FISMA Compliance: Mapping National Institute of Standards and Technology (NIST) Controls to Cisco Security Solutions

Executive Summary

The primary incentive for compliance with the Federal Information Security Management Act (FISMA) is to identify the people, systems, and processes an agency needs to achieve its business objectives, and to protect them appropriately. A secondary incentive is that good FISMA grades bolster an agency's reputation within the House Government Reform Committee and in the eyes of citizens.

This white paper can serve as a reference for IT groups that want to increase information security and ease the path to improving FISMA compliance. It reduces the research that agency IT groups must conduct to achieve FISMA compliance and reduces risk by mapping the control groups defined by the National Institute of Standards and Technology (NIST) to specific security solutions that Cisco® provides in the Cisco® Self-Defending Network portfolio.

Each section of the white paper focuses on one NIST control, describing how that control helps the agency achieve its mission and then listing the Cisco solutions that fulfill that control's requirements. Cisco provides network and security systems that are designed from the outset to operate and be managed as a system. An integrated approach to security helps agencies meet federal government requirements for more effective security, avoids time-consuming and expensive integration work, and reduces management burden. This is a recipe for faster FISMA compliance at lower cost.

FISMA Controls by Types

Table 1 shows FISMA controls by type: technical, management, or operational. This document concerns itself with those controls that appear in boldface type.

Table 1. FISMA Controls by Type

Technical	Management	Operational
AC: Access Control **AU: Audit and Accountability** **IA: Identification and Authentication** **SC: System and Communications Protection**	CA: Certification, Accreditation, and Security Assessments PL: Planning SA: System and Services Acquisition	AT: Awareness and Training **CM: Configuration Management** CP: Contingency Planning **IR: Incident Response** MA: Maintenance MP: Media Protection PE: Physical and Environmental Protection PS: Personnel Security RA: Risk Assessment **SI: System and Information Integrity**

Access Control (AC)

Type of control: Technical

FISMA Requirement

Access Control (AC) addresses access policies and procedures, account management and the associated tools and techniques for access enforcement and password control, systems notifications, separation of duties, session lock and termination, marking and labeling, and remote and wireless access.

Mission Impact

The government's mobile workforce is expanding rapidly as agencies realize the value of remote network access and encourage telework to support plans for Continuity of Operations (COOP). As a result, IT organizations are managing many more mobile and remote devices than ever before, including PCs, laptops, servers, smart phones, and personal digital assistants, often with the same resources. To protect confidentiality and prevent network disruption from attack or infection, IT groups need to validate that users are authorized to access systems and that the users' devices are infection-free and compliant with security policy. To accomplish this, agencies need network-based access controls that securely manage who and what can access the network, as well as when, where, and how that access can occur. The goal is to prevent inappropriate and unauthorized use of critical systems.

Cisco Solutions

Table 2. Cisco Products and Services for Access Control

Function Required for FISMA Compliance	Cisco Products and Services
Access control	• Cisco Secure Access Control Server (ACS) • Network Admission Control • Cisco Catalyst® routers and Cisco routers using the Cisco IOS® Software
Identity-Based Network Services (IBNS)	Cisco Secure ACS
Security management	• Cisco consulting and integration services • Services from Cisco security partners

Major Capabilities of Cisco Solutions for Access Control

- Enables granular control of network access by authorizing different types of network services for users or groups
- Provides comprehensive admission control across all access methods to prevent noncompliant and rogue endpoints from affecting network availability
- Enables user accounting and auditing as well as tracking and monitoring of user behavior inside the LAN
- Promotes greater employee mobility and flexibility, which supports COOP initiatives and can increase productivity and the effectiveness of government services
- Enforces a uniform security policy for all users, regardless of how they access the network
- Reduces the administrative and management burden involved in scaling user and network administrator access to the network
- Centralizes the control of all user privileges and distributes them to hundreds or thousands of access points throughout the network

- Provides detailed reporting and monitoring capabilities of network users' behavior and keeps a record of every access connection and device configuration change across the entire network, as required by FISMA and other security regulations
- Supports a broad variety of access connections, including wired and wireless LAN, dialup, broadband, content, storage, voice-over-IP (VoIP), firewalls, and VPNs

Audit and Accountability (AU)

Type of control: Technical

FISMA Requirement

The Audit and Accountability (AU) control enforces appropriate use policy for network and information systems. It also enables agencies to audit usage of information systems and to validate compliance with standards by producing supporting documentation and reports.

Mission Impact

Agencies need to enforce appropriate use of network-based information systems and be able to produce an audit trail of that usage. Requests to view a security policy or compliance reports can come from stakeholders, regulators, or the Inspector General or other auditors. To help ensure effective audits and demonstrate accountability, agencies need to create, protect, and retain information-system audit records. This will enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity. These capabilities give government the ability to trace network activity to individual users so that they can be held accountable.

