IDERA®

Security and Compliance Whitepaper

ENSURING PII SECURITY

Ensuring the Security of Personally Identifiable Information within U.S. Federal Government Agencies – Using Data Management Tools to Ensure FISMA and Privacy Act Compliance

INTRODUCTION

Safeguarding personally identifiable information (PII) in the possession of the government and preventing incidents and breaches are essential to ensure the federal agencies retain the trust of the American public. This is a responsibility shared by officials responsible for administering privacy and security programs, legal counsel, Agencies' Inspectors General and other law enforcement, as well as 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.

REGULATORY OVERVIEW: PII AND THE FEDERAL GOVERNMENT

Many different businesses and organizations collect 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), Chief Information Security Officers (CISOs), and Senior Agency Officials for Privacy (SAOPs) balance the "basic considerations and assumptions" described in the Office of Management and Budget (OMB) memoranda:

- 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 (FOIA) 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 private information such as name, address, and Social Security number to be 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:

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

Given the difficulty and expense of implementing these 5 statements, it may be helpful to tighten the scope of this challenge 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.

And, of course, all of this requires a good set of policies, procedures, and processes with strong oversight, reporting, and enforcement across all federal agencies. None of these can be accomplished without the core security controls that make up the majority of FISMA compliance.

The National Institute of Standards and Technology (NIST) created Special Publication (SP) 800-122 – Guide to Protecting the Confidentiality of Personally Identifiable Information – to further assist federal agencies in this area. As outlined in the publication:

> This document provides practical, context-based guidance for identifying PII and determining what level of protection is appropriate for each instance of PII. The document also suggests safeguards that may offer appropriate levels of protection for PII and provides recommendations for developing response plans for incidents involving PII.

NIST SP 800-122 is not a direct mandate from any government oversight agency or authority. However, it provides some real-world, common-sense solutions for identifying PII, analyzing its level of risk, and properly protecting it in order to meet the various federal requirements including that of OMB M-07-16: Safeguarding Against and Responding to the Breach of Personally Identifiable Information.

More recently, OMB released memorandum M-17-12: Preparing for and Responding to a Breach of Personally Identifiable Information. This memorandum contains a wealth of information including the following key areas of information security that are often lacking in federal agencies:

- Incident response planning
- Security awareness and training
- Dealing with contracts and contractors
- Risk analysis of the breach
- Breach reporting and notification
- Ongoing incident response testing

A core requirement of memorandum M-17-12 is regarding the SAOP's responsibilities associated with the Privacy Act's system of records notices (SORNs) during the incident response process:

> To appropriate agencies, entities, and persons when (1) [the agency] suspects or has confirmed that there has been a breach of the system of records, (2) [the agency] has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, [the agency] (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with [the agency's] efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

Federal agencies can gain a tremendous amount of insight and assistance into reasonable safeguards and proper incident response planning by adhering to these documents.

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

Databases typically represent the largest concentration of sensitive information and, thus, are a 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 minimal references to databases in the FISMA regulation as well as in the PII protection and incident response guidance provided by the OMB. Even the technical guidance provided by NIST is much more appropriate to process, application, and OS 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.

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.

USING IDERA TOOLS

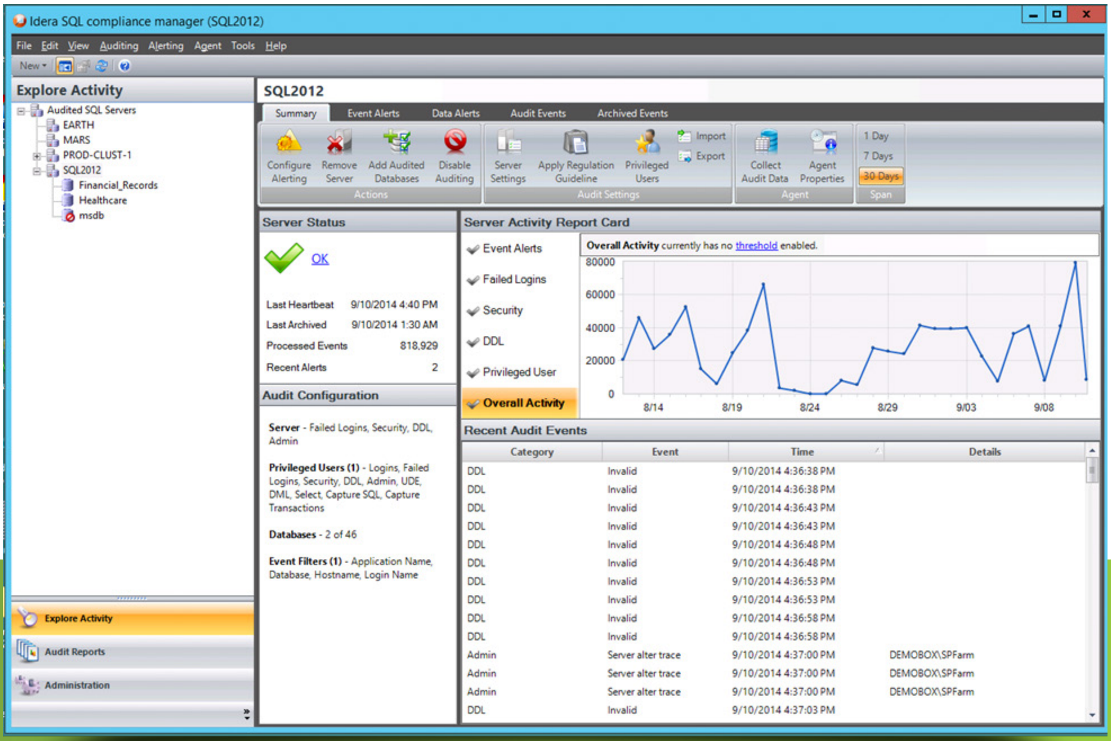
Several IDERA tools address the five basic PII protection fundamentals listed above. Refer to the notes at the bottom of each section below for what areas each product addresses in the relevant FISMA and OMB requirements (as mandated in FIPS 200 and further explained in NIST SP 800-53). It is also recommended to follow the guidelines and recommendations provided in the NIST SP 800-122 document to further implement best practices and ensure compliance. IDERA tools can help you with these tasks.

