IAPP Privacy Certification

Certified Information Privacy Professional/Government (CIPP/G)

Government Privacy

Julie Smith McEwen, CIPP/G, CISSP
Principal Information Systems Privacy and Security Engineer

MITRE

learning objectives

This course material describes the privacy laws, policies and practices specific to U.S. federal and state governments as well as those more broadly applicable to both the public and private sectors. It will equip students to better understand:

- Principles for information security and public records management in government
- Information privacy laws regarding data quality, public access to records, open meetings and other disclosures
- Best practices for privacy auditing and privacy compliance

presenter

Julie Smith McEwen (CIPP/G, CISSP)

Is the Principal Information Privacy and Security Engineer and leads the privacy practice at MITRE Corporation, a federally funded research and development center based in Virginia. Ms. McEwen brings over 22 years of experience working with information privacy and security issues at the Department of Defense, IIT Research Institute and the Logistics Management Institute. She has performed privacy and security work for the U.S. House of Representatives, the Internal Revenue Service and the U.S. Treasury, among other federal agencies.

agenda

- privacy definitions and principles
- public and private sector information laws
- information laws for government practice

agenda

- privacy management
- policy enforcement
- records management
- auditing and compliance

Privacy Definitions and Principles

principles

Fair Information Practices (HEW report, 1973)

- Openness
- Notice
- Use
- Correction
- Accuracy and Security

principles

State of the Practice

- **Currently in the U.S.**
  - Not explicitly guaranteed in the U.S. Constitution
  - The Privacy Act of 1974 addresses privacy of an individual's PII as it exists within a system of records
- **Privacy Defined**
  - Legislation driven by need
  - Characteristics of the custodian rather than data
    - Gramm-Leach-Bliley Act (GLBA)
    - Health Insurance Portability and Accountability Act (HIPAA)
    - Children's Online Privacy Protection Act (COPPA)

principles

Organization for Economic Cooperation and Development (OECD)

- Collection Limitation
- Data Quality
- Purpose Specification
- Use Limitation
- Security Safeguards
- Openness
- Individual Participation
- Accountability

principles

Asia Pacific Economic Cooperation (APEC)

- Based on OECD
  - Intent is to be flexible and adaptable to global Information Operation
- Principles
  - Preventing Harm
  - Notice
  - Collection Limitation
  - Uses of Personal Information
  - Choice
  - Integrity of Personal Information
  - Security Safeguards
  - Access and Correction
  - Accountability

Public and Private Sector Information Laws

info laws

United States Privacy Laws

- Fair Credit Reporting Act (1970)
- Privacy Act (1974)
- Freedom of Information Act (1974)
- Family Educational Rights and Privacy Act (1974)
- Drivers Privacy Protection Act (1994)

info laws

United States Privacy Laws

- Health Insurance Portability and Accountability Act (HIPAA) (1996)
- Children's Online Privacy Protection Act (1998)
- Financial Services Modernization Act (GLBA) (1999)
- USA Patriot Act (2001)
- Data Quality Act (2002)
- E-Government Act (2002)

Information Laws for Government Practice

govmt laws

Freedom of Information Act (FOIA)

- Right for anyone to request access to federal agency records and information
  - Disclosure subject to exemptions discussed on next slide

govmt law

Freedom of Information Act
Exemptions Under FOIA

Exemption One: Classified Information

Exemption Two: Agency's Internal Personnel Rules & Practices

Exemption Three: Exempt by any other Statute

Exemption Four: Privileged & Confidential Trade Secrets, Commercial & Financial Information

Exemption Five: Privileged information Inter or Intra agency Memos

Exemption Six: Personnel, Medical & Similar Files

Exemption Seven: Law Enforcement Records

Exemption Eight: Financial Institution Regulatory Records

Exemption Nine: Geological & Geophysical Data Concerning Wells

govmt laws

Privacy Act of 1974

- Applies only to U.S. Citizens and lawfully admitted permanent resident aliens
- Objectives:
  - Restrict disclosure
  - Grant access
  - Grant amendment
  - Compile only what is relevant and necessary
  - Provide notice of new systems of records

govmt laws

Privacy Act of 1974
System of Records

- The term "system of records" means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual

govmt laws

Privacy Act of 1974
System of Records Notice (SORN)

