IASM Support for FISMA

Introduction

Most U.S. civilian government agencies, and commercial enterprises processing electronic data on behalf of those agencies, are concerned about whether and how Information Assurance products they are considering for purchase can help them "comply with FISMA". This document identifies the FISMA security controls for which Promia's Intelligent Agent Security Manager (IASM) provides implementation support and describes the IASM features that provide that support. Thus, when an agency has completed their FISMA security risk assessment and identified the security controls required in one or more of their information systems, they will then be able to determine how IASM assists in meeting their FISMA-related requirements.

Overview of FISMA

FISMA is an acronym that, depending on the context in which it is used, can refer to one of the following:

- Title III (the Federal Information Security Management Act) of U.S. Public Law 107-347 (the Electronic Government Act), which was signed into law on 17 December 2002;
- The FISMA implementation guidance that PL 107-347 explicitly required the National Institute of Standards and Technology (NIST) to develop and promulgate as Federal Information Processing Standards (FIPS);
- The security risk assessment process that PL 107-347 explicitly requires an agency or commercial enterprise to apply to each information system that is subject to the terms of the law in order to identify the technical security controls that are needed in that system;

This document concentrates on FISMA in the context of the implementation guidance described in the second bullet, since that is where the concrete technical security controls to which IASM is a solution are defined and explained.

As stated in the FISMA (PL 107-347, Title III, §3541):

"The purposes of this subchapter are to:

(1) provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets;

(2) recognize the highly networked nature of the current Federal computing environment and provide effective government-wide management and oversight of the related information security risks, including coordination of information security efforts throughout the civilian, national security, and law enforcement communities;

(3) provide for development and maintenance of minimum controls required to protect Federal information and information systems;

(4) provide a mechanism for improved oversight of Federal agency information security programs;

(5) acknowledge 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; and

(6) recognize that the selection of specific technical hardware and software information security solutions should be left to individual agencies from among commercially developed products."

The FISMA statute tasked NIST with developing:

- Standards to be used by Federal agencies to categorize information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels;
- Guidelines recommending the types of information and information systems to be included in each category; and
- Minimum information security requirements, (i.e., management, operational, and technical security controls), for information and information systems in each such category.

As a result, NIST has produced the following FIPS (Federal Information Processing Standards) and Special Publications:

- **FIPS Publication 199**, *Standards for Security Categorization of Federal Information and Information Systems*, which addresses the first of the three NIST tasks. FIPS Publication 199 establishes security categories for both information and information systems. The security categories are based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization resulting from the operation of its information systems;
- **FIPS Publication 200**, *Minimum Security Requirements for Federal Information and Information Systems*, which addresses the NIST tasking to develop "Minimum information security requirements, (i.e., management, operational, and technical security controls), for information and information systems in each such category". FIPS Publication 200 specifies minimum security requirements for information and information systems supporting the executive agencies of the federal government and a risk-based process for selecting the security controls necessary to satisfy the minimum security requirements. The goal of FIPS Pub 200 is to promote the development, implementation, and operation of more secure information systems within the federal government by establishing minimum levels of due diligence for information security and facilitating a more consistent, comparable, and repeatable approach for selecting and specifying security controls for information systems that meet minimum security requirements.
- **NIST Special Publication 800-37**, *Guide for the Security Certification and Accreditation of Federal Information Systems*, which provides guidance for the security certification and accreditation of information systems supporting the executive agencies of the federal government.
- **NIST Special Publication 800-53**, *Recommended Security Controls for Federal Information Systems,* which provides guidance for selecting and specifying security controls for information systems supporting the executive agencies of the

federal government. The guidelines apply to all components of an information system that process, store, or transmit federal information.

- **NIST Special Publication 800-53A**, *Guide for Assessing the Security Controls in Federal Information Systems*, which provides guidance for assessing the effectiveness of security controls employed in information systems supporting the executive agencies of the federal government. The guidelines apply to the security controls defined in NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*.
- **NIST Special Publication 800-59**, *Guideline for Identifying an Information System as a National Security System*, which provides guidance for identifying an information system as a national security system, which would be excluded from the requirements of FISMA.
- **NIST Special Publication 800-60**, *Guide for Mapping Types of Information and Information Systems to Security Categories*, which provides guidance for determining the types of information and information systems to be included in each category of potential security impact.

Overview of IASM

The Intelligent Agent Security Manager (IASM) is a high-speed, security-hardened appliance that collects, consolidates, and analyzes log data from network and security devices, as well as operating systems and applications, to detect and manage operational and security incidents. It is designed to also pull data from vulnerability management systems as well as databases and syslog servers. As well, it is capable of rapidly reconfiguring itself to receive and process data from new devices, systems, and applications. Log records are first analyzed, pre-filtered, and normalized by intelligent agent for each sensor on the monitored network. The records are then sent to the IASM appliance where the data is then correlated and analyzed further by one or more analytic engines to determine cyber attack profiles in real time.

