

FISMA Compliance

A Holistic Approach to FISMA and Information Security

Copyright© 2006 Internet Security Systems, Inc. All rights reserved worldwide

 **INTERNET | SECURITY | SYSTEMS®**

Ahead of the threat.™

Table of Contents

EXECUTIVE SUMMARY	1
FISMA OVERVIEW	2
AGENCY CHALLENGES	3
THE ISS APPROACH TO FISMA COMPLIANCE	4
Overview	4
ISS FISMA Compliance Solution	5
<i>Assessment</i>	5
<i>Remediation</i>	6
<i>Audit</i>	7
SUMMARY AND CONCLUSIONS	8

EXECUTIVE SUMMARY

Threats and attacks against information systems are on the rise. Internet Security Systems (ISS) and other security companies are now identifying more than 150 new viruses, Trojans, bots and vulnerabilities each week. Attacks launched by dangerous adversaries are targeting information systems globally, including federal systems, to inflict irreparable damage and ultimately threaten our nation's security. As a result, the Federal Information Security Management Act (FISMA) was passed to ensure the protection of the nation's critical infrastructure against vulnerabilities that threaten economic and national security. FISMA provides a framework for developing, implementing, monitoring and reporting on an agency's information security program.

Protecting the nation's infrastructure, sustaining a secure environment against new threats and complying with complex and evolving regulatory requirements pose many challenges for agencies. While progress has been made in identifying and addressing agency security weaknesses, deficiencies continue to exist in security policy, procedures and practices. Maintaining an effective, compliant environment goes beyond periodic audits, paperwork and reporting. It requires a holistic strategy and approach to improving security posture and compliance.

This white paper provides an overview of the Federal Information Security Management Act legislation and discusses how ISS strategic approach to developing and maintaining an enterprise-wide security infrastructure best addresses FISMA requirements and continuous security improvements.

FISMA OVERVIEW

The Federal Information Security Management Act was passed in 2002 as framework to manage risk and ensure the confidentiality, availability and integrity of federal information and information systems. The Act assigns specific development, management, oversight and reporting responsibilities to two federal agencies, the National Institute of Standards and Technology (NIST) and the Office of Management and Budget (OMB).

Federal Information Security Management Act (FISMA)

FISMA provides a framework for ensuring the protection of Government information, operations and assets. The legislation requires agency officials to implement policies, procedures and practices to strengthen information security and reduce security risks. FISMA compliance requires agencies to:

- *Develop an agency-wide security program*
- *Implement and adhere to security configuration standards developed by NIST*
- *Identify and resolve risks*
- *Perform ongoing assessment and testing*
- *Conduct annual reviews on the effectiveness of the agency's information security and privacy programs and report the results to OMB annually*

In order to provide a framework to manage and measure agency security and risk, FISMA tasked NIST with the development of standards and guidelines for selecting, categorizing and assessing information systems. The table below shows the basic NIST framework for FISMA.

NIST STANDARDS AND GUIDELINES FOR MANAGING ENTERPRISE RISK AND FISMA COMPLIANCE		
PROCESS	GUIDELINE	
Develop Security Program	NIST SP 800-18 NIST SP 800-50 NIST SP 800-16	Guide for Developing Security Plans for Information Technology Systems Building an Information Technology Security Awareness and Training Program Information Technology Security Training Requirements: A Role – and Performance-Based Model
Identify and Inventory Assets	OMB Circular A-130	Definition/Categorization of major Information Systems
Select Security Controls	FIPS 200 SP 800-53 SP 800-60	Minimum Security Requirements Recommended Security Controls/Security Assessment Guide for Mapping Types of Information and Information Systems to Security Categories
Categorize Risk	FIPS 199 SP 800-60 SP 800-30	Standards for Security Categorization of Federal Information and Information Systems Guide for Mapping Types of Information and Information Systems to Security Categories Risk Management Guide for Information Technology Systems
Implement Security Controls	SP 800-70	Security Configuration Checklist Program
Assess and Monitor Security Controls	SP 800-53A SP 800-26 SP 800-37	Security Assessment Security Self Assessment Guide Guide for the Security Certification and Accreditation of Federal Information Systems
Respond to Incidents	NIST SP 800-61	Computer Security Incident Handling Guide

AGENCY CHALLENGES

Information security and FISMA compliance present many challenges to federal agencies, including:

- *Ensuring the integrity of information*
- *Maintaining security against new threats*
- *Balancing the demands of complying with evolving regulations*
- *Planning and testing of security controls and contingency plans*
- *Meeting reporting requirements*
- *Improving FISMA scores*
- *Dealing with constrained resources and budgets*

FISMA requires compliance for all data and information systems that support the agency's operations and assets, including those provided by or managed by other agencies or contractors. As part of the FISMA process, agencies must be able to produce a complete and accurate inventory of all systems including their security status and requirements. This can be a difficult task when systems are spread across many organizations and geographies.

