

# 2004 FISMA Report

---

Agency:

Date Submitted:

Submitted By:

Contact Information:

Name:	Jacqueline E. Silber
E-mail:	<a href="mailto:JES@nrc.gov">JES@nrc.gov</a>
Phone:	301-415-1759



**“NRC Report on the Implementation of the  
Federal Information Security Management Act  
For Fiscal Year 2004”  
Prepared by the NRC Chief Information Officer  
October 6, 2004**





A.3. Evaluate the degree to which the following statements reflect the status in your agency, by choosing from the responses provided in the drop down menu. If appropriate or necessary, include comments in the Comment area provided below.

Statement	Evaluation
a. Agency program officials and the agency CIO have used appropriate methods to ensure that contractor provided services or services provided by another agency for their program and systems are adequately secure and meet the requirements of FISMA, OMB pol	Almost Always, or 96-100% of the time
b. The reviews of programs, systems, and contractor operations or facilities, identified above, were conducted using the NIST self-assessment guide, <a href="#">800-26</a> .	Frequently, or 71-80% of the time
c. In instances where the NIST self-assessment guide was not used to conduct reviews, the alternative methodology used addressed all elements of the NIST guide.	Almost Always, or 96-100% of the time
d. The agency maintains an inventory of major IT systems and this inventory is updated at least annually.	Almost Always, or 96-100% of the time
e. The OIG was included in the development and verification of the agency's IT system inventory.	Almost Always, or 96-100% of the time
f. The OIG and the CIO agree on the total number of programs, systems, and contractor operations or facilities.	Almost Always, or 96-100% of the time
g. The agency CIO reviews and concurs with the major IT investment decisions of bureaus (or major operating components) within the agency.	Almost Always, or 96-100% of the time
Statement	Yes or No
h. The agency has begun to assess systems for e-authentication risk.	Yes
i. The agency has appointed a senior agency information security officer that reports directly to the CIO.	Yes

Comments:



**Section C: OIG Assessment of the POA&M Process**

**NOTE: Section C should \*ONLY\* be completed by the OIG. The CIO should leave this section blank.**

**To enter data in allowed fields, use password: fisma**

C.1. Through this question, and in the format provided below, assess whether the agency has developed, implemented, and is managing an agency-wide plan of action and milestone (POA&M) process. This question is for IGs only. Evaluate the degree to which the following statements reflect the status in your agency by choosing from the responses provided in the drop down menu. If appropriate or necessary, include comments in the Comment area provided below.

**C.1**

Statement	Evaluation
a. Known IT security weaknesses, from all components, are incorporated into the POA&M.	
b. <b>Program officials</b> develop, implement, and manage POA&Ms for systems they own and operate (systems that support their program or programs) that have an IT security weakness.	
c. Program officials report to the CIO on a regular basis (at least quarterly) on their remediation progress.	
d. <b>CIO</b> develops, implements, and manages POA&Ms for every system they own and operate (a system that supports their program or programs) that has an IT security weakness.	
e. CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis.	
f. The POA&M is the authoritative agency <b>and</b> IG management tool to identify and monitor agency actions for correcting information and IT security weaknesses.	
g. System-level POA&Ms are tied directly to the system budget request through the IT business case as required in OMB budget guidance (Circular A-11).	
h. OIG has access to POA&Ms as requested.	
i. OIG findings are incorporated into the POA&M process.	
j. POA&M process prioritizes IT security weaknesses to help ensure that significant IT security weaknesses are addressed in a timely manner and receive appropriate resources.	

**Comments:**

**C.1 OIG Assessment of the Certification and Accreditation Process**

Section C should only be completed by the OIG. OMB is requesting IGs to assess the agency's certification and accreditation process in order to provide a qualitative assessment of this critical activity. This assessment should consider the quality of the Agency's certification and accreditation process. Any new certification and accreditation work initiated after completion of NIST Special Publication 800-37 should be consistent with NIST Special Publication 800-37. This includes use of the FIPS 199, "Standards for Security Categorization of Federal Information and Information Systems," to determine an impact level, as well as associated NIST documents used as guidance for completing risk assessments and security plans. Earlier NIST guidance is applicable to any certification and accreditation work completed or initiated before finalization of NIST Special Publication 800-37. Agencies were not expected to use NIST Special Publication 800-37 as guidance before it became final.

<b>Statement</b>	<b>Evaluation</b>
Assess the overall quality of the Agency's certification and accreditation process.  Comments:	

**Section D**

**NOTE: ALL of Section D should be completed by BOTH the Agency CIO and the OIG.**

**To enter data in allowed fields, use password: fisma**

D.1. First, answer D.1. If the answer is yes, then proceed. If no, then skip to Section E. For D.1.a-f, identify whether agencywide security configuration requirements address each listed application or operating system (Yes, No, or Not Applicable), and then evaluate the degree to which these configurations are implemented on applicable systems. **For example:** If your agency has a total of 200 systems, and 100 of those systems are running Windows 2000, the universe for evaluation of degree would be 100 systems. If 61 of those 100 systems follow configuration requirement policies, and the configuration controls are implemented, the answer would reflect "yes" and "51-70%". If appropriate or necessary, include comments in the Comment area provided below.

