Information Management
Data Sheet

Federal Government

IBM InfoSphere Guardium for federal information systems

Continuous monitoring to secure sensitive data and simplify SCAP compliance validation

Highlights

- Continuously monitor data activity to identify and block unauthorized access or changes, including those initiated by privileged users
- Automate assessment of database configurations to identify security vulnerabilities and suggest prioritized remedial actions
- Simplify and automate the implementation of controls to demonstrate compliance with the Federal Information Security Management Act, OMB, SP 800-53 and other mandates
- Maximize security and interoperability by supporting federal standards and best practices including DISA Database STIG vulnerability tests and CVE identifiers
- Monitor, aggregate and understand database entitlements
- Build security into big data environments such as Hadoop, InfoSphere BigInsights™ and NoSQL databases

The challenge of protecting data and validating compliance in federal agencies

According to a March 2013 article in Reuters, cyber attacks and cyber espionage have supplanted terrorism as the top security threat facing the United States.[1] Cleanup from cyberattacks cost an average of USD8.9 million annually.[2] The types of sensitive information targeted in attacks are typically stored in databases, and increasingly in big data repositories, such as Hadoop. As a result, the implementation of data security controls is becoming a very high priority. Furthermore, recent high profile events have called attention to the fact that these controls must also encompass the protection of sensitive data from insiders, particularly administrators who most often have unfettered access to all the data they manage.

> *"We know hackers steal peoples' identities and infiltrate private email. We know foreign countries and companies swipe our corporate secrets. Now our enemies are also seeking the ability to sabotage our power grid, our financial institutions, and our air traffic control systems."*[3]
>
> — President Obama, State of the Union address 2013

In response to the escalating threat to federal information systems, a variety of legislative and regulatory mandates now require federal agencies to implement controls to protect sensitive data. These include Federal Information Security Management Act (FISMA) and National Institute of Standards and Technology (NIST) standards such as Federal Information Processing Standards (FIPS)-200, Special Publications (SP) 800-53 and Security Content Automation Protocol (SCAP) (SP 800-126). Recognizing the real-time nature of current threats and the limited impact that static controls implemented in the past have had on attacks, most agencies are now moving aggressively to meet compliance requirements with capabilities that enable real-time detection and mitigation of security vulnerabilities.

> *"Agencies need to be able to continuously monitor security-related information from across the enterprise in a manageable and actionable way.…To do this, agencies need to automate security-related activities and acquire the tools that correlate and analyze security-related information."*[4]
>
> — Vivek Kundra, Federal CIO

Managing a database infrastructure to address these evolving security and compliance requirements is quite challenging for a variety of reasons, including:

- The shortage of resources with required database and security skills
- The number of systems to be secured, which can range up into the thousands in large agencies
- The highly dynamic nature of these systems, which undergo constant changes
- The need to implement consistent controls and reporting on systems from a variety of vendors
- The effort required to assemble and organize the wide variety of information required to demonstrate compliance with all applicable mandates
- The explosive amount of data speeding through the enterprise, which makes it challenging to understand what is sensitive and how to protect it
- The increasing adoption of big data platforms, such as Hadoop and NoSQL, which means that existing approaches might not scale to embrace new types of data sources

An integrated solution to meet growing data security and compliance requirements

IBM® InfoSphere® Guardium® offers a family of integrated modules for managing the entire data security and compliance life cycle (see Figure 1), irrespective of the size and mix of platforms. Supported platforms include Oracle Database, Microsoft SQL Server, Microsoft SharePoint, IBM DB2®, IBM Informix®, IBM VSAM, Sun MySQL, Sybase ASE, Sybase IQ, IBM PureData™, Teradata, PostgreSQL and FTP products. In addition, to address the challenges of security for big data, InfoSphere Guardium supports Hadoop-based systems, such as Cloudera and InfoSphere BigInsights™, as well as NoSQL databases.

