

# CyberScope and Tighter Cybersecurity Reporting Requirements: Are You Ready?



# CyberScope and Tighter Cybersecurity Reporting Requirements: Are You Ready?

## Contents

<b>Introduction</b> .....	<b>1</b>
<b>FISMA Requirements and Challenges for Agencies and Departments</b> .....	<b>1</b>
<b>Best Practices to Support CyberScope and FISMA</b> .....	<b>2</b>
<b>How Symantec Can Help</b> .....	<b>2</b>
<b>Summary</b> .....	<b>3</b>

# CyberScope and Tighter Cybersecurity Reporting Requirements: Are You Ready?

## Introduction

Federal Information Security Management Act (FISMA) standards designed to enhance the information security posture of agencies and departments have a significant impact on the methods and frequency of monitoring and reporting security-related information. According to a memorandum from the Office of Management and Budget (OMB) dated April 21, 2010, “Agencies need to be able to continuously monitor security-related information across the enterprise in a manageable and actionable way. Chief Information Officers (CIOs), Chief Information Security Officers (CISOs) and other agency management all need to have different levels of this information presented to them in ways that enable timely decision making. To do this, 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 management models and apply them to the vulnerabilities and threats identified by security management tools.”

A key component of these standards, CyberScope, is an interactive information collection tool designed to help agencies fulfill their IT security reporting requirements. In testimony presented to the Senate Homeland Security and Governmental Affairs Subcommittee on Federal Financial Management, Government Information, Federal Services and International Security, Federal CIO Vivek Kundra stated, “CyberScope’s extensive platform is the performance-based solution to years of inefficient and unsecured collection of agency security data.”

With FISMA reporting through CyberScope which began November 15, 2010 and compliance with monthly reporting commencing on January 1, 2011, agencies must act quickly. Can their current methods of monitoring and reporting support these FISMA requirements and allow them to leverage the CyberScope tool? If not, what process and tools should they consider incorporating in their security management programs?

## FISMA Requirements and Challenges for Agencies and Departments

Currently, to comply with existing FISMA standards most federal agencies email and submit hardcopies of individual spreadsheets compiled manually and with a breadth of disparate tools. The process is time consuming, labor intensive, unsecure, and—like all manual processes—it is subjective & subject to human error. Although the process satisfied previous requirements it was neither qualitative, continuous nor automated and therefore unable to support new guidelines.

In addition, security and compliance teams often lack real-time, comprehensive visibility into networks, assets, and the configurations for the enterprises they secure. Legacy tool-sets lack integration and standards capabilities such as support for the National Institute of Standards and Technology (NIST) Security Content Automation Protocol (SCAP) for continuous monitoring and information sharing per the most recent FISMA and OMB memorandum. The resulting information remained in silos and reporting challenges increase the risk of unknown security “gaps” such as rogue networks and devices and unauthorized software. Further, the ability to provide meaningful analysis and insight useful in determining the security posture of the federal government overall is severely hampered.

In order to meet the rigors of these FISMA mandates and leverage the CyberScope Web portal, agencies and departments need to instrument best practices and solutions to:

- Increase productivity through automation.

## CyberScope and Tighter Cybersecurity Reporting Requirements: Are You Ready?

- Integrate and orchestrate information security activities for infrastructure security visibility and compliance.
- Adopt regulatory or risk management frameworks with SCAP-validated tools that support NIST standards.
- Simplify operational and reporting activities for enterprise IT Risk Management from the operator to the CISO.

### Best Practices to Support CyberScope and FISMA

New best practices and solutions will allow agencies to shift millions of dollars now spent producing reports to acquiring automated systems and processes that will meet tighter security mandates and ultimately reduce the cost of FISMA compliance.

In order to streamline support for FISMA and facilitate the use of the CyberScope portal these new systems and processes must be designed to support the “Four A’s:”

- **Automated** - Move from manual and proprietary integrations to an automated system based on leveraging standards, for example SCAP-based metadata exchanges with CVE, CCE, CPE & CVSS.
- **Accurate** - Ensure accuracy based upon discovery and SCAP-based audit.
- **Asset-centric** - Built on an asset-centric data model to support robust reporting and compliance support as a by-product of security.
- **Audit** - Audit networks, end points, and operating systems for violations against internal policies, the US Government Configuration Baseline and Security Technical Implementation Guides (STIGS) to identify vulnerabilities, configuration problems, etc.

### How Symantec Can Help

Symantec™ Risk Automation Suite is ideally suited to meet these FISMA mandates and leverage the CyberScope tool. As the leading fully SCAP-validated enterprise class risk management solution, Symantec Risk Automation Suite helps agencies improve business processes and enhance enterprise visibility by automatically measuring IT and security compliance – within hours of installation. It does this by using and sharing specific SCAP standards to enable continuous, high-speed, discovery for driving vulnerability management, measurement, remediation, and policy compliance evaluation – across all existing assets and infrastructure solutions.

Symantec Risk Automation Suite also streamlines the traditionally complex and manual processes of risk management and compliance, putting the IT risk and security information at the fingertips of those who require it – from the security administrator to the CISO. Because the solution is fully integrated with existing third-party and Symantec solutions, agencies can benefit from SCAP-based integrations and data sharing while improving their overall return on investment in existing infrastructure tools.

Specific capabilities that provide out-of-the box support for the CyberScope portal include:

- Real-time Threat Analysis
- Asset Discovery
- Vulnerability Management
- Closed-loop Remediation Automation
- Configuration Management
- CyberScope Compliance Reporting - with full support for Lightweight Asset Summary Reporting (LASR)

## CyberScope and Tighter Cybersecurity Reporting Requirements: Are You Ready?

By taking an integrated and automated approach to IT risk and compliance management, Symantec Risk Automation Suite shortens windows of vulnerability, supports continuous compliance reporting, and reduces the cost of compliance and the complexities of enterprise risk management.

### **Summary**

Symantec has been at the forefront of guiding SCAP standards, and the Symantec Risk Automation Suite was one of the first SCAP NIST approved tools in the marketplace

With SCAP-validated methodology and standards, public sector agencies gain unprecedented visibility into and control over their IT environment. Users can quickly measure, remediate threats and risks, and continuously verify compliance with these FISMA requirements as well as an array of other standards.

With more than a decade of work with federal agencies, Symantec has developed a deep understanding of the unique challenges government agencies face and how to address these challenges.



## About Symantec

Symantec is a global leader in providing security, storage and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

[http://go.symantec.com/  
federalgovernment](http://go.symantec.com/federalgovernment)

Symantec US Public Sector  
Headquarters  
2350 Corporate Park Drive  
Suite 300  
Herndon, VA 20171  
+1 (703) 885 3563

Symantec helps organizations secure and manage their information-driven world with high availability, business continuity software, compliance risk management, and disaster recovery solutions.

Copyright © 2011 Symantec Corporation. All rights reserved. Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.  
2/2011 21177625