D.2. Answer Yes or No, and then evaluate the degree to which the configuration requirements address the patching of security vulnerabilities. If appropriate or necessary, include comments in the Comment area provided below.

**D.1. & D.2.**

	Yes, No, or N/A	Evaluation
D.1. Has the CIO implemented agencywide policies that require detailed specific security configurations and what is the degree by which the configurations are implemented?	Yes	
a. Windows XP Professional	Yes	Almost Always, or 96-100% of the time
b. Windows NT	Yes	Almost Always, or 96-100% of the time
c. Windows 2000 Professional	N/A	
d. Windows 2000	Yes	Almost Always, or 96-100% of the time
e. Windows 2000 Server	Yes	Almost Always, or 96-100% of the time
f. Windows 2003 Server	Yes	Almost Always, or 96-100% of the time
g. Solaris	Yes	Almost Always, or 96-100% of the time
h. HP-UX	No	
i. Linux	Yes	Almost Always, or 96-100% of the time
j. Cisco Router IOS	Yes	Almost Always, or 96-100% of the time
k. Oracle	N/A	
l. Other. Specify: Novell, AIX	Yes	Almost Always, or 96-100% of the time
	Yes or No	Evaluation
D.2. Do the configuration requirements implemented above in D.1.a-f., address patching of security vulnerabilities?	Yes	Almost Always, or 96-100% of the time

**Comments:**



**Section E: Incident Detection and Handling Procedures**

**NOTE: ALL of Section E should be completed by BOTH the Agency CIO and the OIG.**

To enter data in allowed fields, use password: fisma

E.1. Evaluate the degree to which the following statements reflect the status at your agency. If appropriate or necessary, include comments in the Comment area provided below.

**E.1**

Statement	Evaluation
a. The agency follows documented policies and procedures for reporting incidents internally.	Almost Always, or 96-100% of the time
b. The agency follows documented policies and procedures for external reporting to law enforcement authorities.	Almost Always, or 96-100% of the time
c. The agency follows defined procedures for reporting to the United States Computer Emergency Readiness Team (US-CERT). <a href="http://www.us-cert.gov">http://www.us-cert.gov</a>	Almost Always, or 96-100% of the time

**E.2.**

**E.2. Incident Detection Capabilities.**

	Number of Systems	Percentage of Total Systems
a. How many systems underwent vulnerability scans and penetration tests in FY04?	14	82%
b. Specifically, what tools, techniques, technologies, etc., does the agency use to mitigate IT security risk?		
Answer:		
<div style="border: 1px solid black; padding: 5px; width: fit-content;">See Comments Field Below:</div>		

Comments:

E.2.b.  
 The agency uses intrusion detection in several locations to analyze traffic from the internet and critical networks. We run a daily report of all internet activity with thresholds and explain variances. We employ virus protection on Internet email and at the desktop. We have an Agency-wide program for vulnerability notification and patch deployment. We use a multi-level firewall configuration and house all public facing systems in a DMZ isolated from the Internet and our internal networks. We have operating system baselines for most operating systems in use in the Agency and programs to ensure adherence to standards. We proxy network traffic between the Internet and our internal networks and only allow active content from specific trusted sites. We currently have development projects for enterprise vulnerability scanning and enterprise automated patching.

**Section F: Incident Reporting and Analysis**

**NOTE: ALL of Section F should be completed by BOTH the Agency CIO and the OIG.**

**To enter data in allowed fields, use password: fisma**

F.1. For each category of incident listed: identify the total number of successful incidents in FY04, the number of incidents reported to US-CERT, and the number reported to law enforcement. If your agency considers another category of incident type to be high priority, include this information in category VII, "Other". If appropriate or necessary, include comments in the Comment area provided below

F.2. Identify the **number of systems** affected by each category of incident in FY04. If appropriate or necessary, include comments in the Comment area provided below.

	F.1., F.2. & F.3.					
	F.1. Number of Incidents, by category:			F.2. Number of systems affected, by category, on:		
	F.1.a Reported internally	F.1.b. Reported to US CERT	F.1.c. Reported to law enforcement	F.2.a. Systems with complete and up to-date C&A	F.2.b. Systems without complete and up to-date C&A	F.2.c. How many successful incidents occurred for known vulnerabilities for which a patch was available?
	Number of Incidents	Number of Incidents	Number of Incidents	Number of Systems Affected	Number of Systems Affected	Number of Systems Affected
I. Root Compromise	0	0	0	0	0	0
II. User Compromise	0	0	0	0	0	0
III. Denial of Service Attack	0	0	0	0	0	0
IV. Website Defacement	0	0	0	0	0	0
V. Detection of Malicious Logic	33449	33449	0	0	0	0
VI. Successful Virus/worm Introduction	93	93	0	2	1	0
VII. Other	0	0	0	0	0	0
<b>Totals:</b>	33542	33542	0	2	1	0

**Comments:**

The NRC provides US-CERT, on a monthly basis, a calendar year to date, by each month, summary of security events and virus activity at the NRC. See next page for additional activity details.