Designed to provide ease of use and optimize the utilization of operational resources, InfoSphere Guardium provides a means of automating:

- The identification and classification of unregistered database instances, so that you can ensure controls are applied to all sensitive data, even in highly dynamic environments
- The continuous assessment of database infrastructures to identify, prioritize and accelerate remediation ofvulnerabilities that can be exploited to compromise sensitive data
- The real-time monitoring and enforcement of policies for sensitive data use
- The collection and reporting of audit information to validate compliance with a range of mandates

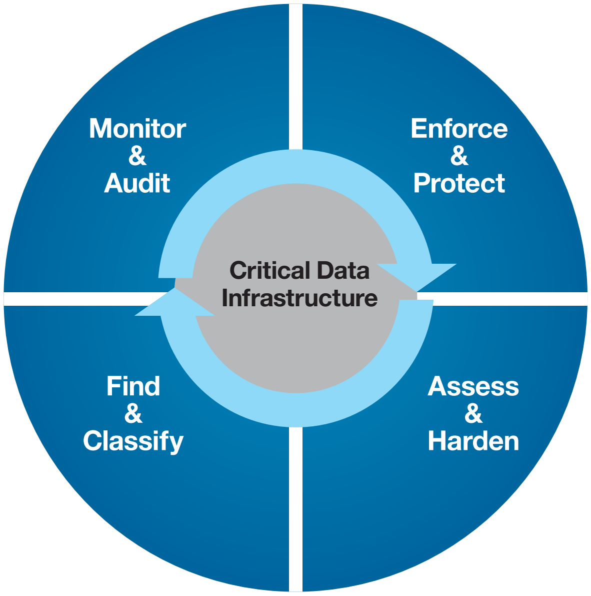
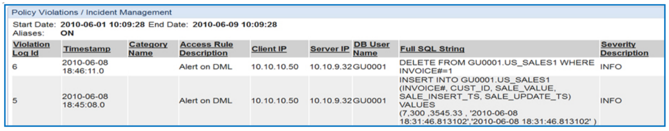


Figure 1: InfoSphere Guardium is a single integrated solution that simplifies all facets of data security and compliance

Continuous monitoring and policy enforcement to protect sensitive data

InfoSphere Guardium Data Activity Monitor is a simple, scalable solution for centralizing and automating the controls needed to protect all kinds of sensitive data in distributed heterogeneous environments, including big data environments. Lightweight host-based probes are installed on any database server with sensitive data, data, enabling all database transactions to be monitored in real time (see Figure 2) without changing database configurations or enabling resource-intensive native logging facilities. Hardware or software collector appliances gather monitored data from the probes, providing analysis, reporting and the secure audit trail required by mandates such as SP 800-53. If a transaction violates the policies configured by your agency (see Figure 3), a number of responses can be specified, ranging from alerting the security team to blocking the transaction in real time. For maximum scalability and flexibility, multiple tiers of appliances can be added to accommodate growth, enabling centralized monitoring and management of security policies agency wide.



Policy Violations / Incident Management

Start Date: **2010-06-01 10:09:28** End Date: **2010-06-09 10:09:28**
Aliases: **ON**

Violation Log Id	Timestamp	Category Name	Access Rule Description	Client IP	Server IP	DB User Name	Full SQL String	Severity Description
6	2010-06-08 18:46:11.0		Alert on DML	10.10.10.50	10.10.9.32	GU0001	DELETE FROM GU0001.US_SALES1 WHERE INVOICE#=1	INFO
5	2010-06-08 18:45:08.0		Alert on DML	10.10.10.50	10.10.9.32	GU0001	INSERT INTO GU0001.US_SALES1 (INVOICE#, CUST_ID, SALE_VALUE, SALE_INSERT_TS, SALE_UPDATE_TS) VALUES (7,300 ,3545.33 , '2010-06-08 18:31:46.813102','2010-06-08 18:31:46.813102')	INFO

Figure 3: InfoSphere Guardium continuously monitors data access in real time to detect policy violations and provides a range of actions for responding when any are detected

