White Paper

Ensuring Personally Identifiable Information (PII) Security within U.S. Government Agencies

Using Data Management Tools to Ensure FISMA and Privacy Act Compliance

Embarcadero Technologies, with contributions from Ron Lewis, Senior Security Analyst, CDO Technologies

January 2009

Safeguarding personally identifiable information in the possession of the government and preventing its breach are essential to ensure the government retains the trust of the American public. This is a responsibility shared by officials accountable for administering operational and privacy and security programs, legal counsel, Agencies' Inspectors General and other law enforcement, and public and legislative affairs. It is also a function of applicable laws, such as the Federal Information Security Management Act of 2002 (FISMA) and the Privacy Act of 1974. (Clay Johnson III, Deputy Director for Management, Office of Management and Budget). [1]

REGULATORY OVERVIEW: PII AND THE FEDERAL GOVERNMENT

Many different organizations collect Personally Identifiable Information (PII), ranging from hospitals and banks to apartment complexes and utility companies. However, government agencies are in a uniquely challenging position—mandated to simultaneously widely disseminate and strongly protect the information they collect. How do Chief Information Officers (CIOs) and Senior Agency Officials for Privacy (SAOPs) balance the basic "considerations and assumptions" described in OMB Circular A-130 [2]:

- The Federal Government is the largest single producer, collector, consumer, and disseminator of information in the United States.
- Government information is a valuable national resource.
- The free flow of information between the government and the public is essential to a democratic society.
- The individual's right to privacy must be protected in Federal Government information activities involving personal information.

These statements, supported by regulations such as the Freedom of Information Act and FISMA, can appear to be in direct conflict with one another. For government agencies, most information should be disclosed by default; however, PII is the opposite—it should always be protected from disclosure except when legally mandated. This, of course, makes complete sense when you think about how you would like your own name and social security number treated by any public or private organization storing that information.

Over the past several years, the OMB has extended FISMA's annual reporting requirements to include specific reviews and reports on each agency's handling of PII. In general, the regulations, mandates, and related guidance boil down to (see Additional Information at the end of this paper for a complete list of current PII-related OMB memos).

1. Know what PII you collect and all the places it is stored and used
2. Reduce the collection and storage of PII wherever you can
3. Control access to PII no matter where or how it is accessed
4. Encrypt all PII both "at rest" (storage) and "in motion" (transmission)
5. Monitor for, alert on, and notify when a privacy breach occurs

---

[1] http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf
[2] http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html

Given the difficulty and expense of implementing these 5 simple statements, it may be helpful to tighten the scope of the problem by reviewing the OMB's definition of PII:
Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. (Clay Johnson III, Deputy Director for Management, Office of Management and Budget).[3]

And, of course all of this requires a good set of policies, procedures, and processes with strong oversight, reporting, and enforcement and it cannot be accomplished without the information security controls that make up the other 99 percent of FISMA compliance.

WHEN PII IS STORED IN A DATABASE: AUDITING, REPORTING, AND PROTECTING

Databases typically represent the largest concentration of sensitive information and, thus, are the primary target of hackers. Sometimes containing millions of records, compromised databases are the most damaging, even if the disclosure is accidental.

Unfortunately for those involved in the design, development, and administration of agency databases, there are almost no explicit references to databases in the FISMA and PII guidance provided by the OMB. Even the technical guidance provided by NIST is much more appropriate to process, application, and O/S controls. Examples are given below to highlight the difference between the two:

EXAMPLE 1 – GENERAL CONTROL

Agencies must now also review their current holdings of all personally identifiable information and ensure, to the maximum extent practicable, such holdings are accurate, relevant, timely, and complete, and reduce them to the minimum necessary for the proper performance of a documented agency function. Agency-specific implementation plans and progress updates regarding this review will be incorporated as requirements in agencies' annual report under FISMA. [4]

EXAMPLE 2 – DATABASE-SPECIFIC CONTROL

Agencies must log all computer-readable data extracts from databases holding sensitive information and verify each extract—including sensitive data—has been erased within 90 days or its use is still required. [5]

---

[3] http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf
[4] http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf
[5] http://www.whitehouse.gov/omb/memoranda/fy2006/m06-16.pdf

USING EMBARCADERO TOOLS

Several Embarcadero tools address the five basic PII protection fundamentals listed above. For a complete control-by-control list of how each product addresses relevant FISMA requirements (as mandated in FIPS 200 and further explained in NIST SP 800-53).

