

PUTTING NIST GUIDELINES FOR INFORMATION SECURITY CONTINUOUS MONITORING INTO PRACTICE

Since Congress instituted the Federal Information Security Management Act (FISMA) of 2002 to address the rapid proliferation of IT security challenges facing government agencies, the National Institute of Standards and Technology (NIST) has recommended regular additions to the Act – many of which have subsequently been adopted into the FISMA compliance process.

This paper discusses how security testing and measurement solutions from Core Security Technologies can help your agency adhere to NIST's recommendations for Information Security Continuous Monitoring as prescribed by the following Special Publications:

- **NIST SP 800-137: *Information Security Continuous Monitoring for Federal Information Systems and Organizations*** is designed to assist organizations in developing a continuous monitoring strategy and implementing a related program.
- **NIST SP 800-39, Revision 1: *Guide for Applying the Risk Management Framework to Federal Information Systems*** establishes a Risk Management Framework (RMF) that promotes the concept of near-real-time risk management through the implementation of a continuous monitoring processes.
- **NIST SP 800-53, Rev 3: *Recommended Security Controls for Federal Information Systems and Organizations*** defines many of the technical security controls needed to implement both SP 800-137 and SP 800-39.

Continuous Monitoring Defined

Let's first look at what NIST means by "Continuous Monitoring." According to NIST, most organizations tend to associate monitoring with periodic security assessments, system reauthorizations, data analysis and associated reporting. In addition to these *passive* security practices, NIST states that a well-designed continuous monitoring strategy must also include *proactive* testing to effectively mitigate risk. NIST describes continuous monitoring as helping to "ensure ongoing situational awareness and control of the security of systems across the organization and *ongoing* knowledge of associated threats and vulnerabilities, despite inevitable changes to organizational information systems and their environments of operation." (NIST SP 800-137, page 6)

Addressing NIST 800-137 Guidance with CORE INSIGHT Enterprise

CORE INSIGHT Enterprise offers a security testing and measurement solution that enables you to continuously and proactively assess the security of your critical information assets – directly mapping to the guidance in NIST SP 800-137. By traversing exploitable web application, network and client-side weaknesses throughout your environment, INSIGHT reveals exposed paths to systems, databases and data types. It delivers clear, definitive metrics for efficiently validating security controls and addressing data breach threats.

NIST cites the following processes as "essential to organization-wide continuous monitoring:"

Ongoing assessment of security controls (including system-specific, hybrid, common controls and PM controls) with assessment frequencies based on an organization-wide continuous monitoring strategy. (NIST Special Publication 800-137, page 10)

- How CORE INSIGHT can help:
 - Assesses IPS/IDS, firewalls and other defenses against real-world network and web application attack techniques
 - Automated attack path planning, combined with real-world exploit-based testing, dynamically reveals paths that attackers and malicious insiders would use to access sensitive assets
 - Proactively identifies weaknesses posing imminent risks

Configuration management and change control processes for organizational information systems, throughout their SDLCs, and with consideration of their operating environments and their role(s) in supporting the organization's missions and core business processes. (NIST Special Publication 800-137, page 10)

- How CORE INSIGHT can help:
 - Able to run continuously to assess changing infrastructure against the latest threats
 - Ensures that defensive technologies are configured and updated properly to protect against current threats
 - Integrates with ticketing and change management systems for seamless vulnerability management
 - Dynamically tests custom and COTS applications using the same techniques as attackers
 - Can easily scale to repeatedly test environments with large numbers of targets
 - Ensures that development resources can focus on addressing *proven* security issues

Security impact analyses (SIA) on changes to organizational information systems and their environments of operation for any adverse security impact to systems, mission/business and/or organizational functions which said systems support. (NIST Special Publication 800-137, page 10)

- How CORE INSIGHT can help:
 - Able to test (and retest) continuously to assess changing infrastructure against the latest threats
 - Automated attack path planning, combined with real-world exploit-based testing, dynamically reveals paths that attackers and malicious insiders could use to access sensitive assets
 - Assesses systems designated as critical and delivers proactive alerts regarding the latest threats and impacts to those systems