The IASM includes the Asset Viewer (AV) graphical user interface, which uses flexible and powerful 3-dimensional, user-definable, graphical components to provide a consolidated visualization of all assets on the monitored network. This visualization includes versions and patch levels of node operating systems, device and application status, ports in use, and other related information. The visualization also allows an operator to navigate between subnets of the monitored network, thus exposing the contextual relationship between those subnets. It also displays both operational and security incidents detected by the IASM appliance in a rapidly comprehensible view suitable to the needs of enterprise network operations center personnel. These visualization models have been operationally validated in a globally distributed enterprise. The visual elements can also be annotated with English descriptions to help operations personnel interpret their networks' electronic terrain.
Under an SBIR contract with the US Navy Computer Network Defense program, Promia jointly developed the IASM, which integrates security countermeasures for security incident detection, management, and response into the Navy network operations centers (NOCs). IASM is a new class of product, categorized as *Security Information Management* (SIM) that automatically collects, normalizes, and analyzes the operational and security event logs of diverse security relevant devices. IASM detects security incidents that are only visible when data available from multiple devices is considered. Having detected the incidents, IASM then identifies candidate

responses based on site-specific organizational policies and provides a unified operator interface for managing the incidents and responses. A requirement of the SBIR program is to reduce the lifecycle costs of technology by generalizing government-specific systems into commercially available products. Along with this requirement for commercializing the IASM technology is the obligation to comply with the policy that US Government organizations must favor the use of information assurance technologies that have been evaluated according to the Common Criteria (ISO 15488).

The IASM Common Criteria (CC) TOE (Target Of Evaluation) is the general purpose Security Information Management Platform that provides the IASM functions that are needed both in an enterprise-specific SIMS – such as the Navy-specific IASM – and can be successfully evaluated using the CC. One of the most important aspects of selecting the functions in the IASM CC TOE was determining which IASM functions could be specified and tested without reference to detailed knowledge of a specific network.
Also included in the IASM family of products is the Network Security Event Sensor (NSES) appliance, which functions as both an integral component of the IASM asset management capabilities and as a stand-alone intrusion and asset detection appliance. The NSES appliance provides: asset identification and mapping, passive asset fingerprinting, IP traffic anomaly detection (which is able to detect Zero-day network attacks), and attack signature sensing based on the Snort engine. The NSES also includes a collection of analytic services including false positive reduction, message aggregation, and IP address white- and black-listing. It also incorporates a "fishbowl" capability that records 1-60 second "snapshots" of IP traffic both before and after a security event for later review by remote analysts. This feature allows rapid propagation of summary event records while retaining contextual traffic information at the sensor level in case forensic review by highly skilled incident analysis personnel is later required.

Figure 1, below, shows the operational concept for how the IASM, NSES, and Asset Viewer fit together with a monitored network.

IASM Support for FISMA

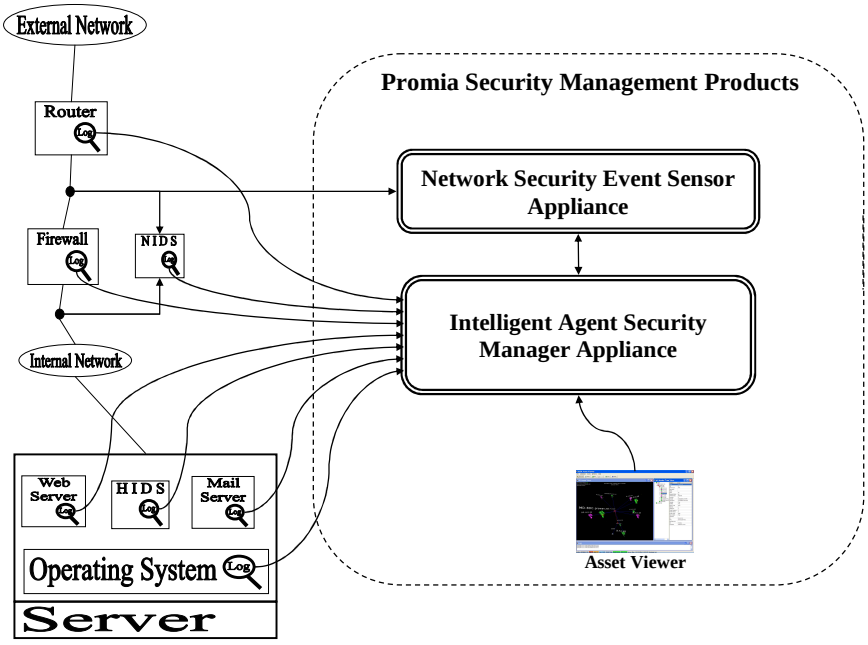

Figure 1 – Promia Security Management Products Operational Concept

In summary, the IASM family of products provides the following set of functions for possible use as part of the IT controls needed to comply with Sarbanes-Oxley requirements:

- Automatic detection (by the NSES) and visualization (by the AV) of hardware, operating system, and software application assets on the monitored network;
- Network intrusion detection sensors (on the NSES) that use both signature- and anomaly-based algorithms to detect known and previously unseen network intrusion attempts;
- Collection and consolidation of operational and security events – from both the NSES and third-party products – into a unified, high-integrity,A security information management (SIM) repository where they are later available for a SOX compliance audit;
- Real-time analysis of events – as they are collected from sensors on the monitored network – by one or more analytic engines to monitor and detect security, operations, and SOX non-compliance incidents as they occur;
- Real-time visualization of emerging incidents, backed up by the ability to drill down through the security, operations, and SOX non-compliance incidents into the events that indicate and support the incident;
- Tools for managing the lifecycle of detected security, operations, and SOX non-compliance incidents: including remediation actions taken to correct detected problems;
- Tools for defining and generating summary and detail reports about security, operations, and SOX non-compliance incidents and actions taken to address the incidents, which can be used for continuous SOX compliance monitoring, as well as compliance audits;

IASM Support for FISMA

Implementing FISMA Technical Security Controls Using IASM

FIPS Publication 200 identifies minimum security requirements that cover seventeen security-related areas with regard to protecting the confidentiality, integrity, and availability of federal information systems and the information processed, stored, and transmitted by those systems. The seventeen areas represent a broad-based, balanced information security program that addresses the management, operational, and technical aspects of protecting federal information and information systems and are the organizational framework for the 163 security controls identified in NIST Special Publication (SP) 800-53. The security-related areas include:

(i) access control;
(ii) awareness and training;
(iii) audit and accountability;
(iv) certification, accreditation, and security assessments;
(v) configuration management;
(vi) contingency planning;
(vii) identification and authentication;
(viii) incident response;
(ix) maintenance;
(x) media protection;
(xi) physical and environmental protection;
(xii) planning;
(xiii) personnel security;
(xiv) risk assessment;
(xv) systems and services acquisition;
(xvi) system and communications protection; and
(xvii) system and information integrity.

The bolded security-related areas above are ones for which the IASM has features that can be used to implement one or more of the security controls assigned to that area. The table below shows each of the security controls for which the IASM provides supporting functionality and describes the IASM feature(s) that support that control.

CNTL NO.	CONTROL NAME	IASM Feature(s) Supporting the Control
Audit and Accountability		
AU-2	Auditable Events	A core feature of IASM is consolidation and management of audit records from multiple devices, OS, and applications. IASM also generates and manages the records of its own operation. This feature was validated by the NIAP evaluation.
AU-3	Content of Audit Records	
AU-4	Audit Storage Capacity	IASM models have 1-2 Terabytes of storage: enough for 180 days of records from medium to large enterprise networks
AU-5	Audit Processing	All aspects of this control are present in IASM and were verified by both analysis and testing by the NIAP evaluation.
AU-6	Audit Monitoring, Analysis, and Reporting	IASM was developed specifically to automate this control and allows the simultaneous use of multiple analysis algorithms to improve the effectiveness of incident detection. Promia is continuously improving the breadth, depth, and effectiveness of the algorithms it provides with IASM.
AU-7	Audit Reduction and Report Generation	All aspects of this control are present in IASM and were verified by both analysis and testing by the NIAP evaluation.