MANAGING CHANGE WITHIN YOUR DATABASES: CHANGE MANAGER

It is important that PII not be compromised as a result of general database configuration problems. Embarcadero® Change Manager™ allows agencies to establish Configuration Standards for Oracle, DB2 LUW, SQL Server, and Sybase databases and run compliance checks between these standards and agency databases on a regularly-scheduled basis. Change Manager is currently being used by many civilian and Department of Defense agencies for this and other purposes.

Change Manager is a mature and sophisticated product that has been in extensive use in government and the private sector for many years. Its uses span the development lifecycle, where it is commonly used to manage, report, and troubleshoot change across any database environment.

It also plays a role in auditing permissions, privileges, and access controls. Maintaining the principle of least privilege is considered a best practice, along with the practice of role-based security. Change Manager can report on changes to users, roles, or groups (including permission changes), and capture point-in-time snapshots of user, role, and permission settings, which can be automatically reported upon. Virtually any object definition—tables, stored procedures, views—can be captured and compared between points in time, providing a definitive historical record that can be used for roll-back, compliance investigation, reporting, or change alerting.

In addition, Change Manager can compare data sets either against a historical snapshot, against a mirrored database, or even against a different brand of database. This can be used to determine if any data had been changed in the event of a breach or to synchronize reference data across multiple databases. Agencies using this technology have experienced significant gains in productivity and capability for compliance-related activities.

FISMA / NIST 800-53 Categories: Access Control, Audit and Accountability, Configuration Management, System and Information Integrity

FINDING AND DOCUMENTING DATABASES WITH PII: ER/STUDIO

Complying with the Federal Information Management Act (FISMA) and automating the reporting process is something that challenges even the most advanced federal agencies. ER/Studio® provides the ability to identify, track, and categorize where sensitive data is stored. With a clear understanding of the data and how it is structured, Embarcadero addresses the

agencies' data documentation needs, allowing it to report on large quantities of data and metadata from disparate sources.

Through reverse- and forward-engineering, ER/Studio enables users to roll out privacy and regulatory tags to databases in development and existing production databases. This type of functionality is also repository-based, so users are able to conduct impact analysis or query an enterprise model for all data elements containing encrypted or secure data.

ER/Studio allows an agency to reverse engineer an existing environment, discover the PII in that legacy environment, tag the PII data elements as sensitive data per FISMA, standardize this across development and production environments, and perform automated annual reporting. Furthermore, using the tagging capability in ER/Studio, an agency can generate the real time reports required by FISMA, should a data compromise or breach be suspected.

The ER/Studio advanced meta-data management tool, ER/Studio Enterprise Portal, takes reporting a step further as a web-based query tool that provides real time reports on metadata information stored in the agency's data models. With a clear understanding of the data contained in agency databases, Embarcadero addresses agencies' PII documentation needs, allowing it to report on large quantities of data and metadata from disparate sources.

FISMA / NIST SP 800-53 Categories: Access Control, Planning, Risk Assessment, System & Services Acquisition

SECURING PII WITHIN DATABASES: DBARTISAN

A key component to preventing a data breach is to control access to databases. Complex environments with databases physically located all over the world, multiple database platforms, and incomplete or hard-to-use native tools make the process of creating user accounts, roles and permissions (as well as removing them) extremely difficult to manage.

DBArtisan provides a single console for managing security, performance, and availability across multiple database platforms simultaneously and managing users, roles, permissions, and passwords. Quickly and easily lock down inactive and terminated employee accounts or remove unnecessary components. You can also monitor on use of shared accounts and terminate sessions using those accounts, all from the same authorized, easy-to-use interface regardless of whether you are working on Oracle, SQL Server, Sybase, DB2, or MySQL.

This tool eases the creation of Standard Operating Procedures (SOPs) for day to day database management, as required by FISMA and simplifies the Trusted Facility Manual (TFM). All of the standard activities can be accomplished in a single, cross-platform tool with an easy to use interface.

