Chief Information Officer

Section Report

2009

Annual FISMA Report

Nuclear Regulatory Commission

Question 1: FISMA Systems Inventory & Question 2: Certification and Accreditation, Security Controls Testing, and Contingency Plan Testing

1. Identify the number of Agency and contractor systems by component and FIPS 199 impact level (low, moderate, high). Please also identify the number of systems that are used by your Agency but owned by another federal Agency (i.e., ePayroll, etc.) by component and FIPS 199 impact level.

2. For the Total Number of Systems Identified by Component/Bureau and FIPS System Impact Level in the table for Question 1, identify the number and percentage of systems which have: a current certification and accreditation, security controls tested and reviewed within the past year, and a contingency plan tested within in accordance with policy.

		FISMA Inventory				Certification and Accreditation (C&A) and Testing					
		1a. Agency Systems	1b. Contractor Systems	1c. Systems owned by another Federal Agency	1d. Total Systems	2a. Number of systems certified and accredited		2b. Number of systems for which security controls have been tested and reviewed in the past year		2c. Number of systems for which contingency plans have been tested in accordance with policy	
Agency/ Component	Category	Number	Number	Number	Total Number	Total Number	% of Total	Total Number	% of Total	Total Number	% of Total
NRC	High	8	1	0	9	9	100	9	100	9	100
	Moderate	14	1	0	15	14	93	15	100	15	100
	Low	0	1	0	1	1	100	1	100	1	100
	Not Categorized	0	0	0	0	0	0	0	0	0	0
	Sub Total	22	3	0	25	24	96	25	100	25	100

No C&A	UPI
License Tracking System (LTS)	42900010402100100111035

No C&A Explanation: *The ATO for LTS was delayed due to system development issues. LTS is now scheduled for completion by the end of this calendar year.*

Question 1: FISMA Systems Inventory & Question 2: Certification and Accreditation, Security Controls Testing, and Contingency Plan Testing

		FISMA Inventory				Certification and Accreditation (C&A) and Testing					
		1a. Agency Systems	1b. Contractor Systems	1c. Systems owned by another Federal Agency	1d. Total Systems	2a. Number of systems certified and accredited		2b. Number of systems for which security controls have been tested and reviewed in the past year		2c. Number of systems for which contingency plans have been tested in accordance with policy	
Agency/ Component	Category	Number	Number	Number	Total Number	Total Number	% of Total	Total Number	% of Total	Total Number	% of Total
Agency Totals	High	8	1	0	9	9	100	9	100	9	100
	Moderate	14	1	0	15	14	93	15	100	15	100
	Low	0	1	0	1	1	100	1	100	1	100
	Not Categorized	0	0	0	0	0	0	0	0	0	0
	Total Systems	22	3	0	25	24	96	25	100	25	100

Question 3: Implementation of Security Controls in NIST Special Publication 800-53

What tools and techniques do you use for continuous monitoring?

Tool/Technique Name	Tool Category
Annual security control testing	Vulnerability Scanners
Quarterly POA&M reporting and reviews	Other
Configuration Management and Control	Other
Annual Contingency plan testing	Other

Question 4: Incident Detection, Monitoring and Reponse Capabilities

4a. What tools, techniques, technologies, etc., does the Agency use for incident detection?

Tool/Technique Name	Tool Category
Antivirus	Antimalware Software
Enterasys Dragon	Intrusion Detection and Prevention Systems
Snort	Intrusion Detection and Prevention Systems
Host-based system integrity software	Intrusion Detection and Prevention Systems
Activeworx, Blue Coat Reporter, and Finjan	Log Analysis Software
Content filtering, Firewall, Poxy	Network Access Control

4b. How many systems (or networks of systems) are protected using the tools, techniques and technologies described in 4(a) above?

25

4c. How often does the Agency log and monitor activities involving access to and modification of critical information?

96 % to 100 %

4d. What percentage of systems maintain audit trails that provide a trace of user actions?

96 % to 100 %

4e. Does the Agency maintain an incident handling and response capability?

Yes

4f. If the answer to 4(e) is yes, what percentage of systems are operated within the Agency's incident handling and response capability?

96 % to 100 %

4g. What tools, techniques, technologies, etc., does the Agency use for incident handling and response?

Tool/Technique Name	Tool Category
US-CERT	Event Correlation Machines
Computer Security Incident Response Team (CSIRT)	Other

Question 5: Security Awareness Training

5a. Report the following for your Agency:

5a(1). Total number of people with log-in privileges to Agency systems.

