

CyberScope and Recent FISMA Guidance from OMB Create New Challenges for Federal Agencies and Considerations for Government Contractors

April 30, 2010

By Jim Graham, Senior Vice President, SecureIT

Overview

With the increase of advanced persistent threats combined with the need for cost savings, the Federal Government is undertaking a dramatic shift in its cybersecurity strategy and annual reporting. The Federal Information Security Management Act (FISMA) requires agencies to report quarterly and annually based on performance measures defined by the Office of Management and Budget (OMB). Until this year, this reporting typically consisted of reports from enterprise FISMA management systems supplemented with spreadsheets.

[Vivek Kundra, the CIO for the Federal Government, recently announced](#) the availability of the [CyberScope](#) system and updated [FISMA reporting guidance](#) for federal agencies. The performance measures were largely associated with system inventory and state of compliance with National Institute of Standards and Technology (NIST) Risk Management Framework implementation. OMB issued its annual guidance for FISMA reporting this year which introduced the

CyberScope application and specified new performance measures with live data feeds which CIOs must support beginning this year.

The purpose of this letter is to provide a perspective on this new guidance and highlight important aspects which impact planning and implementation of cybersecurity both from the perspective of Department and Agency CIOs and CISOs; commercial organizations and non-profit organizations that contract with the Federal government.

CyberScope

The CyberScope system is a web-based application used to collect data from each federal agency through live data feeds and data entry by agency personnel. The expectation is that most Departments will be able to leverage their internal security information management systems to supply the data required. Many departments have deployed or use government-wide applications of Cyber Security Assessment and Management (CSAM), Automated System Security Evaluation and Remediation Tracking System (ASSERT) or the approved product Trusted Agent FISMA (TAF) for enterprise

FISMA performance management. The objective is to put into place a more automated and frequent measurement of security performance and the information collected will continue to expand over time.

2010 FISMA Reporting Guidance

The FISMA was enacted in 2002 to improve information security within the Federal Government. Since its enactment, Federal agencies have been required to report progress annually to the OMB. OMB issues guidance to agencies annually adjusting it to gain insights on different aspects of security, oftentimes driven by security breaches which have recently occurred. Agencies have created inventories of their systems, tracked certification and accreditation (C&A) performance, and reported information regarding incident reporting statistics.

OMB has specified that Federal agencies that contract for services which involve processing Federal government data must appropriately specify security requirements in contracts. OMB ruled that FISMA is required in these instances thus requiring agencies to specify FISMA requirements, identify security impact level (FIPS PUB 199) and ensure the contractor meets these requirements.

There are supporters and detractors to FISMA. The major complaints by detractors are that FISMA requires production of reams of documentation which is costly and that FISMA performance measurement and methods do not accurately portray the security posture of the organization but rather measure the volume of documentation created. There have been a number of efforts by Congress, of which a couple of bills are currently circulating today, that will refocus FISMA to address its shortcomings and improve the quality and speed at which agencies can report their security compliance and posture.

On April 21, 2010, OMB issued its reporting guidance for this year. This guidance was coordinated through the Federal CIO (Vivek Kundra) and the Cybersecurity Coordinator (Howard Schmidt). As like earlier versions of this guidance, the memo provides supplemental guidance to agencies with areas of particular interest to OMB. However, unlike previous years, this guidance outlines new requirements for collection of information and the transmission of this information to OMB

via automated means. OMB states in that “Need to be able to continuously monitor security-related information from across the enterprise in a manageable and actionable way.” OMB goes on to state that in order to achieve continuous monitoring, “agencies need to automate security-related activities, to the extent possible, and acquire tools that correlate and analyze security-related information. Agencies need to develop automated risk models and apply them to the vulnerabilities and threats identified by security management tools.”

This guidance is in stark contrast to prior years which was primarily focused on an annual inventory update and collection of metrics aligned with the NIST Risk Management Framework (number of systems which completed C&A, number of systems which conducted annual CP testing, etc).

The new FISMA guidance from OMB involves a four tiered approach:

1. Data feeds directly from security management tools
2. Government-wide benchmarking on security posture
3. Agency-specific interviews
4. Office of Inspector General (OIG) reviews

All reporting will be required through the new CyberScope application (discussed later in this paper).

