FY2011 CIO FISMA Reporting

FY 2011

Chief Information Officer

Federal Information Security Management Act

Reporting Metrics

Version 1.0

June 1, 2011

Prepared by:

U.S. Department of Homeland Security

National Cyber Security Division

FY 2011 CIO FISMA Reporting

Some questions are informational and may not be specifically mapped to a NIST SP 800-53 requirement or may only be required for a FIPS 199 High impact system. The intent is to gather information on best practices and Agency implementation status beyond minimal requirements. Please answer all questions.

1. SYSTEM INVENTORY

1.1. For each of the FIPS 199 system categorized impact levels in this question, provide the total number of Agency operational, FISMA reportable, systems by Agency component (i.e. Bureau or Sub-Department Operating Element).

1.1a. Agency Operated Systems

1.1a(1) High

1.1a(2) Moderate

1.1a(3) Low

1.1b. Contractor Operated Systems on Behalf of the Agency

1.1b(1) High

1.1b(2) Moderate

1.1b(3) Low

1.1c. Number of systems in 1.1a and 1.1b combined with security authorization to operate

1.1c(1) High

1.1c(2) Moderate

1.1c(3) Low

1.1d. Systems or Services leveraging a public Cloud

1.1d(1) High

1.1d(2) Moderate

1.1d(3) Low

1.1e. Number of Systems or Services in 1.1d with a Security Assessment and Authorization to utilize

1.1e(1) High

1.1e(2) Moderate

1.1e(3) Low

2. ASSET MANAGEMENT

2.1. Provide the total number of Agency Information Technology assets (e.g. router, server, workstation, laptop, blackberry, etc.).

2.1a. Provide the number of Agency information technology assets, connected to the network, (e.g. router, server, workstation, laptop, , etc.) where an automated capability provides visibility at the Agency level into asset inventory information.

2.1b. Provide the number of Agency information technology assets where an automated capability produces Security Content Automation Protocol (SCAP) compliant asset inventory information output.

2.1c. Provide the number of Agency information technology assets where all of the following asset inventory information is collected: Network address, Machine Name, Operating System, and Operating System/Patch Level.

2.2. Has the Agency implemented an automated capability to detect and block unauthorized software from executing on the network? [Please indicate Partial or Full Coverage]

2.3. Has the Agency implemented an automated capability to detect and block unauthorized hardware from connecting to the network? [Please indicate Partial or Full Coverage]

2.4. For your Agency, which type(s) of assets are the most challenging in performing automated asset management? Rank the asset types below from 1-4 with 1 being the most challenging.

2.4a. Servers

2.4b. Workstations/Laptops

2.4c. Network Devices

2.4d. Mobile Devices

3. CONFIGURATION MANAGEMENT

3.1. Provide the number of Agency information technology assets where an automated capability provides visibility at the Agency level into system configuration information (e.g. comparison of Agency baselines to installed configurations).

3.1a. Provide the number of Agency information technology assets where an automated capability produces SCAP compliant system configuration information output.

3.2. Provide the number of types of operating system software in use across the Agency

3.2a. Provide the number of operating system software in use across the Agency for which standard security configuration baselines are defined. Consider an Agency approved deviation as part of the Agency standard security configuration baseline.

3.3. Provide the number of enterprise-wide applications (e.g., Internet Explorer, Adobe, MS Office, Oracle, SQL, etc.) in use at the Agency.

3.3a. Provide the number of enterprise-wide applications for which standard security configuration baselines are defined. Consider an Agency approved deviation as part of the Agency standard security configuration baseline.

4. VULNERABILITY MANAGEMENT

4.1. Provide the number of Agency information technology assets where an automated capability provides visibility at the Agency level into detailed vulnerability information (Common Vulnerabilities and Exposures - CVE).

4.1a. Provide the number of Agency information technology assets where an automated capability produces SCAP compliant vulnerability information output.

5. IDENTITY AND ACCESS MANAGEMENT

5.1. What is the number of Agency network user accounts? (Exclude system and application accounts utilized by processes)

5.1a. How many network user accounts are configured to require PIV to authenticate to the Agency network(s)?