- **A description of the system of records maintained by the agency**
- **The SORN must appear in the Federal Register before the agency begins to operate the system, e.g., collect and use the information**

govmt laws

Privacy Act of 1974

System of Records Notice (SORN)

- System Name
- Security Classification
- System Location
- Authority for Maintenance of the System
- Purpose of the System
- Use and Categories of users
- Policies & Practices for storing, retrieving, accessing, retaining, & disposing of records
- System Manager
- Notification Procedures

govmt laws

E-Government Act

- "...a broad framework of measures that require using Internet-based information technology to enhance citizen access to Government information and services ..." (H.R. 2458)
- Privacy Provisions (section (208) and OMB guidance require federal agencies
  - Post Web site privacy policies in both statement and machine-readable form
  - Conduct Privacy Impact Assessments

govmt laws

E-Government Act
Privacy Impact Assessments (PIAs)

- **PIA is an assessment process for identifying and mitigating the privacy risks from a system**
- **Section 208 requires agencies to conduct a PIA before developing or procuring IT systems that collect, maintain or disseminate information in identifiable form (IIF) from or about members of the public**

govmt laws

E-Government Act
Privacy Impact Assessments (PIAs)

OMB M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act

- What information is to be collected
- Why the information is being collected
- Intended use of the information
- With whom the information will be shared
- What opportunities individuals have to decline to provide information or consent to particular uses of the information
- How the information will be secured
- *Whether a system of records is being created under the Privacy Act*
- Analysis of choices agency made regarding an IT system or collection of information
- Information lifecycle analysis

govmt laws

E-Government Act
Privacy Impact Assessments (PIAs)

- **Exceptions**
  - For national security systems
  - Previously assessed systems under evaluation similar to PIA
  - Internal government operations
  - For government-run websites that do not collect identifiable information about the public
  - System collecting non-identifiable information

govmt laws

E-Government Act
Website Privacy Policy

- In addition to completing PIAs, agencies also must follow the web site policy in Section 208 of the E-Government Act
- The requirements are:
  - Post privacy policies on agency websites used by the public
  - Translate privacy policies into a standardized machine-readable format
  - Report annually to OMB

govmt laws

Data Quality Act of 2002

- Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility and Integrity of Information
- Report annually to OMB the number and nature of complaints received by the agency

govmt laws

Federal Information Security Management Act (FISMA)

- Framework for ensuring the effectiveness of INFOSEC controls
  - Guidelines for monitoring Federal programs
  - Specifies responsibilities of various entities including agency heads, CIOs, and others
  - Specifies requirements for incident response capability, and awareness training
  - Specifies annual reports to Congress