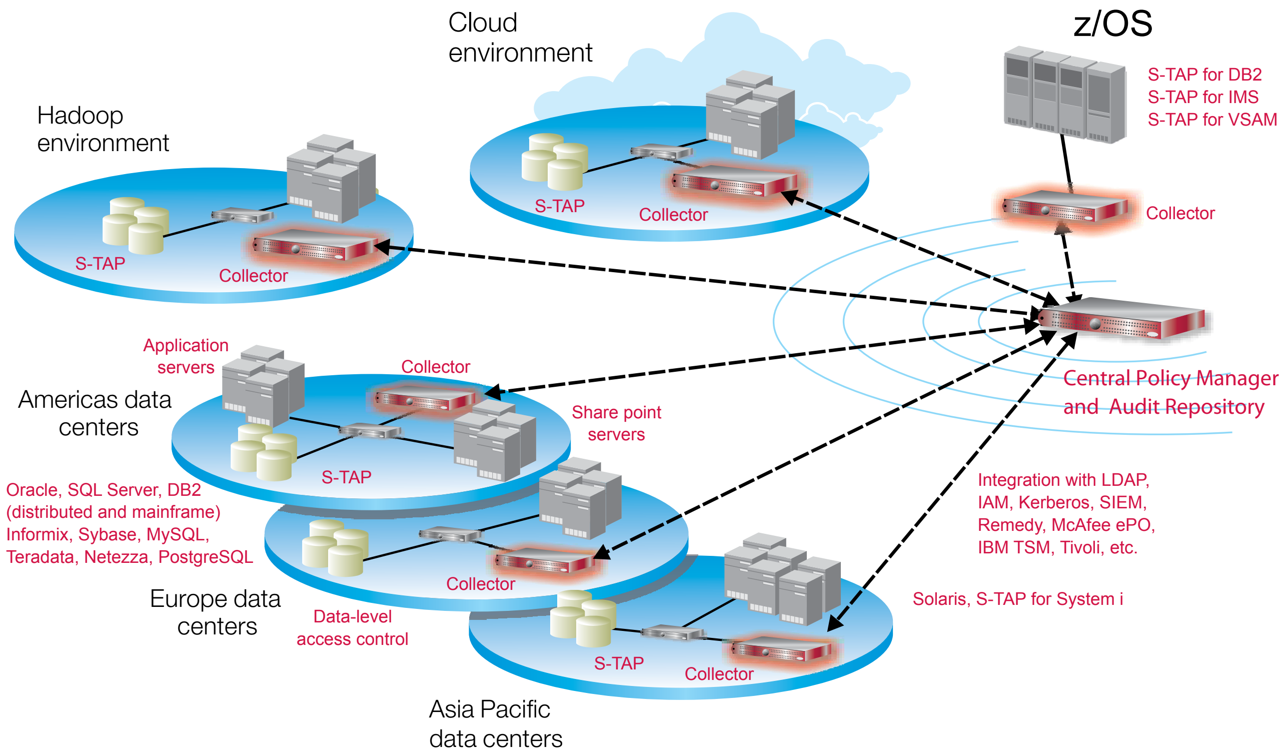

Cloud environment
z/OS
S-TAP for DB2
S-TAP for IMS
S-TAP for VSAM
Hadoop environment
S-TAP
Collector
S-TAP
Collector
Collector
Application servers
Collector
Americas data centers
Share point servers
Central Policy Manager and Audit Repository
S-TAP
Oracle, SQL Server, DB2 (distributed and mainframe) Informix, Sybase, MySQL, Teradata, Netezza, PostgreSQL
Integration with LDAP, IAM, Kerberos, SIEM, Remedy, McAfee ePO, IBM TSM, Tivoli, etc.
Collector
Solaris, S-TAP for System i
Europe data centers
Data-level access control
S-TAP
Collector
Asia Pacific data centers

Figure 2: The scalable InfoSphere Guardium architecture protects sensitive data in large and small environments with centralized aggregation of audit data and centralized management of security policies—agency wide

InfoSphere Guardium Entitlement Reports provide a simple means of aggregating, understanding and utilizing user rights information. You can eliminate the time-consuming and error-prone process of manually collecting and analyzing user rights information and ensure important security gaps are quickly identified, while reducing operational costs through automation. InfoSphere Guardium can be configured to scan all selected databases on a scheduled basis, automatically collecting information on user rights. The result is the ability to maximize sensitive data protection, minimize operational costs and ensure successful audits.