5.1b. How many network user accounts are configured to optionally use PIV to authenticate to the Agency network(s)?

5.2 What is the number of Agency privileged network user accounts (e.g. system administrators)?

5.2a. What is the number of Agency privileged network user accounts that are configured to require PIV credentials to authenticate to the Agency network(s)?

5.2b. What is the number of Agency privileged network user accounts that are configured to optionally use PIV credentials to authenticate to the Agency network(s)?

6. DATA PROTECTION

6.1. Provide the total number of:

6.1a. Mobile computers and devices (excluding laptops)

6.1a(1) Netbooks

6.1a(2) Tablet-type computers

6.1a(3) Blackberries

6.1a(4) Smartphones

6.1a(5) USB devices (Flash drives and external hard drives)

6.1a(6) Other

6.1b Laptops only

6.2. Provide the number of devices in 6.1 that have all user data encrypted with FIPS 140-2 validated encryption.

6.2a. Mobile computers and devices (excluding laptops)

6.2a(1) Netbooks

6.2a(2) Tablet-type computers

6.2a(3) Blackberries

6.2a(4) Smartphones

6.2a(5) USB devices(Flash drives and external hard drives)

6.2a(6) Other

6.2b Laptops only

6.3. Provide the percentage of Agency email systems that implement encryption technologies to protect the integrity of the contents and sender information when sending messages to government agencies or the public such as S/MIME, PGP, or other.

7. BOUNDARY PROTECTION

7.1. Provide the percentage of the required TIC 1.0 Capabilities that are implemented. (Applies only to Federal Civilian Agency TIC Access Providers (TICAP) only. All others should respond N/A.)

7.1a. Provide the percentage of TIC 2.0 Capabilities that are implemented. (Applies only to Federal Civilian Agency TIC Access Providers (TICAP) only. All others should respond N/A.)

7.2. Provide the percentage of TICs with operational NCPS (Einstein 2) deployment. (Applies only to Federal Civilian Agency TIC Access Providers (TICAP) only. All others should respond N/A.)

7.3. Provide the percentage of external network capacity passing through a TIC/MTIPS. (Applies to all Federal Civilian Agencies. DOD should respond N/A.)

7.4. Provide the percentage of external connections passing through a TIC/MTIPS. (Applies to all Federal Civilian Agencies. DOD should respond N/A.)

7.5. Provide the percentage of Agency email systems that implement sender verification (anti-spoofing) technologies when sending messages to government agencies or the public such as DKIM, SPF, or other.

7.6. Provide the percentage of Agency email systems that check sender verification (anti-spoofing technologies) to detect possibly forged messages from government agencies known to send email with sender verification such as DKIM or SPF or other.

7.7. Provide the frequency with which the Agency conducts thorough scans for unauthorized wireless access points.

7.8. Provide the frequency in which the Agency maps their cyber perimeter (e.g. externally visible systems and devices).

8. INCIDENT MANAGEMENT

8.1. What is the number of Agency operational networks on which controlled network penetration testing was performed in the past year?

For the testing conducted above, provide the following information:

8.1a. Percentage of incidents detected by NOC/SOC. (Per NIST 800-61, an incident is defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.)

For the incidents above detected by the NOC/SOC during penetration testing provide the following information:

8.1a(1). Mean-time to incident detection. (The mean time-to-incident detection metric is calculated by subtracting the Date of Occurrence from the Date of Discovery. These metrics are then averaged across the number of incidents detected by the NOC/SOC during penetration testing)

8.1a(2). Mean-time to incident remediation. (The mean time-to-incident remediation is calculated by dividing the difference between the Date of Occurrence and the Date of Remediation for each incident remediated in the metric time period, by the total number of incidents remediated in the metric time period)

8.1a(3). Mean-time to incident recovery. (The mean time-to-incident recovery is calculated by dividing the difference between the Date of Occurrence and the Date of Recovery for each incident recovered in the metric time period, by the total number of incidents recovered in the metric time period)

8.1b. Percentage of penetration testing incidents detected from other sources or business processes.