This guidance applies to all Executive Departments and Agencies. However, micro-agencies will only be required to supply a subset of this data through data entry versus data feeds

Data Feeds from Security Management Tools

What:

Data feeds will include summary information in the following areas for CIOs:

- Inventory
- Systems and Services
- Hardware
- Software
- External Connections
- Security Training

- Identity Management and Access

When:

- 3rd quarter of FY2010, agencies will be required to report on this new information.
- Agencies will continue to report on this information through the FY2010 annual reporting cycle.
- Beginning January 1, 2011, agencies will be required to report on this new information monthly.

OMB's expectation is that Departments and Independent Agencies should be able to leverage existing tools and their existing continuous monitoring programs to produce the data required and the frequency in which this data must be transmitted. If your Department or Agency is unable to provide direct feeds from your existing security management tools for all the required areas, your organization will need to supplement the data feeds with an Excel spreadsheet based on an OMB provided template to permit XML upload to CyberScope. OMB is currently working on the XML schema along with a roadmap for the development of this reporting structure.

Govt-wide Benchmarking of Security Posture

Similar to prior years, Department CIOs must complete and submit a written report based on annual reporting guidance issued by OMB which identifies the performance measures. The change this year is that these questions will be contained in the CyberScope applications. Agencies will complete their response online in CyberScope in lieu of transmission of a letter to OMB.

Agency-Specific Interviews

New this year, OMB intends to dispatch a team of "government security specialists" to conduct interviews with agency personnel. These interviews will focus on agency responses to questions for the Govt-wide benchmarking of security posture and examine the unique threats that the agency faces as a function of its mission. The result of these interviews will be included in the report to Congress.

OIG Reviews

Along with the requirements leveled on Federal CIOs in the FISMA annual reporting guidance from OMB, guidance is provided to the OIGs to aid in developing the scope of their annual audits. OIGs need to ascertain agency performance in the following areas:

- Certification and Accreditation
- Configuration Management
- Security Incident Management
- Security Training
- Remediation/Plans of Actions and Milestones
- Remote Access
- Identity Management
- Continuous Monitoring
- Contractor Oversight
- Contingency Planning

Implications to Government Agencies

CIO/CISOs must determine the present capabilities of their FISMA and security management system(s) to determine if they are currently collecting the data needed for the annual reporting as well as determine how this information will be provided to OMB. CIO/CISOs must review the new guidance to prepare their organization for upcoming reviews by the OIGs. A liaison function is suggested to increase efficiency, accuracy and reduce impact on operational personnel.

Implications to Corporations & Non-Profits

If your organization currently has or is planning on contracts with the Federal government which involve processing federal government data within your organization's IT or facility, you may soon (if not already) be subject to compliance with FISMA. Your organization will need to demonstrate that security controls are in place and may be required to furnish data regarding your security performance on the frequency and standard required by CyberScope. You will need to demonstrate you have the required components (System Security Plan, Security Assessment Report, and Plan of Action & Milestones) to support your assertion. Further, you may be audited by your federal customer's OIG as part of its agency annual FISMA reviews.

About the Author



Jim Graham is the Senior Vice President for Federal Programs at SecureIT. He has over 25 years of experience providing IT solutions and IT security professional services to Federal government agencies and commercial businesses. He has held technical and management leadership positions at McDonald Bradley, DOMAIN Technologies and TRW and is a Certified Information Systems Security Professional (CISSP). Jim is active in industry associations including [ACT/IAC](#) where he is the Vice Chair for Information Security and Privacy. Jim can be reached at jgraham@secureit.com.

trademarks of their respective owners. Information in this document is subject to change without notice.

About SecureIT

SecureIT helps private and public sector clients manage technology risks and implement secure and trusted information systems through effective practices in IT security and privacy. SecureIT provides services and solutions in the areas of Cybersecurity, Information Assurance, Governance & Compliance, IT Audit, and Security Training. SecureIT devises strategies and solutions to address the unique business needs and environments of our clients resulting in reduced risk and increased efficiency. Leveraging our knowledge and experience with industry regulations and standards, we assist our clients to overcome the challenges of compliance with FISMA, FISCAM, HIPAA, HITECH, Privacy Act, SOX, and PCI. Founded in 2001 and located in Reston, VA, SecureIT serves the U.S. Federal Government, Financial Services & Banking, Healthcare, Public, Private and Non-Profit organizations.



1902 Campus Commons Drive, Suite 100
Reston, VA 20191
info@secureit.com
www.secureit.com
703-464-7010

The SecureIT logo, and all page headers, footers and icons are trademarks or registered trademarks of SecureIT Consulting Group. Other company names or products mentioned are or may be