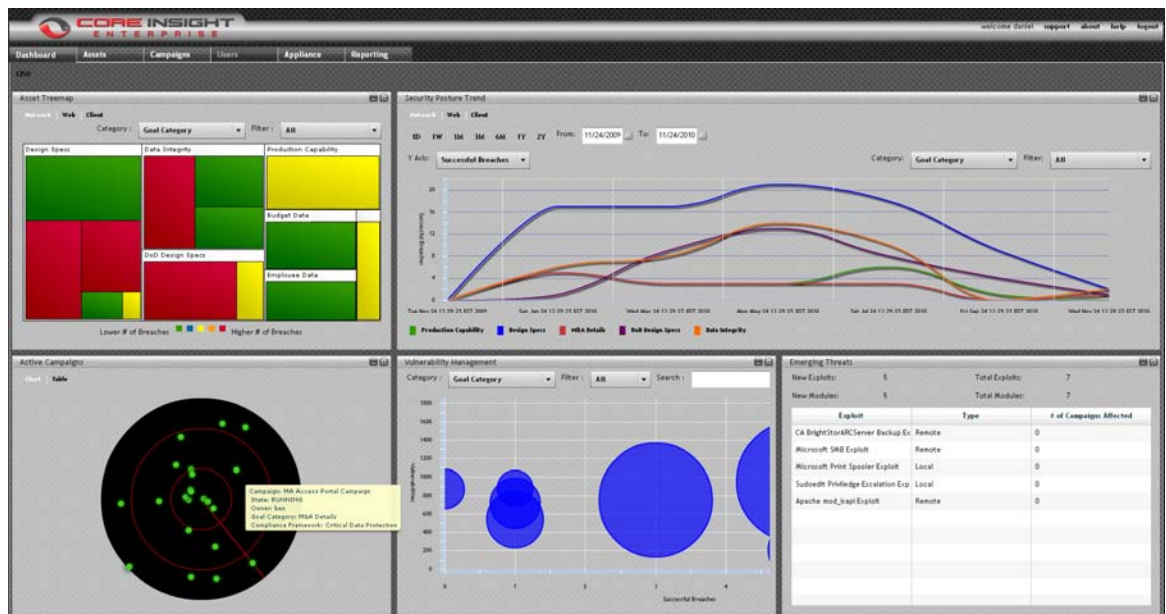
Security status reporting to organizational officials designed to enable data-driven risk mitigation decisions with minimal response times and acceptable data latencies. Considerations include organization relevant threat data. (NIST Special Publication 800-137, page 10)

- How CORE INSIGHT can help:
 - Conducts proactive, real-time assessments of assets identified as critical to the agency
 - Assimilates data from multiple sources (e.g., network and web scanners) to validate potential threats as real
 - Delivers data using terminology specific to your agency, system, location, mandates, data types, etc.
 - Benchmarks security posture, tracks and demonstrates security standing over time

Optimizing Security Metrics

The efficiency and effectiveness of vulnerability remediation initiatives are highly dependent on the quality of security assessment data. It's therefore essential to measure and collect data in a way that most accurately pinpoints and validates *actual* risks to critical assets in your IT environment. NIST recognizes this by not only emphasizing security data collection, but also specifying that the data be meaningful and actionable: "Metrics are measures that have been organized into meaningful information to support decision making. Metrics are developed for system-level data to make it meaningful in the context of mission/business or organizational risk management." (NIST Special Publication 800-137, page 26)

CORE INSIGHT Enterprise enables you to collect and present meaningful data that accurately reflects your IT security standing and allows you to communicate effectively with various constituencies such as contractors and inter-agency personnel, as well as external agencies, centers and facilities. With the solution's dashboards and reports, you benchmark and track your security posture over time – generating metrics reported in terms relevant to your agency, systems, locations, compliance mandates and data types.



The CORE INSIGHT Enterprise CSO Dashboard

CORE INSIGHT Enterprise delivers a wide variety of proactive security data, including:

Security assessment results and risk trends over time

- Track numbers of exposures proven, assets tested and tests conducted
- Show the progress of security testing and vulnerability remediation over time
- Compare and contrast individual tests by location, business unit, system category, data category, or compliance area
- Identify areas with increasing risk requiring additional resources

Emerging threats and how they relate to your testing activities

- Monitor commercial-grade exploits and other testing modules as they are added to INSIGHT
- See how the latest exploits map to your environment
- Quantify critical, exploitable weaknesses as they are distilled from imported vulnerability (network and web) scan data

Snapshots of current security levels across different areas of your IT infrastructure

- View the relative sizes of tested environments and numbers of penetration exposures
- Drill down to quantified test data, asset owner contact info, etc.

