New Guidance on Privacy Controls for the Federal Government

IAPP Global Privacy Summit 2012

March 9, 2012

Dr. Ron Ross
Computer Security Division, NIST

Martha Landesberg, J.D., CIPP/US
The Privacy Office, DHS
The Perfect Storm

- Explosive growth and aggressive use of information technology.
- Proliferation of information systems and networks with virtually unlimited connectivity.
- Increasing sophistication of threat including exponential growth rate in malware (malicious code).

Resulting in an increasing number of penetrations of information systems in the public and private sectors potentially affecting security and privacy...
The Threat Situation

Continuing serious cyber attacks on public and private sector information systems targeting key operations, assets, and individuals…

- Attacks are organized, disciplined, aggressive, and well resourced; many are extremely sophisticated.
- Adversaries are nation states, terrorist groups, criminals, hackers, and individuals or groups with hostile intentions.
- Effective deployment of malware causing significant exfiltration of sensitive information (e.g., intellectual property).
- Potential for disruption of critical systems and services.
Unconventional Threats
Affecting Security and Privacy

Connectivity

Complexity

Culture
Mainstreaming Security and Privacy

- Information security and privacy requirements must be considered *first order requirements* and are critical to mission and business success.

- An effective organization-wide information security and privacy programs help to ensure that security and privacy considerations are specifically addressed in the *enterprise architecture* for the organization and are integrated early into the *system development life cycle*.

- Use *Federal Segment Architecture Methodology* and FEA *Security and Privacy Profile* for implementation.
Mutually Supporting Objectives

- Enterprise Architecture
  - Standardization, consolidation, optimization.

- Information Security
  - Confidentiality, integrity, and availability of information processed, stored, and transmitted by information systems.

- Privacy
  - Confidentiality and integrity of personally identifiable information; collection of information (data minimization); use of information (sharing and disclosure concerns).

*Requires a disciplined, structured process that takes a holistic, organization-wide view...*
Information security and privacy, traditional societal values, are at greater risk today due to the ever increasing size of our digital footprint...
Enterprise-Wide Risk Management

- Multi-tiered Risk Management Approach
- Implemented by the Risk Executive Function
- Enterprise Architecture and SDLC Focus
- Information Security Architecture
- Flexible and Agile Implementation
- Threat Aware
Risk Management Process

Risk Framing

Assess

Respond

Monitor

Risk Framing

Risk Framing

Risk Framing

Risk Framing
Risk Management Framework

**Starting Point**

- **CATEGORIZE Information System**
  - Define criticality/sensitivity of information system according to potential worst-case, adverse impact to mission/business.

**Security Life Cycle**

- **SELECT Security Controls**
  - Select baseline security controls; apply tailoring guidance and supplement controls as needed based on risk assessment.

- **IMPLEMENT Security Controls**
  - Implement security controls within enterprise architecture using sound systems engineering practices; apply security configuration settings.

- **ASSESS Security Controls**
  - Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements for information system).

- **AUTHORIZE Information System**
  - Determine risk to organizational operations and assets, individuals, other organizations, and the Nation; if acceptable, authorize operation.

- **MONITOR Security Controls**
  - Continuously track changes to the information system that may affect security controls and reassess control effectiveness.
A new initiative to develop privacy controls for federal information systems and organizations...
Privacy Control Families

- Families are based upon the Fair Information Practice Principles (FIPPs)
- Use them to build privacy into new or modified:
  - Programs, research, pilots;
  - Information systems;
  - Technology (surveillance cameras, body imaging devices, data mining); and
  - Any other business-related activity that involves personally identifiable information (PII).
Applying Privacy Control Families
(1 of 2)

- Preliminary steps:
  - Identify the types of PII involved;
  - Identify the legal framework that applies; (Statutes, regulations, and policies that must be applied)
  - Map the data flows.
  - Law enforcement and intelligence programs and systems, particularly those that are classified, will require modifications in light of their legal and operational requirements.
Applying Privacy Control Families  
(2 of 2)

- Families are interrelated -- action taken in one family likely will affect the implementation of another.
- Families are not in any particular order and should be considered individually and as a whole.
- Families are iterative and must be revisited to determine the impact of changes to any particular family.
- Families must be analyzed and applied to each agency’s distinct mission, operation, and legal authorities and obligations.
Fair Information Practice Principles

- Transparency
- Individual Participation and Redress
- Purpose Specification
- Data Minimization and Retention
- Use Specification
- Data Quality and Integrity
- Security
- Accountability and Auditing
Privacy Control Families

- Authority and Purpose (AP)
- Accountability, Audit, and Risk Management (AR)
- Data Quality and Integrity (DI)
- Data Minimization and Retention (DM)
- Individual Participation and Redress (IP)
- Security (SE)
- Transparency (TR)
- Use Limitation (UL)
What do we achieve?
Benefits

- Well defined privacy controls that help demonstrate compliance with federal legislation and policies.
- Measurable and enforceable privacy requirements.
- Closer linkage to enterprise cyber security programs to provide a solid foundation for privacy.
- Enterprise-wide defense-in-depth for security and privacy.
- Security and privacy requirements traceability.
Defense-in-Depth

Links in the Security and Privacy Chain: Security and Privacy Controls

- Risk assessment
- Security planning, policies, procedures
- Configuration management and control
- Contingency planning
- Incident response planning
- Security awareness and training
- Security in acquisitions
- Physical and personnel security
- Security assessments and authorization
- Continuous monitoring
- Privacy protection

- Access control mechanisms
- Identification & authentication mechanisms (Biometrics, tokens, passwords)
- Audit mechanisms
- Encryption mechanisms
- Boundary and network protection devices (Firewalls, guards, routers, gateways)
- Intrusion protection/detection systems
- Security configuration settings
- Anti-viral, anti-spyware, anti-spam software
- Smart cards

Adversaries attack the weakest link...where is yours?
Defense-in-Breadth
Requirements Traceability

Legislation, Presidential Directives, OMB Policies
High Level, Generalized, Information Security and Privacy Requirements

Federal Information Processing Standards
FIPS 200: Minimum Information Security Requirements
FIPS 199: Security Categorization

Security and Privacy Controls
NIST Special Publication 800-53

Information Systems and Environments of Operation
Hardware, Firmware, Software, Facilities

Ground Zero

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
NIST Special Publication 800-53, Revision 3
*Recommended Security Controls for Federal Information Systems and Organizations*

*SP 800-53, Revision 4 – Appendix J: Privacy Control Catalog*

NIST Special Publication 800-53A, Revision 1
*Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*

*SP 800-53A, Revision 2 – Privacy Assessment Procedures*
Important Take Aways

- Developing new privacy controls in NIST SP 800-53.
- Creating stronger relationship between security and privacy groups within organizations.
- Providing a standardized approach for specifying privacy requirements within organizations.
- Building on strong foundation of cyber security to achieve a more comprehensive privacy program within organizations.
Contact Information

Dr. Ron Ross
ron.ross@nist.gov
Computer Security Division, NIST

Martha Landesberg, J.D., CIPP/US
martha.landesberg@hq.dhs.gov
The Privacy Office, DHS