White Paper

Achieving FISMA Compliance through Security Information Management

netForensics®

Contents

Executive Summary 1

Introduction: Brief Overview of FISMA 1

The FISMA Challenge: Securing Federal Information and Assets 2

Security Information Management: The Foundation that Enables FISMA Compliance 3

The Case for Security Information Management 4

The netForensics Solution: Aligning with FISMA Objectives 4

Conclusions 5

References 6

netForensics®

Executive Summary

Enacted by the federal government in 2002, the Federal Information Security Management Act (FISMA) recognized the need to define a comprehensive framework for establishing and monitoring of security programs for federal agencies. By effectively managing risk, federal information and assets can be adequately protected.

According to Joshua Bolten, director of the Office of Management and Budget (OMB), which mandates FISMA reporting requirements, "The security of the federal government's information and information systems is a responsibility shared by every agency. The Administration's policy requires federal agencies to take a risk-based, cost-effective approach to secure their information and systems, identify and resolve current IT security weaknesses and risks, as well as protect against future vulnerabilities and threats." [1]

The importance of FISMA cannot be overemphasized—the task of maintaining the federal government's information infrastructure is critical. Yet FISMA compliance presents significant challenges for federal agencies, as well as for any organizations with information systems that deal with federal information. To be compliant, agencies are required to perform inventories of their IT assets, analyze security incidents, develop processes for reporting and monitoring security incidents, and conduct security awareness training. IT organizations need an effective approach to FISMA compliance that involves establishing an agency-wide, risk-based, and cost-effective information-security program.

Security information management (SIM) can enable federal agencies to meet FISMA regulatory compliance directives of accountability, as well as ongoing reporting policies and procedures. The U.S. Department of Labor Mine Safety and Health Administration (MSHA) and the U.S. Agency for International Development (USAID) implemented a security management solution to address their security management challenges, and ultimately meet FISMA regulatory compliance. In fact, by deploying netForensics' nFX Open Security Platform (nFX OSP) for SIM, both federal agencies recently received stellar marks on the FISMA scorecard issued by the House Government Reform Committee, affirming their ability to transform security-related information into actionable intelligence.

Properly implemented, a best-practices SIM solution gives federal agency management real-time visibility into information security-related risk and compliance data. Additionally, SIM can support the agency's broader corporate governance objectives.

Introduction: Brief Overview of FISMA

FISMA was signed into law in December 2002, as part of the Electronic Government Act. Repealing the Computer Security Act of 1987, FISMA was enacted to streamline—while at the same time strengthening—the requirements of its predecessor, the Government Information Security Reform Act (GISRA). Because FISMA compliance is a matter of national security, it is scrutinized at the highest level of government.

Governed by the National Institute of Standards and Technology (NIST), the Act applies to the information and information systems used by federal agencies, and also applies to any organizations, such as contractors and industry partners, that possess or use federal information. Thus, FISMA has a wider applicability than previous security laws. Under FISMA regulations, each federal agency must develop, document, and implement an

netForensics®

agency-wide information-security program.

To comply with FISMA, federal agencies must actively participate in the following:

- Develop a comprehensive security program.
- Ensure that appropriate officials are assigned security responsibility.
- Review periodically the security controls in their information systems.
- Engage in annual security reporting to the OMB.
- Provide internal security awareness training.
- Follow guidelines issued by NIST for information security controls.

Within the FISMA framework, the federal government is able to objectively measure IT security progress and identifiable problems. This information is essential to ensuring that priorities are placed on remediation efforts and IT resources, resulting in the timely resolution of IT security weaknesses.