Addressing NIST 800-39 Guidance with CORE INSIGHT Enterprise

NIST SP 800-39, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*, establishes a Risk Management Framework (RMF) that promotes the concept of near-real-time risk management through the implementation of robust continuous monitoring processes (as outlined in SP 800-137). The RMF encourages the use of automation and automated support tools to provide senior leaders with the necessary information to take credible, risk-based decisions regarding the organizational information systems supporting their core missions and business functions.

Commercially available automated tools, such as those described in NIST SP 800-53 “support situational awareness, or [maintain] awareness of the security state of information systems on an ongoing basis through enhanced monitoring processes.” However, NIST also cites that those tools, as well as corresponding processes designed to generate risk data, are not being deployed in a timely fashion. As a result, system security assessments and authorizations are usually based on infrequently conducted vulnerability scans that test security controls at a single point in time – leaving security professionals unable to measure the real risk to systems between security control test cycles.

To most effectively address operational risk, NIST SP 800-39 specifically calls for risk management to be carried out as a holistic, organization-wide activity that addresses risk from the strategic level to the tactical level – thereby ensuring that risk-based decision making is integrated into every aspect of the organization.

NIST SP 800-39 addresses key areas of IT security including:

Risk Assessments

One major component of the Risk Management Framework covers how organizations *assess* risk within the context of their overall risk strategy. NIST prescribes that all entities determine:

- (i) threats to organizations (i.e., operations, assets, or individuals)
- (ii) vulnerabilities internal and external to organizations
- (iii) the harm (i.e., consequences/impact) to organizations that may occur given the potential for threats exploiting vulnerabilities
- (iv) the likelihood that harm will occur

Risk Tolerance

There is no standard level of organizational risk tolerance. Yet the ramifications of risk decisions based on risk tolerance are profound: Less risk-tolerant organizations may fail to achieve needed mission/business capabilities in their efforts to avoid what appear to be unacceptable risks.

Conversely, more risk-tolerant organizations may focus on near-term mission/business efficiencies at the expense of exposing their environments to security breaches. It's therefore imperative that organizations exercise due diligence in determining risk tolerance – and recognize how fundamental this decision is to the effectiveness of their risk management programs.

Trust and Trustworthiness

The concept of trustworthiness can also be applied to information systems and the information technology products and services that compose those systems. Trustworthiness expresses the degree to which information systems (internal, external and partner) can preserve the confidentiality, integrity and availability of the information being processed, stored or transmitted. A key factor affecting the trustworthiness of information systems is *Security functionality* (i.e., the security features/functions employed within the system). "Security functionality can be obtained by employing within organizational information systems and environments of operation, a combination of management, operational and technical security controls from NIST Special Publication 800-53."

Risk framing

Risk framing is the set of assumptions, constraints, risk tolerances, and priorities/trade-offs that shape an organization's approach to managing risk. These include identifying assumptions about threats, vulnerabilities, consequences/impact, and likelihood. The inputs for risk framing include *Threat Sources* and *Vulnerabilities*.

Threat Sources

Threat sources are events having undesirable consequences or adverse impacts on organizational operations and assets, individuals and other organizations. Threat sources include hostile cyber/physical attacks, and NIST necessitates that organizations provide a succinct characterization of the types of tactics, techniques and procedures employed by adversaries that are to be addressed by safeguards and countermeasures (i.e., security controls). When examining threat sources and events, organizations should identify threat capabilities, intentions and targeting information from all available sources.

Vulnerabilities

In addition to characterizing threat sources and events, organizations should identify approaches used to characterize vulnerabilities. Vulnerabilities can be associated with exploitable weakness or deficiencies in the hardware, software or firmware components that compose organizational information systems (or the security controls employed within or inherited by those systems; or mission/business processes, enterprise architectures; or information security architectures implemented by organizations).