Congress holds agencies accountable to improve their security posture, and therefore links budgetary considerations to agency performance and scoring. Scorecard results show that progress has been made in developing security policies and procedures, though weaknesses continue to exist in the planning and testing of contingency plans, certifying and accrediting systems and remediation.

Complying with evolving, multi-sourced and complex standards and reporting requirements and maintaining a sound security posture against evolving threats can be a challenge. However, the significance of ensuring security and compliance is substantial. This necessitates the implementation of a proactive security and compliance program that continuously protects, monitors, assesses and collects data across numerous agency divisions and sites.

FISMA solutions based solely on products may improve security and FISMA scoring in a specific area, but do not adequately address agency-wide security needs nor sustain protection against evolving threats. Focusing limited resources on interpreting changing compliance standards and reporting requirements diverts critical attention from managing risk and ensuring protection. A more efficient solution is to develop a proactive information security program that integrates quality security policies, processes and supporting technology with business strategy, supports the development of a strategic framework for regulatory compliance and more effectively enables a sustainable security infrastructure. A risk-based framework includes agency-wide security planning, accountability, configuration, implementation and testing, assessment and measurement, remedial action and a continuous improvement process.

THE ISS APPROACH TO FISMA COMPLIANCE

ISS FISMA Compliance solution is a holistic approach using people, processes and tools to implement an enterprise-wide security program that meets FISMA requirements, sustains security improvements, and protects against current and future threats.

OVERVIEW

ISS has applied its solutions in numerous regulatory environments including:

- *HIPAA (Health Insurance Portability and Accountability Act)*
- *Sarbanes-Oxley Act*
- *Gramm-Leach-Bliley Act*
- *SCADA (Supervisory Control And Data Acquisition)*
- *ISO 17799*
- *California Breach Law (Bill No. 1386)*

ISS FISMA solution is based on knowledge and experience gained across all of these areas.

ISS has learned that organizations that take a strategic approach to implementing a complete security solution achieve the most success. Establishing the right infrastructure of people, processes and tools builds an environment of awareness and protection from which compliance follows.

In support of developing such a program, ISS draws on its knowledge, experience, and capabilities, including its:

- *Position as an established world leader in security since 1994*
- *Track record with 11,000 customers worldwide – including every major agency of the US Government*
- *Proactive security intelligence conducted by the ISS X-Force, which forms the basis for all ISS services and products*
- *Standardized policies and procedures known to work for FISMA*
- *Documents, tools and checklists that can be put in place to support procedures as well as reporting requirements*
- *Award-winning suite of enterprise-class software solutions that form a framework for supporting a complete security program*
- *Global Security Operations Centers that continuously monitor security threats and evolving complex compliance requirements to facilitate proactive information security management*

ISS FISMA COMPLIANCE SOLUTION

ISS helps agencies evaluate, protect, manage and improve security and compliance through a comprehensive three-phased approach, beginning with **an assessment of an agency's compliance environment** and a **prioritized roadmap** for implementing improvements in security performance and compliance; **delivery and implementation of products and services** to help remediate security weaknesses and sustain security improvements; and **ongoing audits** of security program effectiveness and compliance in order to monitor and protect against future security threats.

The end result is a complete security solution focused on protecting critical and sensitive information.