VALIDATING DATABASE CONTROLS: **SQL COMPLIANCE MANAGER**

One of the biggest burdens of FISMA compliance is monitoring and reporting PII data access and usage. IDERA SQL Compliance Manager provides an automated means of alerting and reporting on user activity for accessing PII. SQL Compliance Manager provides a continuous automated means of auditing database-level control functionality at the point closest to the data (e.g., the database), and generating reports to demonstrate that the controls are operating as expected.

Agencies often get stuck housing more PII than necessary. SQL Compliance Manager shows which PII is actually being used, how frequently, by whom, and by which method the data is being accessed. SQL Compliance Manager can quickly identify the location of sensitive data down to the column level, and audit and alert on that data, to more effectively manage the PII assets.

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



OK

Last Heartbeat 9/10/2014 4:40 PM
Last Archived 9/10/2014 1:30 AM
Processed Events 818,929
Recent Alerts 2

Server - Failed Logins, Security, DDL, Admin

Privileged Users (1) - Logins, Failed Logins, Security, DDL, Admin, UDE, DML, Select, Capture SQL, Capture Transactions

Databases - 2 of 46

Event Filters (1) - Application Name, Database, Hostname, Login Name

Overall Activity currently has no threshold enabled.

Category	Event	Time	Details
DDL	Invalid	9/10/2014 4:36:38 PM	
DDL	Invalid	9/10/2014 4:36:38 PM	
DDL	Invalid	9/10/2014 4:36:43 PM	
DDL	Invalid	9/10/2014 4:36:43 PM	
DDL	Invalid	9/10/2014 4:36:48 PM	
DDL	Invalid	9/10/2014 4:36:48 PM	
DDL	Invalid	9/10/2014 4:36:53 PM	
DDL	Invalid	9/10/2014 4:36:53 PM	
DDL	Invalid	9/10/2014 4:36:58 PM	
DDL	Invalid	9/10/2014 4:36:58 PM	
Admin	Server alter trace	9/10/2014 4:37:00 PM	DEMOBOX\SPFarm
Admin	Server alter trace	9/10/2014 4:37:00 PM	DEMOBOX\SPFarm
Admin	Server alter trace	9/10/2014 4:37:00 PM	DEMOBOX\SPFarm
DDL	Invalid	9/10/2014 4:37:03 PM	