## Summary of Security Events and Virus Activity: December, 2003 through August, 2004

<u>Type</u>	<u>Pri</u>	<u>Dec. 2003</u>	<u>Jan. 2004</u>	<u>Feb. 2004</u>	<u>Mar. 2004</u>	<u>Apr. 2004</u>	<u>May. 2004</u>	<u>Jun. 2004</u>	<u>Jul. 2004</u>	<u>Aug. 2004</u>	<u>TOTALS</u>
<b>Root Compromise</b>	5	0	0	0	0	0	0	0	0	0	0
<b>User Compromise</b>	4	0	0	0	0	0	0	0	0	0	0
<b>Denial of Service:</b>											
Attempted: Mail Gateway	5	2453	3431	3096	3573	3112	3219	3761	4110		3800
Successful: Mail Gateway	5	0	0	0	0	0	0	0	0		0
Attempted: Web Server	5	131	1754	3114	2134	1508	16	297	466		618
Successful: Web Server	5	0	0	0	0	0	0	0	0		0
Total:	5	2584	5185	6210	5707	4620	3235	4058	4576		4418
<b>Web Site Defacement</b>	5	0	0	0	0	0	0	0	0		0
<b>Reconnaissance Activity</b>		36915	59734	41852	12406	10733	7334	11384	11728		14317
<b>Misuse of Resources</b>											
Attempt to Relay Spam through NRC gateway	1	673	1429	962	743	803	632	867	955		1093
Attempt to exploit the NRC Web Server	3	2699	290	4170	5310	4021	3897	3489	9360		8952
Total		3372	1719	5132	6053	4824	4529	4356	10315		10045
<b>Virus/Malicious Code Activity</b>											
E-mail (Gwava) Detected/Quarantined	3	157	61	1071	6860	0	2753	7827	4117		970
Servers:											
Detected	3	82	0	367	0	5650	2377	0	0		0
Cleaned		0	0	0	0	0	0	0	0		0
Quarantined		82	0	2	0	0	0	0	0		0
Workstations:											
Detected	3	61	15	96	26	0	114	160	212		473
Cleaned		1	0	1	0	0	0	45	32		14
Quarantined		60	7	8	3	0	81	94	177		463
<b>Total Virus/Malicious Code Activity</b>	3	300	76	1534	6886	5650	5244	7987	4329		1443
<b>Other</b>		0	0	0	0	0	0	0	0		0

93

33449

### Priority Levels

Exploit  
 Damage  
 Alert  
 Warning and observation

### NRC

5  
 4  
 3  
 1 & 2

### FedCIRC

1  
 2  
 3  
 4

**Section G: Training**

**NOTE: ALL of Section G should be completed by BOTH the Agency CIO and the OIG.**

**To enter data in allowed fields, use password: fisma**

G.1. Has the agency CIO ensured security training and awareness of all employees, including contractors and those employees with significant IT security responsibilities? If appropriate or necessary, include comments in the Comment area provided below.

G.1.							
G.1.a.	G.1.b.		G.1.c.	G.1.d.		G.1.e.	G.1.f.
Total number of employees in FY04	Employees that received IT security awareness training in FY04, as described in NIST Special Publication 800-50		Total number of employees with significant IT security responsibilities	Employees with significant security responsibilities that received specialized training, as described in NIST Special Publications 800-50 and 800-16		Briefly describe training provided	Total costs for providing IT security training in FY04 (in \$'s)
	Number	Percentage		Number	Percentage		
3468	3023	87.17%	34	32	94.12%	SEE COMMENTS SECTION BELOW	\$46,300
G.2.							
				Yes or No			
a. Does the agency explain policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency wide training?				Yes			

Comments:

During FY 2004, all new staff were provided initial IT security awareness training, all staff were provided refresher IT security awareness training, and those with specific security responsibilities (such as the Information Systems Security Officers formally appointed for each of the applications and systems) were provided role-based awareness training. The on-line awareness course includes the following topics: Threats-Vulnerabilities, Malicious Software, Passwords, Internet Security, Mobile Computing, Personal Use, Software Licenses, Marking (of media), Reporting Incidents, and (User) Responsibilities. The course ends with a ten-question quiz as well as the opportunity for employees to answer three bonus questions before printing out their certificate of completion. The Information Systems Security Officers Awareness Course includes the following topics: Planning and Budgeting, Policy and Regulations, Risk Management, Personnel Security, Security Controls, Continuity of Operations, Certification, and Procurement, as well as a quiz and certificate. Special training sessions with live instructor(s) are offered to provide specialized and remedial understanding of such topics as special handling of sensitive data and media. Other activities include an annual observance of Computer Security Awareness Day and computer security articles in the monthly agency news magazine.