How CORE INSIGHT Enterprise Addresses Risk Management Objectives

By traversing exploitable web application, network and client-side weaknesses throughout your environment, INSIGHT can reveal the precise risk to systems, databases and data types that you deem as "critical," thereby helping you lower your risk profile. Unlike other security solutions, it does not scan for potential vulnerabilities, monitor for incidents, or model threats; it proactively uses the same offensive techniques that criminals employ to find and exploit weaknesses that expose critical assets to data breaches. In addition, INSIGHT enables you to:

- Continuously reassess the security of assets as new attack techniques surface, as new vulnerabilities are discovered, and infrastructure changes.
- Test the internal and external relationships between inter-connected IT systems.
- Determine remediation priorities to ensure that security improvements are aimed at addressing the most critical, true risks.

Continuous Monitoring and the Penetration Testing Security Control (NIST SP 800-53, rev. 3)

According to NT SP 800-53:

A continuous monitoring program allows an organization to maintain the security authorization of an information system over time in a highly dynamic environment of operation with changing threats, vulnerabilities, technologies, and missions/business processes. Continuous monitoring of security controls facilitates near real-time risk management and promotes organizational situational awareness with regard to the security state of the information system. The organization assesses the security controls in an information system as part of:

- *security authorization or reauthorization;*
- *meeting the FISMA requirement for annual assessments;*
- *continuous monitoring; and*
- *testing/evaluation of the information system as part of the system development life cycle process.*

(NIST Special Publication 800-53, Revision 3, page F-32/33)

One of the specific control enhancements outlined in the guidance promotes the use of penetration testing to “improve the readiness of the organization [and] to improve the security state of the system and organization.” (NIST Special Publication 800-53, Revision 3, page F-34)

Penetration Testing Defined by NIST

NIST SP 800-53 describes penetration in the following way:

Penetration testing exercises both physical and technical security controls. A standard method for penetration testing consists of ...

- *pretest analysis based on full knowledge of the target system;*
- *pretest identification of potential vulnerabilities based on pretest analysis; and*
- *testing designed to determine exploitability of identified vulnerabilities.*

Red team exercises are conducted as a simulated adversarial attempt to compromise organizational missions and/or business processes to provide a comprehensive assessment of the security capability of the information system and organization. While penetration testing may be laboratory-based testing, red team exercises are intended to be more comprehensive in nature and reflect real-world conditions.

Information system monitoring, malicious user testing, penetration testing, red-team exercises, and other forms of security testing (e.g., independent verification and validation) are conducted to improve the readiness of the organization by exercising organizational capabilities and indicating current performance levels as a means of focusing organizational actions to improve the security state of the system and organization. Vulnerabilities

uncovered during red team exercises are incorporated into the vulnerability remediation process.

(NIST Special Publication 800-53, Revision 3, page F-34).

Maximizing the Value of Existing Vulnerability Management Activities

Vulnerability scanning is also a specific control within the guidance. NIST recommends scanning for vulnerabilities in systems and applications on a regular basis. However, for further vulnerability validation, NIST advocates “malicious user testing, penetration testing, red-team exercises, and other forms of security testing.” (NIST Special Publication 800-53, Revision 3, page F-37)

Specifically, NIST recommends employing an independent penetration testing agent or penetration testing team to:

- *Conduct a vulnerability analysis on the information system; and*
- *Perform penetration testing on the information system based on the vulnerability analysis to determine the exploitability of identified vulnerabilities.*

Furthermore, NIST recommends that penetration testing include:

- *pre-test identification of potential vulnerabilities based on pre-test analysis; and*
- *testing designed to determine exploitability of identified vulnerabilities.*

(NIST Special Publication 800-53, Revision 3, page F-95)

Addressing NIST SP 800-53a Security Testing Guidance with CORE INSIGHT Enterprise and CORE IMPACT Pro

Using Core Security’s test and measurement solutions, CORE INSIGHT Enterprise and CORE IMPACT Pro, security professionals proactively validate their security controls while revealing actual paths that attackers could take to expose critical assets.

CORE INSIGHT Enterprise continuously replicates threats while seeking to compromise defined business assets through web, network and client-side channels. CORE INSIGHT Enterprise helps security executives to benchmark and measure enterprise-wide security posture, verify actual business risks, and validate mandated security controls.

CORE IMPACT Pro replicates attacks across web applications, network systems, endpoints, email users Wifi networks, and network devices. Users have granular control over the largest library of commercial-grade exploits available, plus a full complement of pre- and post-exploitation capabilities.

