Privacy and the Government: Major Issue Areas for Security Educators

Barbra Symonds

IBM

In response to data breaches across the government, the Office of Management and Budget (OMB) issued several memoranda on safeguarding PII

OMB M-06-15

May 22, 2006

- Restates Privacy Act Requirements
- Conduct Policy and Process Review
- Weaknesses identified must be included in agency Plan of Action and Milestones (POA&M)
- ***Remind Employees of Responsibilities for Safeguarding PII, the rules for acquiring and using such information, and the penalties for violating these rules***

OMB M-06-16

June 23, 2006

- Requires agencies to perform a technology assessment to ensure appropriate safeguards are in place, including:
  - Encryption standards
  - Allow remote access only with two-factor authentication
  - Use a “time-out” function for remote access and mobile devices
  - Log all computer-readable data extracts and time parameters
- System Review (NIST Checklist)

http://www.whitehouse.gov/omb/memoranda/2006.html

In response to data breaches across the government, the Office of Management and Budget (OMB) issued several memoranda on safeguarding PII

OMB M-06-19

July 12, 2006

- Revises current reporting requirements to require agencies to report **all** (electronic and physical form) incidents involving personally identifiable information (PII) to US-CERT **within one hour** of discovery (both suspected and confirmed breaches)
- Privacy and Security Funding Reminder

OMB M-06-20

July 17, 2006

- Identifies additional FISMA reporting instructions for privacy
- Results from the OMB M-06-15 review of policies and procedures for protecting PII must be included as an appendix
- Privacy updates must be submitted quarterly with the security updates to the President's Management Agenda scorecard

OMB M-07-16

May 22, 2007

- Publish a routine use for their systems of records allowing for the disclosure of information in the course of responding to a breach of federal data
- Review use of SSNs, eliminate unnecessary collection of SSNs, and participate in government-wide efforts to explore alternates to SSNs
- Each agency should develop a breach notification policy and plan

http://www.whitehouse.gov/omb/memoranda/2006.html

OMB M-07-16 requires agencies to develop and implement a breach notification policy within 120 days (from May 22, 2007) to prevent and manage PII breaches

AREA	DESCRIPTION	DUE DATE[1]	RQMT[2]
PRIVACY ACT REQUIRE-MENTS	Establish Rules of Conduct and penalties for non-compliance	120 DAYS	Existing
	Establish administrative, technical, and physical safeguards to ensure security/ confidentiality of PII	120 DAYS	Existing
	PII maintained within a Systems of Records must be maintained in accordance with the Privacy Act	120 DAYS	Existing
	Publish a routine use for their systems of records allowing for the disclosure of information in the course of responding to a breach of federal data	120 DAYS	NEW
SECURITY REQUIREMENTS	Categorize systems in accordance with FIPS 199	120 DAYS	Existing
	Implement minimum security requirements from FIPS 200	120 DAYS	Existing
	Conduct a Certification and Accreditation for information systems in accordance with NIST 800-37	120 DAYS	Existing
	Train employees initially and annually on their privacy and security responsibilities	120 DAYS	Existing
	Include privacy and security training in tele-work programs	120 DAYS	Existing
	Encrypt data on mobile computers	120 DAYS	Existing
	Two-Factor authentication for remote access	120 DAYS	Existing
	Use time-out function for remote access and mobile devices	120 DAYS	Existing
	Log all computer-readable data extracts from databases holding sensitive information and verify each extract, including whether sensitive data has been erased within 90 days or its use is still required	120 DAYS	Existing
	Employees with access to PII must sign an annual document describing responsibilities	120 DAYS	Existing
PRIVACY REQUIRE-MENTS	Review PII holdings for accuracy, completeness, and minimum necessary and report on implementation under FISMA and publish a review schedule	120 DAYS	NEW
	Review use of SSNs	120 DAYS	NEW
	Eliminate unnecessary collection of SSNs	18 MONTHS	NEW
	Participate in government-wide efforts to explore alternates to SSNs	120 DAYS	NEW

1) Days in the due date column represent approximate timeframes from the date of issuance of OMB M-07-16
2) Indicates whether the requirement (RQMT) is existing, new or modified

OMB M-07-16 requires agencies to develop and implement a breach notification policy within 120 days (from May 22, 2007) to prevent and manage PII breaches (continued)

AREA	DESCRIPTION	DUE DATE[1]	RQMT[2]
FISMA REQUIREMENTS	Implement procedures for detecting, reporting and responding to security incidents including mitigating risks associated with such incidents before substantial damage is done	120 DAYS	Existing
	Establish formal incident handling and response mechanisms	120 DAYS	Existing
	Instruct all employees in their roles and responsibilities regarding responding to incidents	120 DAYS	Existing
	Report all incidents involving PII to US-CERT (confirmed or suspected)	120 DAYS	Existing
	Categorize confirmed or suspected breaches of PII as Category 1 "Unauthorized Access or Any Incident Involving PII"	120 DAYS	NEW
INICDENT MANAGEMENT REQUIREMENTS	Each agency should develop a breach notification policy and plan	120 DAYS	NEW
	Establish an agency response team including the Program Manager of the program experiencing the breach, CIO, CPO or SAOP, Comms, Leg Affairs, General Counsel and Management Office (budget and procurement)	120 DAYS	NEW
	Develop and implement an appropriate policy outlining the rules of behavior and identifying consequences and corrective actions available for failure to follow these rules	120 DAYS	NEW

1) Days in the due date column represent approximate timeframes from the date of issuance of OMB M-07-16
2) Indicates whether the requirement (RQMT) is existing, new or modified

Privacy as a Business Enabler… Really!

- The Foundation for Strong Privacy is Data Governance and Information Management
  - What Purpose, What Information, What Sources, What Users
- Better Privacy Controls Improve Business Innovation and Enable Mission Success
  - Bake In Privacy Controls during IT Development, Minimize Risk Mitigation, Fail Well during a Breach Incident
- Fewer Paper Records Increase Individual Privacy
  - Paper records cannot be tracked for Need to Know, Least Privilege, and Audit Trail
- Privacy and Security Must Work Together
  - It's not an "Either/Or" conversation
- Awareness Training cannot and *should not* be a one-size-fits-all solution
  - Privacy and Information Protection must consider an organization's unique requirements, guiding principles and internal culture

De-Mystifying the Privacy Challenge: Provide Management with Simple Questions that Connect to the Underlying Privacy Principles

Issue to Address	Privacy Guideline
What is the business problem I am solving?	PURPOSE
Do I have the authority to collect and/or use this information?	AUTHORITY
Do I need to collect new information or use existing information differently to solve the problem?	ROUTINE USE, SYTEM OF RECORD NOTICE
Did I properly notify people that I will be collecting this information?	NOTICE AND CONSENT
Did I tell people why I need to collect the information?	NOTICE
Do the individuals have a choice to provide their data?	CHOICE, CONSENT, OPT-IN
Do the individuals have a path to request corrections to their data if they believe it is incorrect?	AMENDMENT
If I plan on sharing my information with another system/agency, do I know if the transfer of the data is authorized?	AUTHORITY, ROUTINE USE, COMPUTER MATCHING, MOU
If I am developing a new system, have I completed all the required privacy reviews?	PIA, SORN, INFORMATION COLLECTION