Cisco Solutions

Cisco solutions for the AU control include tools to generate reports for annual inspector general audits. Cisco Security Manager generates reports on infrastructure configuration, including inventory. Cisco Secure Access Control Server keeps a record of every access connection and device configuration change across the entire network. Cisco Secure Monitoring, Analysis, and Response System (Cisco Secure MARS) correlates network anomalies with security incidents.

Table 3. Cisco Products and Services for Audit and Accountability

Function Required for FISMA Compliance	Cisco Products and Services
Security management	• Cisco Security Manager • Cisco Secure Access Control Server • Cisco Secure Monitoring, Analysis, and Response System (Cisco Secure MARS) • CiscoWorks Network Compliance Manager • CiscoWorks Security Information Management Solutions (SIMS)
Consulting and integration services	• Cisco Advanced Services • Services from Cisco Certified Partners in security

Major Capabilities of Cisco Solutions for Audit and Accountability

- Maintains a system log of network events and administrative actions
- Correlates events as they happen at different levels of the network—desktop, server, network—to show the entire security incident
- Automatically diagnoses the root cause of a security breach and suggests possible remedial actions

- Dynamically links to the Cisco Security Manager system, enabling operators to quickly execute remedial action
- Maintains an access control database for audit and for nonrepudiation, which is essential for prosecution

Configuration Management (CM)

Type of control: Operational

FISMA Requirement

The Configuration Management (CM) control addresses policies and procedures, change control, monitoring of configuration changes, configuration settings, and access restrictions for configuration changes.

Mission Impact

Changes to a router or switch configuration, whether intentional or accidental, have the potential to disrupt the agency network. Therefore, agencies need a way to control and track all changes to the information system. This requires a policy that governs configuration changes and provides automated enforcement of the policy by the network. The goals are to protect the network, reduce network outages, verify network resiliency, and demonstrate regulatory and IT compliance. The ability to control and track changes also helps agencies identify security gaps in their current configurations, track and control changes, and pinpoint misconfigurations in their environment. After identifying problems, agencies need a way to resolve them in a timely manner.

Cisco Solutions

Table 4. Cisco Products and Services for Configuration Management

Function Required for FISMA Compliance	Cisco Products and Services
Configuration management	• Cisco Security Manager • Cisco Configuration Assurance Solution • CiscoWorks Network Compliance Manager
Consulting and integration services	• Cisco Advanced Services • Services from Cisco Certified Partners in security

Major Capabilities of Cisco Solutions for Configuration Management

- Lowers cost of ownership by reducing the number of systems to maintain
- Reduces risk by enabling verification and test of configuration changes before they are applied to the production network
- Enforces change-control procedures
- Enables consistent policy enforcement
- Enables rapid, automated deployment of policy updates
- Reduces risk from operator error

System and Information Integrity (SI)

Type of control: Operational

FISMA Requirement

The System and Information Integrity (SI) control addresses policies and procedures, remediation of security flaws, security alerts and advisories, malicious code protection, intrusion detection and prevention tools and techniques, protection against spyware and other malicious code, application and information integrity, and more.

Mission Impact

As part of e-government initiatives, agencies share information with the public and other constituents over networks. This requires two security precautions. The first protects sensitive citizen and government information from disclosure or alteration in transit and in storage. The second prevents disruption from network infection or attack, which requires the ability to identify, report, and remediate system flaws before allowing a connection to the network. The SI control refers to the IT staff’s ability to patch systems in a timely manner; protect against worms, viruses, and spyware; and monitor and protect the systems from both external and internal attacks.

Cisco Solutions

Table 5. Cisco Products and Services for System and Information Integrity

Function Required for FISMA Compliance	Cisco Products and Services
Perimeter protection	Cisco ASA 5500 Series Adaptive Security Appliance
Encryption tools for confidentiality and information integrity	Cisco IPSec VPN, Cisco SSL VPN Client, Secure Shell (SSH)
Intrusion detection and prevention	• Cisco Intrusion Prevention System (IPS) • Cisco Security Agent, for desktops and servers
Anti-X defense (virus, spyware, malware)	• Network Admission Control • Cisco Trust Agent • Cisco Security Agent
Security management	• Cisco Security Manager • Cisco Secure Monitoring, Analysis, and Response System (Cisco Secure MARS) • Cisco Secure IntelliShield Alert Manager • Cisco Incident Control System (ICS), developed jointly with Trend Micro
Consulting and integration services	• Cisco Advanced Services • Product Security Incident Response Team (PSIRT) • Services from Cisco Certified Partners in security