Key pre-defined Entitlement Reports include:

- Accounts with system privileges
- All system and administrative privileges, shown both by user and role
- Object privileges by user
- All objects with public access
- User privileges by object
- Roles granted to users and roles
- Grants and revocation of privileges
- Execute privileges by procedure

One of the biggest trends in federal information systems is the move to big data infrastructures. Big data environments help agencies process, analyze and derive maximum value from new data formats, as well as traditional structured formats, in real time. As big data environments ingest more data, agencies will face significant risks and threats to the repositories containing this data. Unique challenges of big data environments include:

- Schema-less distributed environments, where data from multiple sources can be joined and aggregated in arbitrary ways, make it challenging to establish access controls
- The nature of big data—high volume, variety and velocity—makes it difficult to ensure data integrity
- Aggregation of data from across the enterprise means sensitive data is in a repository
- Another data source to secure, and most existing data security and compliance approaches will not scale

InfoSphere Guardium is among the first to market to deliver security for data environments by monitoring big data activity from applications and users (both internal and external) in real time and taking action on policy violations. InfoSphere Guardium also reports on activities to fulfill compliance requirements and support forensic investigations.

Enhanced security with automated identification of software and configuration flaws

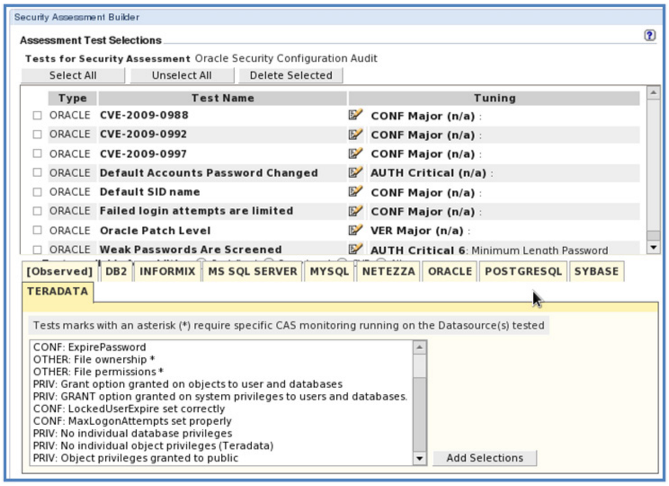
One interagency initiative to support improved real-time detection and mitigation of security vulnerabilities is the Information Security Automation Program. The objective of the program is to automate standards-based security configuration assessment and compliance reporting activities, including those related to database infrastructures. With automated and regular security assessments, agencies can evaluate the strength of their database environments, compare it with guidelines and measure improvements over time.

InfoSphere Guardium Database Vulnerability Assessment and Configuration Auditing System (CAS) modules combine to automate the following SCAP CVE, CCE and CPE functions:

- The ability to scan specified high-value database infrastructures on a schedule or on demand
- Comprehensive identification of database vulnerabilities (see Figure 4), such as missing patches, misconfigured privileges, weak passwords and default vendor accounts
- An extensive library of tests that uses industry-wide best practices including CIS benchmarks and the Defense Information Systems Agency Database Security Technical Guides (STIG)
- The capability to create custom tests to tailor vulnerability assessments to unique application environments
- Identification of changes to configuration files and other objects external to the database, such as the authentication or communications encryption settings, that can affect the security posture of your infrastructure
- A summary security health report card (Figure 5) and supporting details including specific issues identified, Common Vulnerability Scoring System (CVSS) scores, Common Vulnerability and Exposure (CVE) identifiers and concrete recommendations to strengthen database security
- Complete report generation and data export capabilities

To facilitate further use of the security information generated by InfoSphere Guardium, IBM supports the development of standards for the interchange of software flaw and security configuration information, such as SP 800-126.

With InfoSphere Guardium, you can continuously test your entire database environment, irrespective of the size and mix of platforms, to identify and prioritize the remediation of software and configuration flaws, while minimizing use of scarce technical resources.