4,840

5a(2). Number of people with log-in privileges to Agency systems that received information security awareness training during the past fiscal year, as described in NIST Special Publication 800-50, "Building an Information Technology Security Awareness and Training Program."

4,730 (98%)

5a(3). Number of people with log-in privileges to Agency systems that received information security awareness training using an ISSLOB shared service center. (Breakout total for b.)

4,730 (98%)

5a(4). Total number of employees with significant information security responsibilities.

403

5a(5). Number of employees with significant security responsibilities that received specialized training as described in NIST Special Publication 800-16, "Information Technology Security Training Requirements: A Role-and Performance-Based Model".

130 (32 %)

5a(6). Total costs for providing information security training in the past fiscal year (in $'s).

$122,128

5b. Briefly describe the training provided in 5a(2) and 5a(5) and how you measure its effectiveness:

Comments:	Annual Computer Security Awareness, ISSO Awareness, System Administration Awareness, laptop Security Controls Course, NRC utilized the ISS LoB training for FY09 which does not have testing mechanism to measure effectiveness.

Question 6: Peer-to-Peer File Sharing

Does the Agency explain policies regarding the use of peer-to-peer file sharing in information security awareness training, ethics training, or any other Agency-wide training?

Yes

Question 7: Configuration Management

7a. Is there an Agency-wide configuration policy?

Yes

7a(1). Enter the systems/platforms/applications for which configuration policies exist and provide the implementation status. Identify all that are applicable.

OS/Platform/System	Implementation Status
Cisco IOS	**Policy fully implemented** **What tools and techniques is your Agency using for monitoring compliance?** Tool/Technique Name: CIS Benchmark - http://www.cisecurity.org/ — Tool Category: Configuration Scanners
Cisco Pix Firewall	**Policy fully implemented** **What tools and techniques is your Agency using for monitoring compliance?** Tool/Technique Name: CIS Benchmark - http://www.cisecurity.org/ — Tool Category: Configuration Scanners

<table>
<tr><th>OS/Platform/System</th><th>Implementation Status</th></tr>
<tr><td>HP HP-UX 10</td><td>Policy fully implemented
What tools and techniques is your Agency using for monitoring compliance?
<table>
<tr><th>Tool/Technique Name</th><th>Tool Category</th></tr>
<tr><td>CIS Benchmark - http://www.cisecurity.org/</td><td>Configuration Scanners</td></tr>
<tr><td>DISA Standards</td><td>Configuration Scanners</td></tr>
</table></td></tr>
<tr><td>IBM AIX 5</td><td>Policy fully implemented
What tools and techniques is your Agency using for monitoring compliance?
<table>
<tr><th>Tool/Technique Name</th><th>Tool Category</th></tr>
<tr><td>CIS Benchmark - http://www.cisecurity.org/</td><td>Configuration Scanners</td></tr>
<tr><td>DISA Standards</td><td>Configuration Scanners</td></tr>
</table></td></tr>
<tr><td>Microsoft Office 2003</td><td>Policy fully implemented
What tools and techniques is your Agency using for monitoring compliance?
<table>
<tr><th>Tool/Technique Name</th><th>Tool Category</th></tr>
<tr><td>DISA Gold</td><td>Configuration Scanners</td></tr>
</table></td></tr>
<tr><td>Microsoft Office 2007</td><td>Policy fully implemented
What tools and techniques is your Agency using for monitoring compliance?
<table>
<tr><th>Tool/Technique Name</th><th>Tool Category</th></tr>
<tr><td>DISA Gold</td><td>Configuration Scanners</td></tr>
</table></td></tr>
<tr><td>Microsoft Windows Server 2000</td><td>Policy fully implemented
What tools and techniques is your Agency using for monitoring compliance?
<table>
<tr><th>Tool/Technique Name</th><th>Tool Category</th></tr>
<tr><td>DISA Gold</td><td>Configuration Scanners</td></tr>
</table></td></tr>
<tr><td>Microsoft Windows 2000 Active Directory</td><td>Policy fully implemented
What tools and techniques is your Agency using for monitoring compliance?
<table>
<tr><th>Tool/Technique Name</th><th>Tool Category</th></tr>
<tr><td>DISA Gold</td><td>Configuration Scanners</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>OS/Platform/System</th><th>Implementation Status</th></tr>
<tr><td>Microsoft Windows Server 2003</td><td>Policy fully implemented
What tools and techniques is your Agency using for monitoring compliance?<table><tr><th>Tool/Technique Name</th><th>Tool Category</th></tr><tr><td>DISA Gold</td><td>Configuration Scanners</td></tr></table></td></tr>
<tr><td>Microsoft Windows Server 2008</td><td>Policy fully implemented
What tools and techniques is your Agency using for monitoring compliance?<table><tr><th>Tool/Technique Name</th><th>Tool Category</th></tr><tr><td>DISA Gold</td><td>Configuration Scanners</td></tr></table></td></tr>
<tr><td>Microsoft Windows XP</td><td>Policy fully implemented
What tools and techniques is your Agency using for monitoring compliance?<table><tr><th>Tool/Technique Name</th><th>Tool Category</th></tr><tr><td>DISA Gold</td><td>Configuration Scanners</td></tr></table></td></tr>
<tr><td>Oracle Database 8i</td><td>Policy fully implemented
What tools and techniques is your Agency using for monitoring compliance?<table><tr><th>Tool/Technique Name</th><th>Tool Category</th></tr><tr><td>CIS Benchmark - http://www.cisecurity.org</td><td>Configuration Scanners</td></tr></table></td></tr>
<tr><td>Oracle Database 9i</td><td>Policy fully implemented
What tools and techniques is your Agency using for monitoring compliance?<table><tr><th>Tool/Technique Name</th><th>Tool Category</th></tr><tr><td>CIS Benchmark - http://www.cisecurity.org</td><td>Configuration Scanners</td></tr></table></td></tr>
<tr><td>Oracle Database 10g</td><td>Policy fully implemented
What tools and techniques is your Agency using for monitoring compliance?<table><tr><th>Tool/Technique Name</th><th>Tool Category</th></tr><tr><td>CIS Benchmark - http://www.cisecurity.org</td><td>Configuration Scanners</td></tr></table></td></tr>
</table>