Major Capabilities of Cisco Solutions for System and Information Integrity

- Enables comprehensive security management and monitoring
- Automatically identifies, reports, and remediates security flaws in devices attempting to connect to the network
- Manages the flaw remediation process and automatically installs updates without intervention from the agency employee or IT
- Periodically determines the state of information system components, regarding malware remediation
- Provides monitoring and analysis to alert and advise the staff of improper use
- Ensures that desktop and server configurations comply with prevailing policy

- Automatically learns of new threats from trusted resources
- Adapts policy changes without disruption to ongoing live operations
- Provides protection against day-zero threats using signature-based and behavior-based methods
- Prevents unauthorized changes to configuration and addition of nonapproved software

Identification and Authentication (IA)

Type of control: Technical

FISMA Requirement

The Identification and Authentication (IA) control addresses policies and procedures, device and host identification and authentication, authenticator management, feedback, and cryptographic authentication.

Mission Impact

Government agencies need the ability to continuously monitor, audit, and report on every user and device gaining access to the network. The immediate goal is information protection; the larger goal is national security. To fulfill their missions, agencies must limit information system access to authorized users, processes acting on behalf of authorized users, or authorized devices, including other information systems. They must also limit access to the types of transactions and functions for which users are authorized. These measures help ensure that unauthorized users are denied access and that information integrity remains protected.

Table 6. Cisco Products and Services for Identification and Authentication

Function Required for FISMA Compliance	Cisco Products and Services
Authentication and authorization	Cisco Secure Access Control Server (ACS)
Access control	Network Admission Control
Identity management	• Identity-Based Network Services (IBNS) • Network Access Control (NAC) • Services from Cisco Advanced Services or Cisco Certified Partners

Major Capabilities of Cisco Solutions for Identification and Authentication

- Provides authentication and validation of devices and software
- Authenticates users for full or limited access
- Automatically detects, isolates, and remediates noncompliant devices

System and Communications Protection (SC)

Type of control: Technical

FISMA Requirement

The System and Communications Protection (SC) control addresses policies and procedures, application partitioning, removal of information remnants, distributed-denial-of-service (DDoS) protection, control plane resource priority, transmission integrity and confidentiality, key management, certificate authorities, and more.

Mission Impact

New communications technologies such as IP telephony and wireless personal digital assistants are blurring the boundaries between traditional networks and communications systems. Therefore, agencies need protections for privacy and integrity not only for government and citizen data but also for video and voice conversations. The SC control protects information confidentiality as well as critical information systems and data. Traditionally, perimeter security solutions such as firewalls and intrusion detection systems have handled these protections. However, those systems alone cannot adequately protect against unknown threats and today's more sophisticated blended threats. Agencies now need multiple layers of defense. As the only IT resource that is pervasive throughout an enterprise or agency, including headquarters and branch offices, the network plays a vital role in protecting systems and communications. Agencies achieve the best protection when every element in the network acts a point of defense, a central tenet of the Cisco Self-Defending Network.

Cisco Solutions

Table 7. Cisco Products and Services for System and Communications Protection

Function Required for FISMA Compliance	Cisco Products and Services
Boundary protection	Network boundaries: • Cisco ASA 5500 Series Adaptive Security Appliance • Cisco firewall solutions (Cisco PIX firewalls, Cisco Firewall Security Modules, Cisco ASA 5500 Series Adaptive Security Appliances) • Cisco Intrusion Prevention System/Intrusion Detection System • Cisco IOS Software • Cisco integrated services routers • Cisco Catalyst 6500 Series Switches with security modules (SecureLAN) Individual hosts: • Cisco Security Agent • Network Admission Control
Encryption, confidentiality, and integrity tools	• Cisco IPSec and SSL VPN solutions • Cisco ASA 5500 Series Adaptive Security Appliance • Cisco VPN Concentrators • Cisco firewall solutions • Cisco integrated services routers • Cisco Aironet Wireless Access Points and Controllers • Cisco MDS 9000 Series SAN Switches
Quality of service (QoS)	QoS/Control Plane Policing, a feature of Cisco IOS Software
Intrusion detection and prevention	• Cisco IDS/IPS 4200 Series • Cisco ASA 5500 Series Adaptive Security Appliance • Cisco integrated services routers
Anti-X	• Cisco Security Agent • Cisco ASA 5500 Series Adaptive Security Appliance • Cisco integrated services routers
Security management	• Cisco Security Manager • Cisco Secure MARS
Consulting and integration services	• Cisco Advanced Services • Services from Cisco Certified Partners in security
Policy enforcement	• Cisco Security Manager • Network Admission Control • CiscoWorks Network Compliance Manager