Core’s products address a number of Penetration Testing best practices originally specified in *NIST SP 800-53a, Appendix G*:

What NIST SP 800-53a Says	How Core Security Solutions Can Help
<p>Testing Targets and Attacker Profiles</p> <p>“Organizations specify which components within the information system are subject to penetration testing and the attacker’s profile to be adopted throughout the penetration testing exercises.”</p>	<p>Core allows security testers to assess IT systems of their choosing from the standpoint of an attacker, in a safe and controlled manner. Core products also assess a broader range of attack vectors than any other penetration testing solutions available today.</p>
<p>Penetration Testing Training</p> <p>“Organizations train selected personnel in the use and maintenance of penetration testing tools and techniques.”</p>	<p>All customers receive training for multiple users regarding how to best use the solution to perform automated testing within their unique environments.</p>
<p>Testing Tool Updates</p> <p>“Effective penetration testing tools should have the capability to readily update the list of attack techniques and exploitable vulnerabilities used during the exercises.”</p> <p>“Organizations should update the list of attack techniques and exploitable vulnerabilities used in penetration testing in accordance with an organizational assessment of risk or when significant new vulnerabilities or threats are identified and reported.”</p>	<p>All customers receive an average of 30+ security updates each month, including new exploits and other testing modules as they become available. The result of cutting-edge vulnerability research and threat expertise generated across the CoreLabs research, Core Engineering, and Core Security Consulting Services groups, the updates enable customers to stay ahead of the complex information security threats facing their organizations on a daily basis.</p>
<p>Automated Penetration Testing</p> <p>“Whenever possible, organizations should employ tools and attack techniques that include the capability to perform penetration testing exercises on information systems and security controls in an automated manner.”</p>	<p>Widely recognized for their comprehensive, commercial-grade automated testing capabilities, Core solutions enable security staff to scale assessments across networks, endpoints and web applications at a breadth and depth never before possible. This is accomplished by automating complex, time-consuming manual tasks that have traditionally required specialized training.</p>
<p>Reporting and Vulnerability Prioritization</p> <p>“The information obtained from the penetration testing process should be shared with appropriate personnel throughout the organization to help prioritize the vulnerabilities in the information system that are demonstrably subject to compromise by attackers of a profile equivalent to the ones used in the penetration testing exercises.”</p>	<p>Core’s products provide precise actionable data about the targeted network, hosts and applications; audits of all tests performed; and details about proven vulnerabilities in clear, easily understood formats, allowing organizations to share test results with multiple constituencies to better prioritize remediation efforts. All Core solutions import and assess data from network and web scanning technologies, thereby discerning true exposures from hundreds or thousands of potential threats.</p>

What NIST SP 800-53a Says	How Core Security Solutions Can Help
<p>Integration Between Penetration Testing and Patch/Vulnerability Management</p> <p>“Penetration testing should be integrated into the network security testing process and the patch and vulnerability management process.”</p>	<p>In addition to providing automated network penetration testing capabilities, our solutions integrate with leading vulnerability scanners and patch management tools to improve the productivity and effectiveness of overall vulnerability management efforts.</p> <p>Supported network scanning solutions:</p> <ul style="list-style-type: none"> • Nessus™ • GFI LANguard™ • Lumension PatchLink Scan™ • Nmap Security Scanner • eEye Retina® • IBM ISS® • nCircle IP360® • Qualys QualysGuard® <p>Supported web scanning solutions:</p> <ul style="list-style-type: none"> • IBM Rational AppScan® • HP WebInspect® • NTOSpider® <p>Supported patch management solution:</p> <ul style="list-style-type: none"> • Lumension PatchLink Update™
<p>Going Beyond Vulnerability Scanning</p> <p>“An effective penetration test goes beyond vulnerability scanning, to provide explicit and often dramatic proof of mission risks and an indicator of the level of effort an adversary would need to expend in order to cause harm to the organization’s operations and assets, to individuals and to other organizations.”</p>	<p>Core’s solutions use patented technology to mirror multi-vectored, privilege escalation and pivoting methods employed by today’s sophisticated hackers and malware authors. By utilizing goal-based testing, organizations can identify the complex paths that attackers traverse across multiple layers of IT infrastructure to expose critical data and systems.</p>
<p>Real-World Testing</p> <p>“An effective penetration test approaches the information system as the adversary would, considering vulnerabilities, incorrect system configurations, trust relationships between organizations, and architectural weaknesses in the environment under test.”</p>	<p>Core’s solutions give testers the ability to see how multiple vulnerabilities across various assets can be exploited to pivot deeper into underlying systems. They mimic the activity of popular attacks such as injection attacks, Trojans and botnets that expand their scope over time and target numerous vulnerabilities. It also illustrates holes and points of failed integration across defensive security systems that allow multistaged attacks to infiltrate IT operations and validates the efficacy of existing security measures in warding off complex threats.</p>