<table>
<tr><th>OS/Platform/System</th><th>Implementation Status</th></tr>
<tr><td>Sun Solaris 9</td><td>Policy fully implemented
What tools and techniques is your Agency using for monitoring compliance?
<table>
<tr><th>Tool/Technique Name</th><th>Tool Category</th></tr>
<tr><td>CIS Benchmark - http://www.cisecurity.org</td><td>Configuration Scanners</td></tr>
</table></td></tr>
<tr><td>Sun Solaris 10</td><td>Policy fully implemented
What tools and techniques is your Agency using for monitoring compliance?
<table>
<tr><th>Tool/Technique Name</th><th>Tool Category</th></tr>
<tr><td>CIS Benchmark - http://www.cisecurity.org</td><td>Configuration Scanners</td></tr>
</table></td></tr>
<tr><td>Microsoft .NET Framework 1</td><td>Policy fully implemented
What tools and techniques is your Agency using for monitoring compliance?
<table>
<tr><th>Tool/Technique Name</th><th>Tool Category</th></tr>
<tr><td>NSA - http://www.nsa.gov/snac</td><td>Configuration Scanners</td></tr>
</table></td></tr>
</table>

7b. Indicate the status of the implementation of FDCC at your Agency:

7b(1). Agency has documented deviations from FDCC standard configuration.

Yes

7b(2). New Federal Acquisition Regulation 2008-004 language, which modified "Part 39-Acquisition of Information Technology," is included in all contracts related to commons security settings.

Yes

7b(3). List the percentage of workstations and laptops that are in compliance.

90 % to 100 %

Question 8: Systems Incident Reporting

Indicate whether or not the Agency follows documented policies and procedures for reporting incidents internally, to US-CERT and to law enforcement.

8a. How often does the Agency follow documented policies and procedures for identifying and reporting incidents internally?

96 % to 100 %

8b. How often does the Agency comply with documented policies and procedures for timelines of reporting to US-CERT?

96 % to 100 %

8c. How often does the Agency follow documented policies and procedures for reporting to law enforcement?

96 % to 100 %

Question 9: Performance Metrics for Security Policies and Procedures

Please provide three (3) outcome/output-based performance metrics your Agency uses to measure the effectiveness or efficiency of security policies and procedures. The metrics must be different than the ones used in these FISMA reporting instructions, and can be tailored from NIST's Special Publication 800-55 "Performance Measurement Guide for Information Security."

Metric Name	Metric Description
Implementation measures	Percentage of systems with approved ATO, and percentage of systems with policy compliance.
Effectiveness Measures	Annual scanning for operating system vulnerabilities, and security control implementation
Impact Measures	Degree of overall public trust gained by information security program

Question 10: HSPD-12

Number of FISMA applications in which Federal employees and contractors are using HSPD-12 Personal Identity Verification credentials for access.

1