FISMA / NIST 800-53 Categories: Access Control, Audit and Accountability, Personnel Security

VALIDATING DATABASE CONTROLS AND STREAMLINING PII STORAGE: DSAUDITOR

One of the biggest burdens of FISMA compliance is monitoring and reporting PII data access and usage. DSAuditor provides an automated means of generating the required FISMA reports documenting that PII is only being accessed by authorized users. It also provides a means of identifying and recording unauthorized access attempts so that system owners can proactively monitor for real world threats. DSAuditor is the only tool that provides a continuous automated means of validating database level control functionality at the point closest to the data (e.g., the database)—that is that the controls are operating as expected.

Agencies often get stuck housing more PII than necessary. DSAuditor shows which PII is actually being used, how frequently, by whom, and by which method the data is being accessed. DSAuditor can quickly identify dormant and rarely utilized PII data which enables Federal agencies to streamline PII storage and more effectively manage the PII assets.

CONCLUSION

Safeguarding personally identifiable information and remaining in compliance with government regulations is a difficult challenge made easier with database tools from Embarcadero Technologies.

For additional information on how Embarcadero can help you document and securely manage your databases, please visit www.embarcadero.com, or contact your local sales rep for more information, including the Embarcadero white paper: Mapping Embarcadero Products to FISMA Requirements.

ADDITIONAL INFORMATION

Federal Information Security Management Act of 2002	http://csrc.nist.gov/drivers/documents/FISMA-final.pdf
Health Insurance Portability and Accountability Act of 1996	http://www.cms.hhs.gov/HIPAAGenInfo/Downloads/HIPAALaw.pdf
Privacy Act of 1974	http://opm.gov/feddata/USC552a.txt

OMB PII GUIDANCE

Title	Description	URL
M-06-15: Safeguarding Personally Identifiable Information	Requires Senior Agency Official for Privacy to conduct a review of PII-related policies and procedures	http://www.whitehouse.gov/omb/memoranda/fy2006/m-06-15.pdf
M-06-16: Protection of Sensitive Agency Information	States required protections when PII cannot be protected by physical security (mobile devices, laptops, remote access)	http://www.whitehouse.gov/omb/memoranda/fy2006/m06-16.pdf
M-07-16: Safeguarding Against and Responding to the Breach of Personally Identifiable Information	Requires the development and implementation of a breach notification policy	http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf
M-07-19: FY 2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management	Extends 2007 FISMA reporting requirements to include an appendix specifically on agency meeting PII safeguards (the above memos, reduction in collection/holding of PII, enforcement policies)	http://www.whitehouse.gov/omb/memoranda/fy2007/m07-19.pdf
M-08-09: New FISMA Privacy Reporting Requirements for FY 2008	Identifies additional privacy reporting requirements that will be required for FISMA 2008 (internal reviews, summary of policies and advisories issued during the year, written complaints and how they were handled)	http://www.whitehouse.gov/omb/memoranda/fy2008/m08-09.pdf
M-08-21: FY 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management	Specifies 2008 FISMA reporting requirements (same categories as 2007 with some additional questions in the report template)	http://www.whitehouse.gov/omb/memoranda/fy2008/m08-21.pdf

NIST INFORMATION SECURITY GUIDE

FISMA Implementation Project	http://csrc.nist.gov/groups/SMA/fisma/index.html
Special Publications	http://csrc.nist.gov/publications/PubsSPs.html
FIPS 199	http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf
FIPS 200	http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

Embarcadero Technologies, Inc. is a leading provider of award-winning tools for application developers and database professionals so they can design systems right, build them faster and run them better, regardless of their platform or programming language. Ninety of the Fortune 100 and an active community of more than three million users worldwide rely on Embarcadero products to increase productivity, reduce costs, simplify change management and compliance and accelerate innovation. The company's flagship tools include: Embarcadero® Change Manager™, CodeGear™ RAD Studio, DBArtisan®, Delphi®, ER/Studio®, JBuilder® and Rapid SQL®. Founded in 1993, Embarcadero is headquartered in San Francisco, with offices located around the world. Embarcadero is online at www.embarcadero.com..