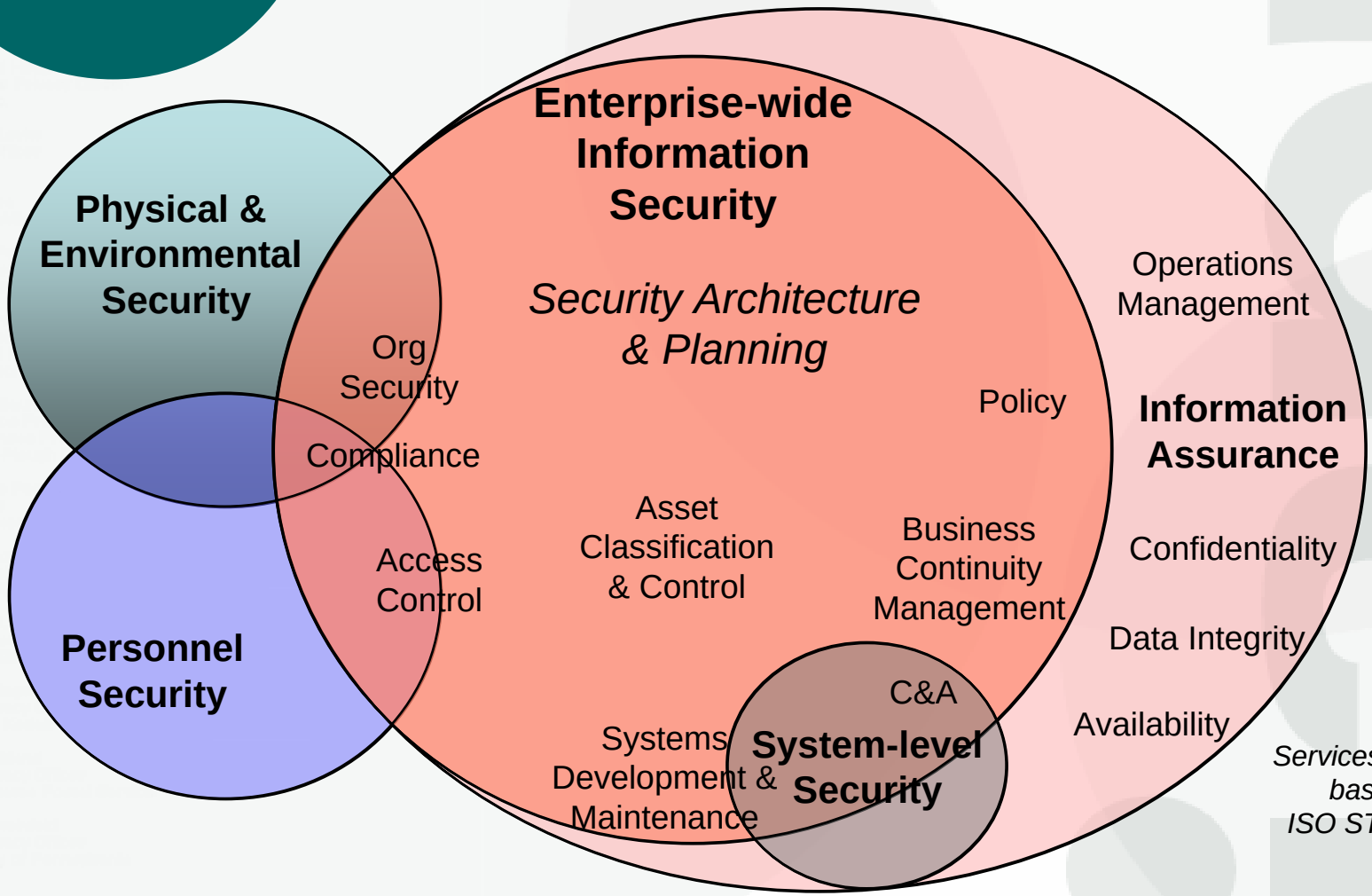
govmt laws

Federal Information Security Management Act (FISMA)

"Each Federal agency shall develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source…" **– Federal Information Security Management Act of 2002**

govmt laws

FISMA: System vs. Enterprise



Services identified based on ISO STD 17799

Prepared by The MITRE Corporation, 8-1-05

govmt laws

Open Meetings Laws

- Federal Advisory Committee Act (FACA)
  - Enacted to ensure that advice rendered to the executive branch is objective and accessible to the public
- Government in Sunshine Act
  - Enacted to ensure that collegial bodies within federal agencies do not have meetings and make decisions in secret
  - Prescribes procedures that an agency must follow to claim an exemption from an open meeting

Privacy Management

privacy mgmt

Agency Responsibilities

- OMB Circular A-130, Management of Federal Information Resources, Appendix 1: Federal Agency Responsibilities for Maintain Records About Individuals
  - Head of each agency is responsible for reports, reviewing training activities and violations
  - Dept. of Commerce
    - Issues information protection guidelines
  - Office of Personnel Management
    - Develops and maintains standards and procedures
    - Develops and conducts Privacy Act training programs
  - National Archives and Records Administration (NARA)
    - Issues instructions on format of notices and rule
  - Office of Management and Budget (OMB)
    - Issues guidelines and directives
    - Reviews reports

privacy mgmt

Key OMB Privacy-Related Memoranda

- OMB M-05-04, Policies for Federal Agency Websites
- OMB M-04-26, Personal Use Policies and "File Sharing" Technology
- OMB M-00-13, Privacy Policies and Data Collection on Federal Web Sites
- OMB M-99-18, Privacy Policies on Federal Web Sites