DDoS protection	• Cisco Guard DDoS Mitigation Appliances • Cisco Traffic Anomaly Detectors • QoS, a feature of Cisco IOS Software • Cisco Intrusion Prevention System As features of Cisco integrated service routers and Cisco ASA 5500 Series Adaptive Security Appliances: • Adaptive Security Algorithms • Control Plane Policing • Access Control Lists • SYN flood protection • Unicast Reverse Path Forwarding • RFC 2827 filtering
Public access protection	Application inspection capabilities of: • Cisco 5500 Series Adaptive Security Appliances • Cisco integrated services routers • Cisco Intrusion Prevention System • Cisco Security Agent, for host-based protection

Major Capabilities of Cisco System and Communications Protection Solutions

- Enables IT staff to control, deploy, and enforce policies according to the current business requirements
- Supports federal COOP and telework initiatives
- Protects network from DoS and DDoS attacks
- Protects privacy by encrypting communications
- Prevents infection from worms and viruses and helps mitigate network attacks
- Enables real-time monitoring of security events
- Provides real-time, continuous auditing
- Accelerates incident response by enabling proactive rather than reactive response
- Simplifies management
- Enables adaptation to constantly changing security threats

Incident Response (IR)

Type of control: Operational

FISMA Requirement

The Incident Response (IR) control addresses policies and procedures, incident handling, incident reporting, and incident response assistance, including forensic services and automated tools where applicable.

Mission Impact

Worms or virus outbreaks can spread globally in just minutes. Therefore, early detection and proactive response have become crucial for protecting agency data, assets, and information systems; and for ensuring confidentiality of data and communications. Agencies need to respond within minutes of the outbreak to help ensure that government services remain available and to decrease the costs associated with damage remediation.

Cisco Solutions

The Cisco Incident Control System (ICS) solution defends the global network within minutes of an outbreak anywhere in the world. Using up-to-the-moment threat intelligence from Trend Micro, an industry-leading expert in antivirus and worm mitigation, Cisco ICS collaborates with the agency's

Cisco network and security devices to rapidly distribute worm and virus immunization capabilities throughout the network. A faster, proactive response prevents worms and viruses from becoming entrenched, thus helping ensure network availability and decreasing the costs associated with damage cleanup.

Table 8. Cisco Products and Services for Incident Response

Function Required for FISMA Compliance	Cisco Products and Services
Perimeter security protection	• Cisco Guard DDoS Mitigation Appliances • Cisco integrated services routers • Cisco ASA 5500 Series Adaptive Security Appliance • Cisco Firewall Services Module • Cisco Incident Control System
Intrusion detection and prevention	• Cisco Security IntelliShield Alert Manager • Cisco IDS and Cisco IPS 4200 Series Sensors • Cisco Security Agent, providing predictive response • Network Admission Control, for quarantine and remediation
Security management	• Cisco Security Manager • Cisco Secure Monitoring, Analysis, and Response System (Cisco Secure MARS) • CiscoWorks Network Compliance Manager
Consulting and integration services	• Cisco Advanced Services • Services from Cisco Certified Partners in security • Product Security Incident Response Team (PSIRT)

Major Capabilities of Cisco Incident Response Solutions

- Proactively prevents infection from worms and viruses
- Harnesses existing Cisco network and security devices to adapt in real time for a coordinated networkwide response
- Gives agency IT groups granular control of how Cisco ICS mitigation policies are deployed in the network
- Provides timely, accurate, continuously updated, targeted alerts of major threats and vulnerabilities to Cisco and third-party software and hardware products, with links to remediation solutions
- Facilitates real-time incident response by automatically correlating raw log reports to events, and events to incidents
- Reduces the complexity of security threat management
- Automatically learns new threats and adapts dynamically
- Reduces the need for incident response by preventing threats before they occur
- Automates documented incident-response procedures

Conclusion

Good agency governance depends on the effective management of internal controls and on the availability, confidentiality, and integrity of information within the organization. An agency's reputation, ability to serve the public, and productivity all depend on the defense of business processes and on the compliance with a growing array of legislation and regulation, including FISMA.

The network plays a major role in FISMA compliance because it touches every aspect of the extended organization and its business processes. The Cisco Self-Defending Network aligns with the controls recommended by FISMA and NIST 800-53, as described in this white paper. Agencies can minimize the research required for FISMA compliance—and avoid the risks of trial and error—by adopting an integrated approach to security to develop a Self-Defending Network. Agency IT groups do not need to implement all NIST controls at once; rather, they may implement them incrementally according to their importance to the agency mission.

For more information on the Cisco Self-Defending Network, visit: http://www.cisco.com/go/sdn.

For more information on Cisco services for federal government, visit: http://www.cisco.com/go/federal.

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C02-390654-00 09/07