FINDING AND DOCUMENTING DATABASES WITH PII: **ER/STUDIO**

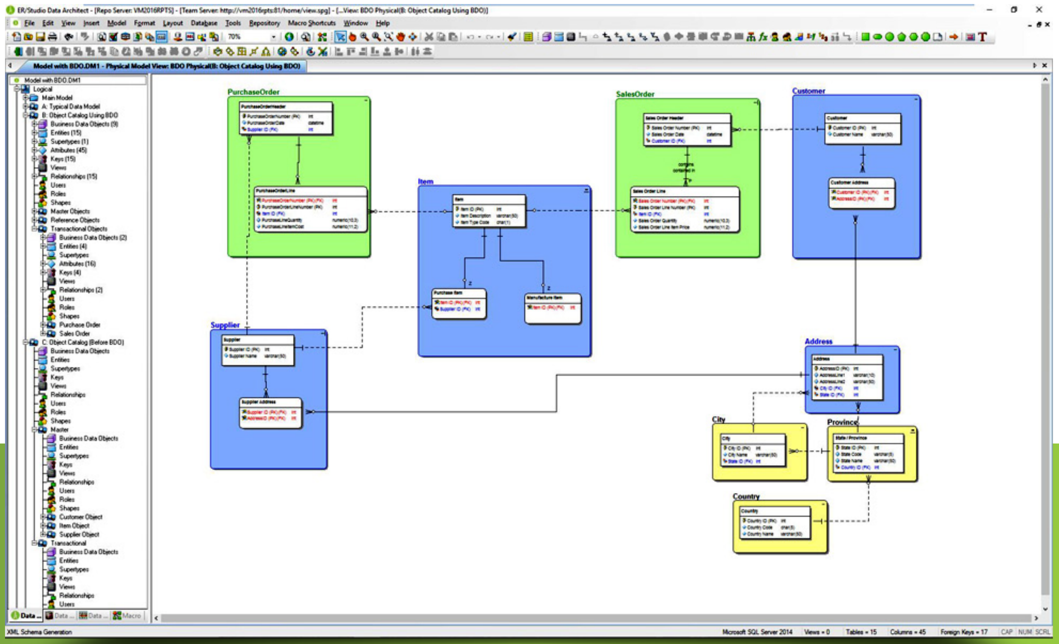
Complying with FISMA and automating the reporting process is something that challenges even the most advanced federal agencies. ER/Studio provides the ability to identify, track, and categorize where sensitive data is stored. With a clear understanding of the data and how it is structured, ER/Studio 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 Data Architect enables users to associate privacy and regulatory tags to objects contained in databases in development and existing production databases. These security parameters are saved as attachments at the entity and/or attribute level in the data dictionary. Users are able to 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 advanced metadata management tool, ER/Studio Team Server, takes reporting a step further with 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, ER/Studio addresses agencies' PII documentation needs, allowing them to report on large quantities of data and metadata from disparate sources.

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



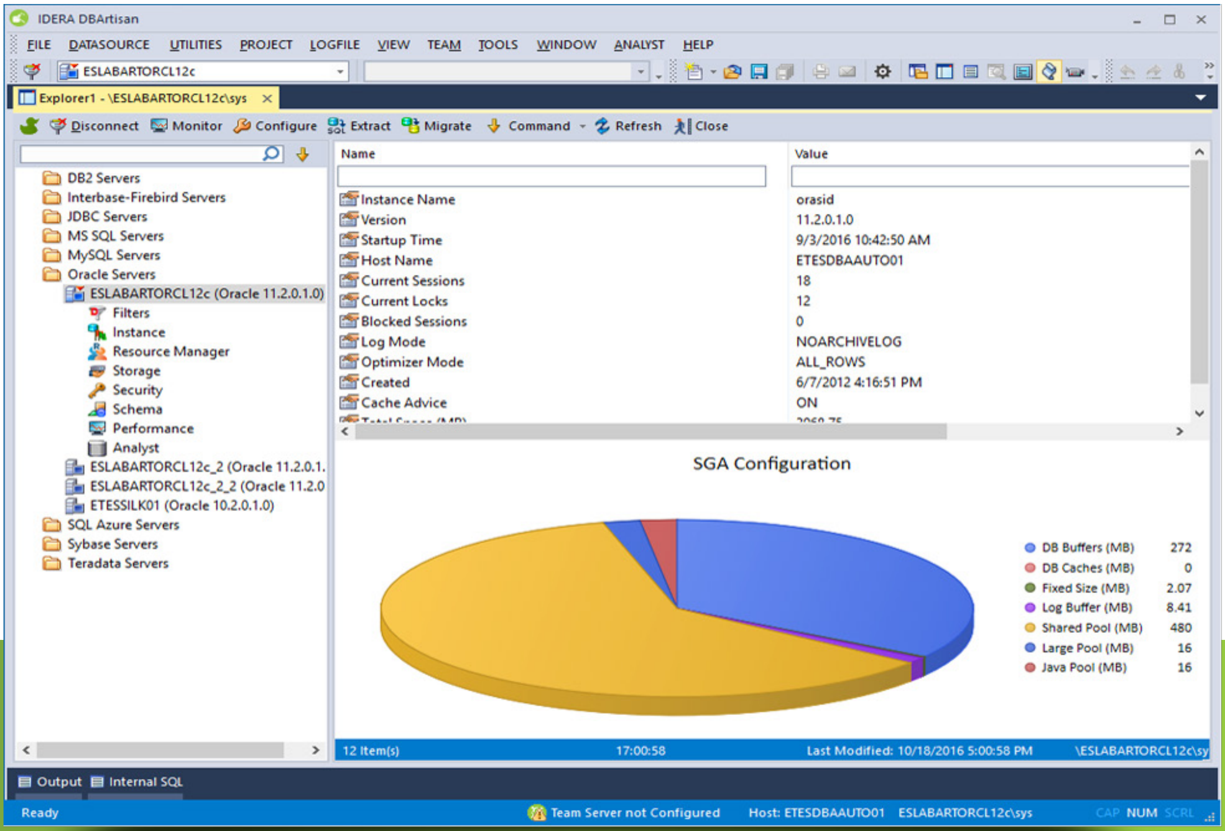
SECURING PII WITHIN DATABASES: **DBARTISAN**

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 managing user accounts, roles and permissions (as well as removing them) extremely difficult.

