy is being intruded upon is extremely likely, and/or it is nearly certain that adverse events will occur if no additional corrective measures are taken.

Common Privacy Mistakes: Collection and Use of PII

- **Failing to realize that PII is collected, used, and/or maintained in a system**
- **Collecting, using, and/or maintaining more PII than is necessary**
 - **For example, Social Security Numbers are often collected and used when they are not needed**
- **Routine uses of PII are not defined with enough detail to make it difficult for “mission creep” to occur**

Common Privacy Mistakes: Notices and Privacy Impact Assessment (PIA)

- **Failing to publish a notice when a system of records is present**
- **Performing a PIA without performing a true analysis of privacy impact**
- **Assuming that security controls and information security measures have addressed privacy concerns**

Common Privacy Mistakes: Notices and Privacy Impact Assessment (PIA)

- **Failing to update a notice and/or PIA when there is a change in a system related to the collection and use of PII**
- **Examples of system changes include:**
 - **Conversions**
 - **Anonymous to non-anonymous**
 - **Significant system management changes**
 - **Significant merging**
 - **New public access**
 - **Commercial sources**
 - **New interdepartmental or interagency uses**
 - **Internal flow or collection**
 - **Alteration in character of data**

Common Privacy Mistakes: Operational Privacy Issues

- **Allowing unauthorized or inappropriate access to PII (e.g., do not have a need-to-know)**
- **Providing or accepting unauthorized PII sharing with another agency or third party**
- **Browsing or using PII for any purpose other than performing official duties**
- **Leaving PII unattended on a printer or fax**
- **Emailing PII without a Privacy Notice attached or without either encrypting or password protecting the PII**
- **Not physically securing a computer that contains PII, particularly a laptop**
- **Improperly disposing of PII**



Section 5: Conclusion

Conclusion

- **Privacy protection is an important issue for government agencies**
 - **Each organization should**
 - **Establish a comprehensive privacy program and execute that program strategically**
 - **Understand the connection between information privacy and security**
 - **Benefits include**
 - **Having an approach in place to prevent privacy problems from occurring and handle privacy problems when they do arise**
 - **Increased level of privacy assurance**
 - **Increased public confidence that PII is appropriately protected**
- **Conducting privacy audits will enable organizations to measure the effectiveness of their privacy programs and identify measures to implement in order to improve those programs.**