Assessment Test Selections

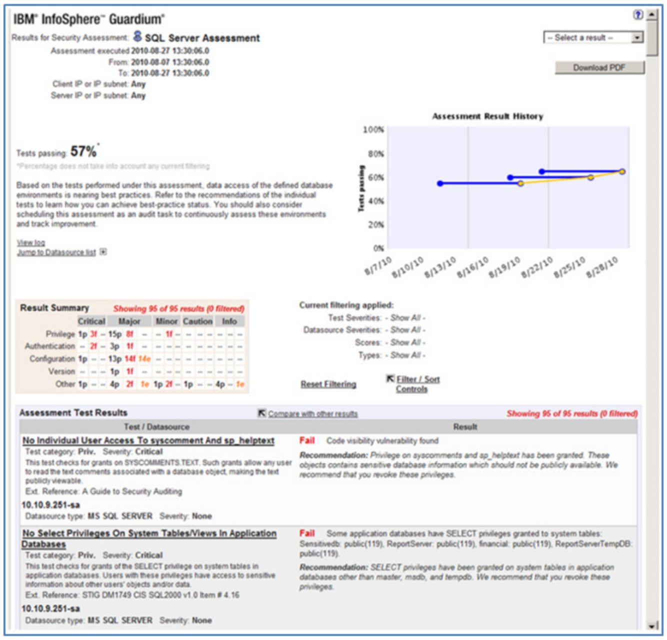
Tests for Security Assessment Oracle Security Configuration Audit

	Type	Test Name	Tuning
□	ORACLE	CVE-2009-0988	CONF Major (n/a) :
□	ORACLE	CVE-2009-0992	CONF Major (n/a) :
□	ORACLE	CVE-2009-0997	CONF Major (n/a) :
□	ORACLE	Default Accounts Password Changed	AUTH Critical (n/a) :
□	ORACLE	Default SID name	CONF Major (n/a) :
□	ORACLE	Failed login attempts are limited	CONF Major (n/a) :
□	ORACLE	Oracle Patch Level	VER Major (n/a) :
□	ORACLE	Weak Passwords Are Screened	AUTH Critical 6: Minimum Length Password

Tests marks with an asterisk (*) require specific CAS monitoring running on the Datasource(s) tested

CONF: ExpirePassword
OTHER: File ownership *
OTHER: File permissions *
PRIV: Grant option granted on objects to user and databases
PRIV: GRANT option granted on system privileges to users and databases.
CONF: LockedUserExpire set correctly
CONF: MaxLogonAttempts set properly
PRIV: No individual database privileges
PRIV: No individual object privileges (Teradata)
PRIV: Object privileges granted to public

Figure 4: InfoSphere Guardium automates the testing of heterogeneous database infrastructures to identify and accelerate remediation of software and configuration flaws



Results for Security Assessment: SQL Server Assessment
Assessment executed 2010-08-27 13:30:06.0
From: 2010-08-07 13:30:06.0
To: 2010-08-27 13:30:06.0
Client IP or IP subnet: Any
Server IP or IP subnet: Any

Tests passing: 57%*
*Percentage does not take into account any current filtering

Based on the tests performed under this assessment, data access of the defined database environments is nearing best practices. Refer to the recommendations of the individual tests to learn how you can achieve best-practice status. You should also consider scheduling this assessment as an audit task to continuously assess these environments and track improvement.

Result Summary Showing 95 of 95 results (0 filtered)

	Critical			Major			Minor			Caution			Info		
Privilege	1p	3f	–	15p	8f	–	–	1f	–	–	–	–	–	–	–
Authentication	–	2f	–	3p	1f	–	–	–	–	–	–	–	–	–	–
Configuration	1p	–	–	13p	14f	14e	–	–	–	–	–	–	–	–	–
Version	–	–	–	1p	1f	–	–	–	–	–	–	–	–	–	–
Other	1p	–	–	4p	2f	1e	1p	2f	–	1p	–	–	4p	–	1e

Current filtering applied:
Test Severities: - Show All -
Datasource Severities: - Show All -
Scores: - Show All -
Types: - Show All -

Assessment Test Results Showing 95 of 95 results (0 filtered)

Test / Datasource	Result
No Individual User Access To syscomment And sp_helptext Test category: Priv. Severity: Critical This test checks for grants on SYSCOMMENTS.TEXT. Such grants allow any user to read the text comments associated with a database object, making the text publicly viewable. Ext. Reference: A Guide to Security Auditing 10.10.9.251-sa Datasource type: MS SQL SERVER Severity: None	Fail Code visibility vulnerability found Recommendation: Privilege on syscomments and sp_helptext has been granted. These objects contains sensitive database information which should not be publicly available. We recommend that you revoke these privileges.
No Select Privileges On System Tables/Views In Application Databases Test category: Priv. Severity: Critical This test checks for grants of the SELECT privilege on system tables in application databases. Users with these privileges have access to sensitive information about other users' objects and/or data. Ext. Reference: STIG DM1749 CIS SQL2000 v1.0 Item # 4.16 10.10.9.251-sa Datasource type: MS SQL SERVER Severity: None	Fail Some application databases have SELECT privileges granted to system tables: Sensitivedb: public(119), ReportServer: public(119), financial: public(119), ReportServerTempDB: public(119). Recommendation: SELECT privileges have been granted on system tables in application databases other than master, msdb, and tempdb. We recommend that you revoke these privileges.