IASM Support for FISMA

CNTL NO.	CONTROL NAME	IASM Feature(s) Supporting the Control
AU-8	Time Stamps	IASM implements this control (which was verified by both analysis and testing by the NIAP evaluation) for its internal use and also provides mechanisms to normalize events consolidated from other devices, OS, and applications to its internal time reference.
AU-9	Protection of Audit Information	All aspects of this control are present in IASM and were verified by both analysis and testing by the NIAP evaluation.
AU-10	Non-repudiation	Subject to the information being part of the audit records produced by relevant other devices, OS, and applications, IASM analytic engines can be developed to implement this control. If the originating devices, OS, & applications digitally sign the audit record, the non-repudiation case is stronger.
AU-11	Audit Retention	IASM models have 1-4 Terabytes of storage: enough for 180 days of records from medium to large enterprise networks
Certification, Accreditation, and Security Assessments		
CA-7	Continuous Monitoring	Subject to the appropriate configuration of other devices, OS, and applications on the IS, IASM can monitor and report on the availability and operation of control implementations.
Configuration Management		
CM-2	Baseline Configuration	IASM asset management features provide tools for both establishing the baseline and detecting and managing changes to the baseline.
CM-3	Configuration Change Control	IASM asset management features provide partial support for “documenting completed changes to the information system.”
CM-4	Monitoring Configuration Changes	IASM asset management features detect the addition of new devices, OS, & applications, which supports this control.
Contingency Planning		
CP-9	Information System Backup	IASM provides the hardware and software to conduct tape backups of the consolidated audit records from other devices, OS, & applications on the IS, as well as its internal audit trail.
CP-10	Information System Recovery and Reconstitution	IASM can restore the consolidated audit records of other devices, OS, & applications on the IS from tape backups.
Incident Response		
IR-1	Incident Response Policy and Procedures	IASM provides support for multiple incident response roles and for automation of the workflow between and within those roles.
IR-2	Incident Response Training	Promia developed a simulation product that it uses for IASM usage training that can support this control at customer sites.
IR-3	Incident Response Testing	Promia conducts similar testing as part of its IASM quality and security assurance processes, which can be leveraged into IASM customer solution consulting.
IR-4	Incident Handling	IASM was developed specifically to automate the analysis and detection of security incidents: even including the simultaneous use of multiple analysis algorithms to improve the effectiveness of incident detection. IASM has features to categorize incidents, recommend responses, and automate those responses. Finally, IASM has user interface workflow support to ensure involvement of appropriate personnel as required by the organization’s incident handling process.
IR-5	Incident Monitoring	
IR-6	Incident Reporting	Customers can use IASM’s report generation feature to produce incident reports for appropriate authorities. IASM includes report templates for several such authorities. For authorities with automated reporting mechanisms, IASM’s automated incident response feature can be used to integrate the submission of the reports into the customer’s automated internal incident management process.

IASM Support for FISMA

CNTL NO.	CONTROL NAME	IASM Feature(s) Supporting the Control
System and Services Acquisition		
SA-4	Acquisitions	IASM can meet acquisition requirements for CC evaluation.
SA-5	Information System Documentation	As a result of its CC evaluation, IASM is shipped with user and administrator documentation, as well as installation, generation, & startup instructions. Likewise, Promia maintains the internals documentation required by an EAL3 evaluation and can make it available as part of customer solution consulting
SA-8	Security Design Principles	The IASM component of any customer solution has been shown to comply with the security design principles specified in CC EAL3.
SA-10	Developer Configuration Management	The IASM component of any customer solution has been shown to comply with the configuration management requirements of CC EAL3, as well as the additional requirements of CC ALC_FLR.2 for flaw remediation.
SA-11	Developer Security Testing	The IASM component of any customer solution has been shown to comply with function security testing requirements of CC EAL3. In addition, Promia has extensive experience supporting the CT&E of IASM according to DITSCAP.
System and Communications Protection		
SC-2	Application Partitioning	IASM is a dedicated hardware appliance with no mechanisms for running user-developed code.
SC-3	Security Function Isolation	Using both SSL at the network level and role-based access control to its operational and administrative user interfaces, IASM ensures isolation of its security functions from users on the information system being monitored and protected.
SC-5	Denial of Service Protection	As a mechanism for detecting DoS attacks, IASM provides the system operators with information needed to counteract those attacks before they affect the system operation.
SC-8	Transmission Integrity	IASM uses SSL to protect the integrity and confidentiality of both event data that it collects from the information system being monitored and protected and its own user interfaces.
SC-9	Transmission Confidentiality	
SC-10	Network Disconnect	IASM enforces this control on both user interfaces and event collection agents.
SC-11	Trusted Path	IASM uses SSL to establish the trusted path between itself and the operator or administrator's browser.
SC-12	Cryptographic Key Establishment & Management	IASM uses the standard mechanisms within SSLv3
SC-13	Use of Validated Cryptography	The SSL implementation in IASM has been validated according to FIPS 140-2
SC-17	Public Key Infrastructure Certificates	IASM can use PKI certificates when they are available.
System and Information Integrity		
SI-2	Flaw Remediation	The asset manage feature of IASM can provide better information about components of the IS that might be subject to newly discovered flaws. Also, Promia has an aggressive flaw remediation program in place in the event of IASM flaws.
SI-4	Intrusion Detection Tools and Techniques	IASM is designed to be a core component of solutions for this control.
SI-5	Security Alerts and Advisories	IASM incident management and response management features can automate some parts of this control.
SI-6	Security Functionality Verification	If appropriate events are logged and forwarded to IASM, it can provide real-time detection of anomalous security function behavior in other components of the IS.
SI-7	Software and Information Integrity	In combination with HIDS that provide integrity checking, IASM can provide real-time detection of anomalous changes to critical resources.