ISS Approach to Reducing Risk and Improving Security



Assessment

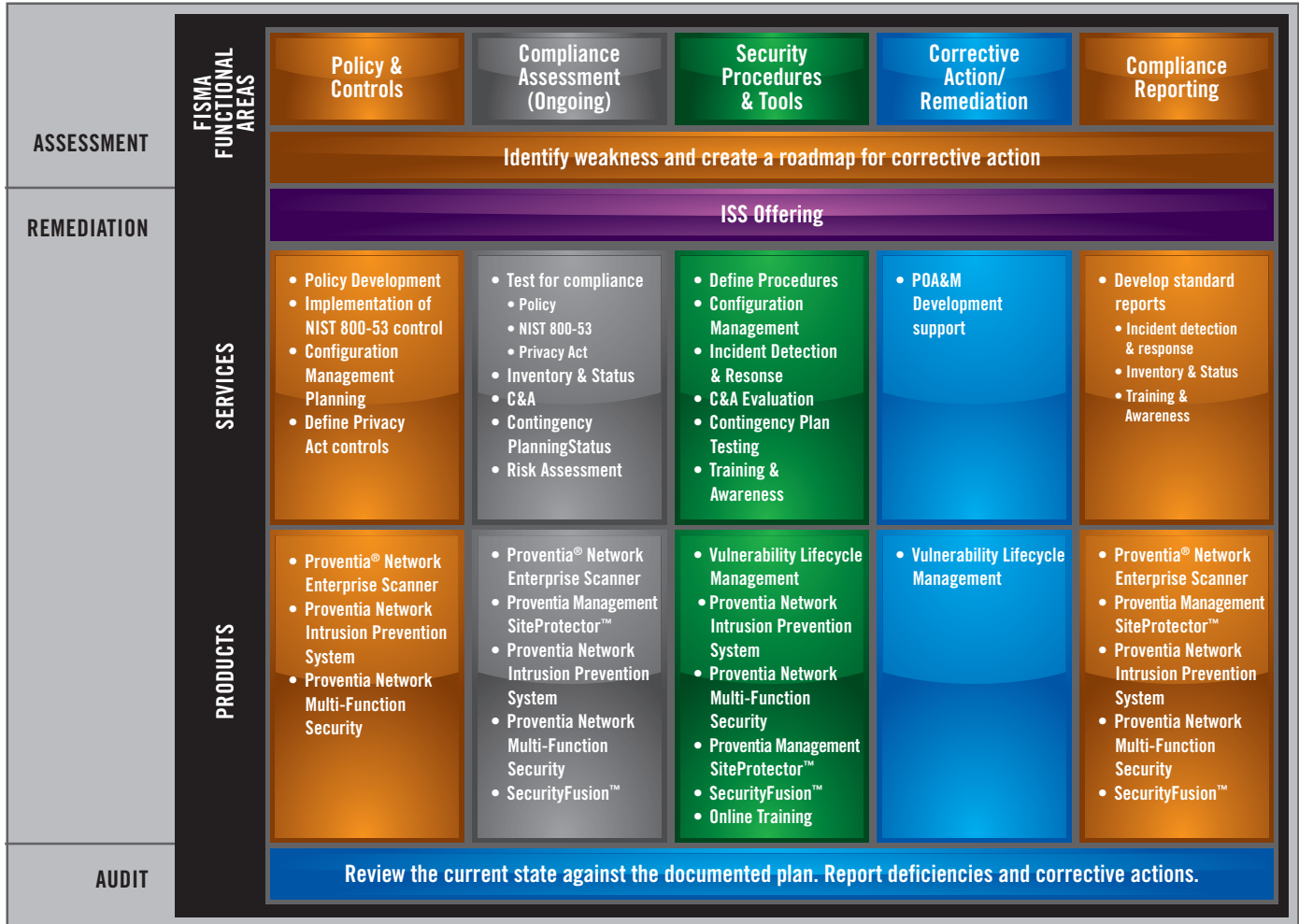
ISS begins the FISMA compliance process with a thorough evaluation of an agency's security program. ISS performs comprehensive discovery for areas such as Security Architecture, Security Management Practices and Operational Security. The ISS FISMA team performs an exhaustive audit to assess the organization's posture against the required NIST standards to ensure FISMA regulatory compliance. ISS reviews every element of the agency's security practice, including but not limited to:

- Policies and procedures
- Configuration management
- Contingency planning and testing
- Penetration testing and vulnerability remediation
- Emergency response and disaster recovery plans
- Training and awareness

The assessment is a 4-6 week effort tailored to an agency's unique needs and designed to accurately deliver the insights required to thoroughly address agency-specific FISMA reporting requirements. ISS will institute a strategy of ongoing compliance auditing so the organization will be able to achieve and maintain compliance over time. ISS provides a detailed evaluation of the agency's compliance performance and a prioritized roadmap of recommendations for implementing security program and compliance reporting improvements.

Remediation

The Remediation phase implements a total security solution using appropriate products and services to develop and sustain a compliance-driven enterprise infrastructure. ISS executes the roadmap of prioritized security improvement recommendations to achieve full FISMA compliance.



For each of the FISMA functional areas defined in the illustration above, ISS provides a complete solution of services and products designed to improve overall information security and protection and to meet compliance requirements.

Policies and Controls

Policies and controls are critical building blocks to compliance, and ISS develops the necessary policies or improves existing policies, and develops or improves configuration management plans.

Compliance Assessment

Just having policies and controls is not sufficient unless they are tested and proven effective. ISS provides the agency with the appropriate tools to help test for compliance as well as the professional services support for installing and configuring the tools. ISS security experts compile inventories and complete certification and accreditation (C&A) documentation, processes and systems, including quality assurance policies and procedures for C&A. ISS provides professional consulting services to conduct threat and risk assessments, including multiple sites and contractor locations.

Security Procedures and Tools

The ISS FISMA team can develop missing procedures or improve existing procedures such as password control, login activation/deactivation and software change controls. The team can also advise clients on the effectiveness of existing tools and make recommendations for improvements that can be designed to scale and implemented agency-wide to ensure consistency.

The ISS solution includes professional consulting services to evaluate existing C&As and, if necessary, perform C&As. ISS also develops any reporting tools necessary to achieve compliance with respect to C&As.