The FISMA Challenge: Securing Federal Information and Assets

- Risk Assessment — The complying organization must use an approach to risk assessment that considers historical, real-time, and potential vulnerabilities, while enabling rapid action to prevent historical threats from occurring. Risks must be identified based on visibility into the security devices or controls in place, as well as the underlying, internal applications and data that those controls are protecting. Policies must be assessed and infrastructures must be hardened to ensure that past threats do not recur. Quick, decisive action must be taken when real threats do occur, and those need to be effectively separated from false-positives. Vulnerabilities must be proactively patched against the most critical systems. Finally, progress in these areas must be demonstrated against an acceptable baseline.
- Incidence Response — Complying organizations must define a process for incidence response as part of a comprehensive approach to FISMA compliance. Acceptable thresholds for responding must be identified, the chosen incidence response must be process followed, and the process thoroughly documented to prove adherence and assess the response. The incidence response process must illustrate that reasonable action was taken before systems were compromised. In the best-case scenario, the process should be operationalized through a workflow-based solution.
- Intrusion Detection System and Tools — Inherent in the network, complying organizations need a powerful attack detection and prevention capability, for both common and unique attacks. In addition to detecting intrusions, such intrusions, as well as how the system responds to those intrusions, must be thoroughly detailed in reports.
- Malicious Code Protection — Complying organizations must prevent malware from compromising data in critical systems, and bar access to confidential or classified information. Controls must be implemented to prevent malware, and in the event that those controls are compromised, quick detection and decisive action to eradicate it is needed. Additionally, controls must be demonstrated, and any shortcomings inherent in those controls should be identifiable.
- Individual Identification and Authentication — Agencies need to closely and

netForensics®

thoroughly monitor network access violations, such as repeated failed login attempts, with an effective identity-management system and network admission-control program. A system should be implemented that provides real-time visibility, and enables adequate enforcement of the admission control policies, especially when alerts surface.

- Monitor Change Activity — All system status and configuration changes, as well as security infrastructure modifications, must be detectable, with an implemented process for reporting on them.
- Logging and Audit Controls — To monitor for malware and to demonstrate that intrusion detection is functioning properly, agencies need a correlation technology that encompasses all network security devices, applications, and databases. To log an audit, an architecture should reliably collect the data and ensure it is readily available at all times.
- Supervision and Review — With a comprehensive reporting structure in place, agencies must implement processes and policies for the timely and thorough review of all reporting outcomes. These reporting processes must also include the steps to take given the various potential reporting results.

Security Information Management: The Foundation that Enables FISMA Compliance

Federal regulations do not dictate the particular technologies that a company must employ to fulfill compliance obligations. Yet the federal government is aware that technology can assist in ensuring compliance. The Act in fact states that the federal government:

> *"…acknowledges that commercially developed information security products offer advanced, dynamic, robust, and effective information security solutions, reflecting market solutions for the protection of critical information infrastructures important to the national defense and economic security of the nation that are designed, built, and operated by the private sector."* [2]

A comprehensive and specific approach to meeting compliance with FISMA requirements must start with leveraging the right security management solution—one that enables real-time monitoring and historical, on-the-fly reporting. But technology alone is not the answer. An in-depth approach that integrates existing assets—including people, processes, and policies—with technology is the most viable means to successfully attaining compliance.

Assuming the following responsibilities to prove diligence in managing information security risk helps organizations meet FISMA requirements, as well as those of other privacy and security regulations:

- Define a policy-driven security management program that can be incorporated early on into business processes — Identify the people and technology controls needed to satisfy the organization's security mission and ensure compliance. Also, ensure that security initiatives are integrated into business processes at their onset, rather than after the fact.
- Validate security controls — Provide for the monitoring and reporting of controls on human actions and decisions, process controls, and information technology controls.
- Implement a risk management approach to information security — Comprise active

netForensics®

monitoring of risk as defined and measured by key control indicators (KCIs) and key risk indicators (KRIs), correlating the relative value of information assets, the threats to the confidentiality, integrity, and availability of the assets, and the vulnerability of the systems and architecture that store and carry the assets.

- Demonstrate due diligence in the application of internal controls — Create a link between the security infrastructure and policy by capturing all security events from all network hosts, devices, and assets in an auditable database.
- Develop and implement an effective security-incident management process — Demonstrate that the proper steps were taken to correct systems and adjust policy if a non-compliant situation is identified.
- Enable reporting that can help demonstrate compliance — Demonstrate the ongoing security of compliance-related assets over a period of time, recreating the organization's security posture in the event of an audit, and enabling security performance management against metrics that can be leveraged for corporate governance initiatives.
- Establish capabilities for archiving and data preservation — Preserve near-term and long-term data in its purest form for forensics and evidentiary presentation.

By implementing effective, comprehensive policies and procedures for establishing accountability and consistent reporting practices, federal agencies can successfully meet FISMA regulatory compliance directives.

The Case for Security Information Management

To better respond to security threats, maintain compliant operations, and ensure the continuity of key business processes, federal agencies are turning to SIM solutions, and meeting FISMA requirements in the process. The U.S. Department of Labor Mine Safety and Health Administration identified the need for increased visibility to successfully meet FISMA challenges, and chose to align its technology initiatives with agency business needs. By implementing a security management solution, the Administration was able to correlate security events across multiple data sources, identify and prioritize real threats and risks, and demonstrate the ability to immediately apply the appropriate response.