What NIST SP 800-53a Says	How Core Security Solutions Can Help
<p>Validation of Existing Security Controls</p> <p>“An effective penetration test validates existing security controls (including risk mitigation mechanisms such as firewalls, intrusion detection and prevention systems).”</p>	<p>Core’s solutions allow organizations to proactively test the efficacy of their network, endpoint, web application and email defenses both to ensure they are working properly, and to aid in the process of evaluating products to determine ROI and influence future buying decisions.</p>
<p>Activity Logging</p> <p>“An effective penetration test provides a verifiable and reproducible log of all the activities performed during the test.”</p>	<p>Core’s solutions track all testing and user activities and create detailed logs of all user behavior as well as logging targeted network and hosts, penetration tests performed, exploits used and details about proven vulnerabilities.</p>
<p>Actionable Results for Effective Remediation</p> <p>“An effective penetration test provides actionable results with information about possible remediation measures for the successful attacks performed.”</p>	<p>Core’s solutions arm customers with the highly specific data they need to reduce vulnerabilities, prioritize remediation efforts and better manage risks; including providing links to relevant remediation data to help guide customers into the next stage of the vulnerability management process.</p>

Core’s security testing and measurement solutions provide some of the most effective means by which to demonstrate your adherence to FISMA and NIST SP 800 (137 and 53) guidance. By acquiring the ability to carry out regular, controlled and safe assessments across a wide range of vectors, federal agencies are able to provide explicit proof of their adherence, along with associated documentation, to GAO auditors, Cyber Scope and other governing bodies as they implement and manage their continuous monitoring programs.

Next Steps ...

For additional information on the Core security family of comprehensive security testing products, please contact us at 617-399-6980 or via email at federalsales@coresecurity.com. You can also visit our website at www.coresecurity.com.



Appendix: The Office of Management and Budget (OMB) and the Continuous Asset Evaluation, Situational Awareness, and Risk Scoring (CAESARS) Reference Architecture

In a memorandum dated April 5, 2010, the OMB Chief Information Officer restated their commitment to continuous monitoring, "Continuous monitoring is the backbone of true security." This is security that moves beyond compliance and paperwork. The threats to our nation's information security continue to evolve and therefore our approach to cybersecurity must confront these new realities on a real-time basis.

OMB memo memorandum (M-10-15), provides guidelines to the federal departments and agencies (D/A) for Federal Information Security Management Act (FISMA) reporting. The OMB memorandum urges D/A to continuously monitor security-related information from across the enterprise in a manageable and actionable way. The reference architecture, the Continuous Asset Evaluation, Situational Awareness, and Risk Scoring (CAESARS) – is provided to D/As to develop this important capability. The document states that continuous monitoring of computing and network assets requires ...

... up-to-date knowledge of the security posture of every workstation, server, and network device, including:

- *operating system,*
- *software*
- *patches*
- *vulnerabilities and*
- *antivirus signatures*

Information security managers use the summary and detailed information to manage and report the security posture of their respective agency. The objective of the Continuous Asset Evaluation, Situational Awareness, and Risk Scoring reference architecture (CAESARS) is to provide a summary of the various posture monitoring and risk scoring systems that can be applied by agencies seeking to use risk scoring principles in their information security program. At its core, CAESARS is an architecture framework and decision support system.

CAESARS and Cyberscope

The OMB states that agencies should not build separate systems for reporting. Any reporting should be a by-product of agencies' continuous monitoring programs and security management tools. The types of information that OMB requires to be reported through CyberScope are broader in scope than the status of individual assets, which are the focus of the CAESARS reference architecture. Nevertheless, the CAESARS reference architecture can directly support the achievement of some of the OMB objectives by ensuring that the inventory, configuration, and vulnerabilities of systems, services, hardware, and software are consistent, accurate, and complete. A fundamental underpinning of both the CAESARS reference architecture and the OMB reporting objectives is full situational awareness of all agency IT assets.