ISS develops a plan for testing contingency plans and works with the agency to test the contingency plans for correctness and effectiveness.

Procedures and tools are only effective if personnel are aware of them and trained to properly use them. ISS provides training through Internet-based courseware on security awareness. ISS can also provide customized onsite training on the use and administration of security procedures.

Corrective Action and Remediation

The ISS FISMA team works with agency personnel to develop Plans of Action and Milestones (POA&Ms) for correcting deficiencies. ISS also helps with the execution plans and uses milestones and metrics to measure progress and success.

Compliance Reporting

ISS provides a suite of products and custom configuration resources to ensure that the proper reporting can be provided to support the FISMA reporting process.

Audit

An effective security program is a continuously improving process that monitors risks, measures improvements and ensures resilience in the face of change. ISS provides ongoing audits to review corrective actions and measure security and compliance improvements. This allows an agency to review and measure progress periodically, promoting ongoing improvements to increase scores at FISMA reporting time.

During an audit, the ISS team measures the performance improvements against the discovered weaknesses and remediation plans to ensure the effectiveness of remedial actions and to ascertain measurable improvement. ISS assesses and monitors an agency's resiliency against new vulnerabilities and threats and identifies corrective actions to more effectively manage risk and maintain information integrity.

Continuous monitoring, measurement and validation of security program improvements ensure that the agency's infrastructure governs security effectively and that the nation's assets are protected.

SUMMARY AND CONCLUSIONS

Protecting the privacy and security of federal information and systems and complying with FISMA requirements is a significant challenge to federal agencies. Faced with cost-effectively meeting FISMA compliance requirements while achieving business objectives and mission, agencies must be efficient to balance both demands.

A best-practice approach to FISMA compliance requires development, implementation and continuous measurement and monitoring of an agency-wide, risk-based security program. Such a solution instills accountability, proactive protection, integrity and continuous improvement. ISS holistic approach to FISMA compliance helps agencies implement an adaptive environment that improves their security posture and ensures ongoing compliance. ISS goal is to build quality, measurable validation and continuous improvement processes into security and compliance programs.

ISS leverages its knowledge of regulatory compliance, a complete suite of products and services, proactive intelligence research and world-class security experience to help agencies effectively comply with FISMA and sustain information integrity.

ISS: The Trusted Security Provider to Federal Agencies

Agencies can rely on ISS to help them achieve FISMA compliance and improve information security. An established world leader in security since 1994, ISS delivers proven cost efficiencies and reduces regulatory and business risk across the enterprise for more than 11,000 customers worldwide, including every major agency of the US Government. ISS products and services are based on the proactive security intelligence conducted by ISS X Force research and development team — the unequivocal world authority in vulnerability and threat research. With headquarters in Atlanta, ISS has additional operations throughout the Americas including Washington DC, Asia, Australia, Europe and the Middle East. For more information, visit the ISS Web site at www.iss.net or call 800-776-2362.

GLOBAL HEADQUARTERS

6303 Barfield Road
Atlanta, GA 30328
United States
Phone: (404) 236-2600
e-mail: sales@iss.net

REGIONAL HEADQUARTERS

Australia and New Zealand

Internet Security Systems Pty Ltd.
Level 6, 15 Astor Terrace
Spring Hill Queensland 4000
Australia
Phone: +61 (0)7 3838 1555
Fax: +61 (0)7 3832 4756
e-mail: aus-info@iss.net

Asia Pacific

Internet Security Systems K. K.
JR Tokyu Meguro Bldg. 3-1-1
Kami-Osaki, Shinagawa-ku
Tokyo 141-0021
Japan
Phone: +81 (3) 5740-4050
Fax: +81 (3) 5487-0711
e-mail: jp-sales@iss.net

Europe, Middle East and Africa

Ringlaan 39 bus 5
1853 Strombeek-Bever
Belgium
Phone: +32 (2) 479 67 97
Fax: +32 (2) 479 75 18
e-mail: isseur@iss.net

Latin America

6303 Barfield Road
Atlanta, GA 30328
United States
Phone: (404) 236-2709
Fax: (509) 756-5406
e-mail: isslatam@iss.net

Copyright© 2006 Internet Security Systems, Inc. All rights reserved worldwide.

Internet Security Systems, the Internet Security Systems logo, Proventia, SiteProtector and Ahead of the Threat are trademarks or registered trademarks of Internet Security Systems, Inc. Other marks and trade names mentioned are the property of their owners, as indicated. All marks are the property of their respective owner and used in an editorial context without intent of infringement. Specifications and content are subject to change without notice.
Distribution: General

PRO-FISMAWP-0406

 **INTERNET | SECURITY | SYSTEMS®**
Ahead of the threat.™

6303 BARFIELD ROAD | ATLANTA, GA 30328 | 800.776.2362 | FAX 1.404.236.2626