- OMB M-05-08, Designation of Senior Agency Officials for Privacy
- OMB M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002
- OMB M-01-05, Guidance on Inter-Agency Sharing of Personal Data – Protecting Personal privacy

privacy mgmt

Federal Agency Websites

- OMB M-05-04, Policies for Federal Agency Websites
  - Establish and maintain information dissemination product inventories, priorities, and schedules
  - Ensure information quality
  - Establish and enforce agency-wide linking policies
  - Establish and maintain communications with and state and local governments to ensure agency creates information dissemination products that meet their respective needs
  - Include a search function
  - Use approved domains
  - Implement security controls
  - Protect privacy
  - Maintain accessibility
  - Manage records

privacy mgmt

Use Policies and File Sharing

- OMB M-04-26, Personal Use Policies and "File Sharing" Technology
  - Details actions agencies must take to ensure appropriate use of certain technologies used for file sharing across networks
  - Use applies to controlled information, including personal information

privacy mgmt

Privacy Policies & Data Collection

- OMB M-00-13, Privacy Policies and Data Collection on Federal Web Sites
  - Agency must establish clear privacy policies for its web activities
  - Agencies can only use "cookies" or other automatic means of collecting information if they give clear notice of those activities, and
    - They must have a compelling need to gather the data on the site
    - They must have appropriate and publicly disclosed privacy safeguards for handling information derived from cookies

privacy mgmt

Federal Policies on Web Sites

- OMB M-99-18, Privacy Policies on Federal Web Sites
  - Add privacy policies to known, major entry points to sites and any web page where substantial PII is collected from the public
  - Policy must clearly inform visitors to the site:
    - What information is collected about individuals
    - Why it is collected
    - How it will be used
  - Guidance and Model Language for Federal Web Site Privacy Policies is an attachment

privacy mgmt

Functional Positions

- Chief Information Officer *(CIO)*
  - Advises agency head on information resource implications of strategic planning decisions
  - Advises agency head on design, development, & implementation of information resources
  - Actively participates in budget process in establishing investment priorities
  - Monitors compliance with policies, procedures, & guidance
- Chief Security Officer *(CSO)*
  - Responsible for protecting confidentiality, integrity, and availability of data

privacy mgmt

Functional Positions

- OMB M-05-08, Designation of Senior Agency Officials for Privacy
  - Responsibilities
    - Ensures agency's implementation of information privacy protections
    - Reviews agency's information privacy procedures
    - Performs central policy role within agency

Policy Enforcement

Multiple Policies

- Different organizations may have different privacy needs
- As a result, different agencies have their own policies, regulations, and guidance that they follow

Records Management

records management

Management Process

- Agencies will:
  - Ensure that records management programs provide adequate and proper documentation of activities
  - Ensure the ability to access records
  - Obtain approval of the Archivist of the U.S. for retention schedules
  - Follow guidance from the National Archives and records Administration (NARA)
  - Provide records management training and guidance to staff

records management

Management Process

- OMB M-01-05: Guidance on Inter-Agency Sharing of Personal Data – Protecting Personal Privacy
  - Notice
  - Consent, as appropriate
  - Redisclosure limitations
  - Accuracy
  - Security controls
  - Minimization
  - Accountability
  - Privacy Impact Assessments

Auditing & Compliance

policy
enforcement

Processes

- Organizations
  - Office of Management and Budget (OMB)
  - Inspector General (IG)
  - General Accounting Office (GAO)
- Assessments
  - Throughout the Data Lifecycle
  - Integral to the Privacy Program
- Audits
  - Planned

auditing & compliance

Workforce Hiring

- Office of Personnel Management (OPM)
  - Maintains the Personnel Management Manual (PMM)
- Background screening
  - Used by a number of agency to determine suitability of candidates
- Agencies must request written permission to gain access to financial and medical records

auditing & compliance

Reporting Obligations

- All
  - Equal Employment Opportunity Commission (EEOC)
  - Federal government is covered by:
    - Title VII of the Civil Rights Act (Title VII),
    - Age Discrimination in Employment Act (ADEA)
    - Equal Pay Act
  - Department of Health and Human Services: Office of Civil Rights (HHR-OCR)
  - Department of Justice

Q + A

Open Discussion: Reasonable post-session questions:

jmcewen@mitre.org

Office: (443) 695-1108

I would like to acknowledge the contributions by other MITRE Corporation employees in the development of this briefing:

Bruce Bakis
Richard Graubart
Vijay Rachamadugu
Stuart Shapiro
Bruce Sabol

IAPP Certification Promoting Privacy