The U.S. Agency for International Development employed a security management platform to meet its mandated FISMA objectives. The Agency leveraged the platform to collect and correlate security events from different vendor technologies and help measure the organization's overall risk and security posture.

For both agencies, nFX OSP enabled, and continues to enable, high marks on FISMA's annual Federal Computer Security Report Card. The annual scorecard shows to what degree agencies meet the mandates of FISMA.

The netForensics Solution: Aligning with FISMA Objectives

netForensics enables an efficient strategy for examining the adequacy and effectiveness of information security policies, procedures, and practices. nFX OSP automates the collection and correlation of the immense volumes of data created through security initiatives. The platform also provides periodic assessments of the risk and degree of harm that could result from unauthorized access, modifications, or destruction to information and information systems that support the operations and assets of the

netForensics®

agency, as required by FISMA.

More specifically, nFX OSP provides federal agencies the following tools and technologies to meet FISMA requirements:

- Risk assessment based on asset value, threats, and vulnerabilities.
- Incident-resolution management, integrating incidence response processes with existing enterprise workflow systems, and thus enabling accelerated incidence response through its collaborative approach.
- Compliance asset dashboards that provide real-time monitoring of the status of an organization's security posture at the network, asset, and business unit levels.
- Embedded knowledge base that provides guidance in analyzing, documenting, and reporting on security issues, including newly discovered vulnerabilities, malware, and vendor-specific vulnerability data.
- Strong correlation of intrusion-detection system events, including vulnerability correlation, statistical correlation, historical correlation, and rules correlation.
- Security operations performance measurement, with reports that focus on vulnerability, threat, and incidence response for all compliance-related assets in the enterprise.
- Detection and reporting on viruses, worms, and other malicious code; on all system status and configuration changes; and on privilege and authorization changes.
- Centralized application and device monitoring tool, enabling comprehensive collection, correlation, analysis, reporting, and retention of audit events from disparate applications, security devices, network devices, servers, and desktops, thus transforming data into actionable intelligence.
- A highly scalable and redundant security architecture that grows as organizations grow, and changes as business needs change.

Using these tools and technologies, federal IT organizations can effectively manage information security risk, and consequently demonstrate FISMA compliance.

Conclusion

FISMA requirements have intensified the need for federal government agencies to improve the security of IT systems, applications, and data. By presenting a baseline of requirements for government agencies, FISMA calls for using information-security best practices of risk and vulnerability measurement to ensure the integrity, confidentiality, and availability of federal information systems. Through FISMA-related efforts, agencies can help strengthen the protection of information assets that are vital to national security.

A fully implemented SIM solution like nFX OSP, along with alignment of human, process, and information controls, enables federal agencies to meet FISMA objectives. By leveraging existing technology and tools, federal agencies can identify, assess, and report on security-related issues, information, and events, and can ultimately provide tangible evidence of their efforts.

References

1. Memorandum for Heads of Executive Departments and Agencies: Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT

netForensics®

Security Reporting, Executive Office of the President, Office of Management and Budget, Joshua B. Bolten, Director, Washington, D.C., August 6, 2003.

2. Federal Information Security Management Act of 2002, Public Law 107-347, USC 44 Chapter 35, Subchapter III Information Security.

About netForensics

netForensics transforms all security related information into actionable intelligence, enabling more than 450 enterprises and government agencies to better respond to security threats, maintain compliant operations, and ensure the continuity of key business processes.

By harnessing the power of our award-winning Security Information Management platform that manages more security events at more organizations than any other product in the marketplace, we help customers deliver security management solutions that rely on the availability of timely and relevant information security information.

We facilitate these actionable security intelligence (ASI) solutions by rationalizing security information from strategic applications and critical compliance-related assets, as well as the perimeter devices that protect them. ASI solutions make this information available to technology domains and users within the security organization and beyond — by unifying network and security organizations, while supporting IT governance, enterprise compliance, and risk management initiatives.

200 Metroplex Drive • Edison, NJ 08817 • p 732.393.6000 • f 732.393.6090
www.netforensics.com • info@netforensics.com

netForensics®

netForensics, the netForensics logo, nFX, and nFXpert are trademarks of netForensics, Inc. Other third-party trademarks are the property of their respective owners.
© 2006 netForensics,Inc. All Rights Reserved.