Figure 5: Prioritized results of vulnerability assessments are summarized in a security health report card, with supporting detail and recommendations on concrete steps to improve security provided

Automate and streamline compliance activities

InfoSphere Guardium provides an integrated workflow automation application to streamline compliance processes and ensure that action is taken to remediate all identified issues. The application automates report generation, distribution to stakeholders and management of electronic sign-offs and escalations. Compliance workflow automation results are stored in a tamper-proof repository along with audit data so agencies can demonstrate to auditors that all policy violations have been recorded and resolved in a timely manner and that audit data has not been altered. Figure 6 shows the modules that help demonstrate compliance to federal requirements. Compliance workflow automation eliminates costly, cumbersome, error-prone manual processes.

InfoSphere Guardium Module	Federal Requirement
Database Vulnerability Assessment	SP 800-53, CIS, DoD Database STIG, CVE and CVSS as specified in SP 800-126
Configuration Auditing System for OS level file monitoring	DoD Database STIG, CVE and CVSS as specified in SP 800-126
Configuration Auditing System for server configuration monitoring	DoD Database STIG, CVE and CVSS as specified in SP 800-126
Database Activity Monitor	Continuous monitoring

Figure 6: InfoSphere Guardium simplifies and automates the implementation of controls to demonstrate compliance with a variety of government specific mandates

Implemented by leading federal and state agencies

Leading federal and state agencies have selected the InfoSphere Guardium solution because it provides a simple, scalable means of securing a wide variety of sensitive data by means of continuous monitoring and assessment, while accommodating the need to simplify compliance validation processes. Customers include federal, civilian, defense and intelligence agencies. These include agencies with a focus on finance, social services, security and infrastructure management.

About InfoSphere Guardium

InfoSphere Guardium is the most widely used solution for preventing information leaks from data centers and ensuring the integrity of enterprise data. It is installed for more than 500 customers worldwide, including:

- Five of the top 5 global banks
- Four of the top 6 insurers
- Top government agencies
- Two of the top 3 retailers
- Twenty of the world's top communication service providers
- Two of the world's favorite beverage brands
- The most recognized name in personal computing
- A top 3 auto maker
- A top 3 aerospace company
- A leading supplier of business intelligence software

InfoSphere Guardium was the first solution to address the core data security gap by providing a scalable, cross-database management system enterprise platform that both protects databases in real time and automates the entire compliance auditing process. InfoSphere Guardium is also among the first to market with security solutions for big data environments.

InfoSphere Guardium is part of IBM InfoSphere, an integrated platform for defining, integrating, protecting and managing trusted information across your systems. The InfoSphere platform provides all the foundational building blocks of trusted information, including data integration, data warehousing, master data management and information governance, all integrated around a core of shared metadata and models. The portfolio is modular, so you can start anywhere and mix and match InfoSphere software building blocks with components from other vendors, or deploy multiple building blocks together for increased acceleration and value.

The InfoSphere platform provides an enterprise-class foundation for information-intensive projects, providing the performance, scalability, reliability and acceleration needed to simplify difficult challenges and deliver trusted information to your business faster.

For more information

To learn more about IBM InfoSphere Guardium, contact your IBM sales representative or visit: **ibm.com**/guardium

IBM Corporation
IBM Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
April 2013

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

[1] Hosenball, Mark and Patricia Zengerle. “Cyber attacks leading threat against U.S.: spy agencies.” Reuters. March 12, 2013.

[2] Messmer, Ellen. “Cyberattacks in U.S. cost an average $8.9 million annually to clean up, study says.” Network World. October 8, 2012.

[3] Abdullah, Halimah. “Watch where you click: International cyber attacks on the rise.” CNN. March 12, 2013.

[4] Office of Management and Budget, April 21, 2010 Memorandum for Heads of Executive Department and Agencies on FY2010 FISMA Reporting

Please Recycle