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*



Name	Value
Instance Name	orasid
Version	11.2.0.1.0
Startup Time	9/3/2016 10:42:50 AM
Host Name	ETESDBAAUTO01
Current Sessions	18
Current Locks	12
Blocked Sessions	0
Log Mode	NOARCHIVELOG
Optimizer Mode	ALL_ROWS
Created	6/7/2012 4:16:51 PM
Cache Advice	ON

12 Item(s) 17:00:58 Last Modified: 10/18/2016 5:00:58 PM \ESLABARTORCL12c\sy

Ready Team Server not Configured Host: ETESDBAAUTO01 ESLABARTORCL12c\sys

MANAGING CHANGE WITHIN YOUR DATABASES: **DB CHANGE MANAGER**

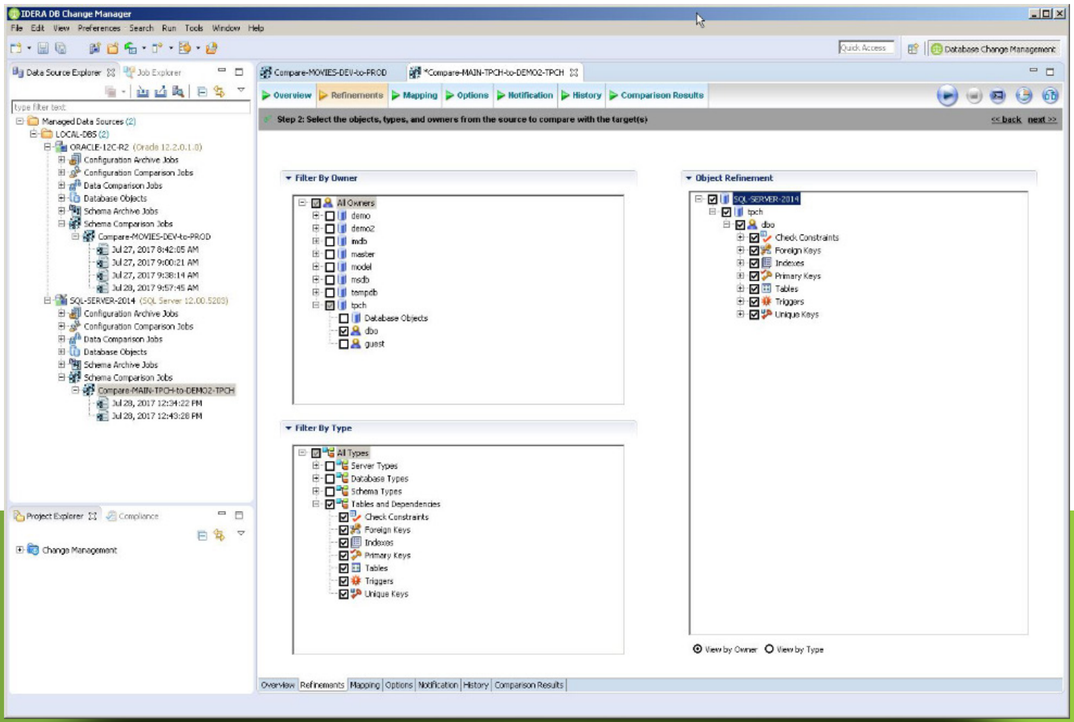
It is important that PII not be compromised as a result of general database configuration problems. IDERA DB Change Manager allows agencies to establish configuration standards for Oracle®, DB2® LUW®, SQL® Server, and Sybase® databases and run compliance checks between these standards and agency databases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

DB 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 changes across database environments.

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. DB 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, DB 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 was 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*



Step 2: Select the objects, types, and owners from the source to compare with the target(s)

CONCLUSION

Enabling federal agencies to properly safeguard PII and remain in compliance with government regulations is a difficult challenge made easier with database tools from Idera, Inc. Not only will the tools help safeguard PII from unauthorized exposure, they can be a tremendous asset during any necessary auditing, incident response, and breach investigation activities required of federal agencies.

For additional information on how Idera, Inc. can help you document and securely manage your databases, please visit www.idera.com.

ADDITIONAL RESOURCES

Federal Information Security Management Act of 2002

Privacy Act of 1974