8.2. For FY11, what percentage of applicable US-CERT SARs (Security Awareness Report) (or Information Assurance Vulnerability Alerts for DOD) has been acted upon appropriately by the Agency?

8.3. Provide the number of times in the past year the Agency participated in the Joint Agency Cyber Knowledge Exchange (JACKE). (These meetings are monthly)

9. TRAINING AND EDUCATION

9.1. What is the average frequency with which users receive supplemental cybersecurity awareness training content beyond the annual training requirement (content could include a single question or tip of the day)? (This question will be answered by subcomponent) (daily, weekly, monthly, quarterly, annually, never)

9.2. Provide the total number of Agency-sponsored phishing attack exercises, if conducted.

9.2a. Provide the number of Agency-sponsored phishing attack exercises that revealed results of potential compromise (e.g., users clicked on an embedded link).

9.3. Provide the number of Agency users with network access privileges.

9.3a. Provide the number of Agency users with network access privileges that have been given security awareness training annually.

9.4. Provide the number of Agency network users with significant security responsibilities.

9.4a. Provide the number of Agency network users with significant security responsibilities that have been given specialized, role based, security training annually.

9.5. At what frequency is security awareness training content (that is provided to users) updated by the Agency or training provider? (daily, weekly, monthly, quarterly, annually, never)

9.5a. Comments:

9.6. At what frequency is specialized, role based, security training content (that is provided to users) updated by the Agency or training provider? (daily, weekly, monthly, quarterly, annually, never)

9.6a. Comments:

9.7. Provide the estimated percentage of new users to satisfactorily complete security awareness training before being granted network access.

9.8. Does your Agency's annual security awareness training include:

9.8a. Information on the security risks of wireless technologies and mobile devices.

9.8b. Awareness of the organization's security policies/procedures for mobile devices.

9.8c. Mitigation of risks by maintaining physical control of mobile devices, encrypting sensitive information, disabling wireless functionality when not in use, and procedures for reporting lost or stolen mobile devices?

9.8d. Content on how to recognize and avoid phishing attacks.

10. REMOTE ACCESS

10.1. Provide the number of remote access connection methods (e.g. Dial-up, VPN, Clientless-VPN or SSL, etc.) the Agency offers to allow users to connect remotely to full access of normal desktop Agency LAN/WAN resources/services. Connection methods refer to options the Agency offers to users allowing them to connect remotely.

10.1a. For those methods provided above, provide the number that:

10.1a(1). Require only UserID/password.

10.1a(2). Require only PIV credentials.

10.1a(3). Optionally accepts PIV credentials.

10.1a(4). Require other forms of two-factor authentication.

10.1a(5). Utilize FIPS 140-2 validated cryptographic modules.

10.1a(6). Prohibit split tunneling and/or dual-connected laptops where the laptop has both an active wired and wireless connection.

10.1a(7). Are configured, in accordance with OMB M-07-17, to time-out after 30 minutes of inactivity which requiring re-authentication.

10.1a(8). Scan for malware upon connection.

10.1a(9). Require Government Furnished Equipment (GFE).

10.1b. For those connection methods that require GFE as in question 10.1a(9) above, provide the number of connection methods that:

10.1b(1). Assess and correct system configuration upon connection.

10.2 List the remote access connection methods identified in 10.1

11. NETWORK SECURITY PROTOCOLS

11.1. Provide the number of:

11.1a. External facing DNS names (second-level, e.g. www.dhs.gov).

11.1b. External facing DNS names (second-level) signed.

11.1c. Provide the percentage of external facing DNS hierarchies with all sub-domains (second-level and below) entirely signed.

12. SOFTWARE ASSURANCE

12.1 Provide the number of information systems, developed in-house or with commercial services, deployed in the past 12 months.

12.1a. Provide the number of information systems above (12.1) that were tested using automated source code testing tools. (Source code testing tools are defined as tools that review source code line by line to detect security vulnerabilities and provide guidance on how to correct problems identified.)

12.1b. Provide the number of the information systems above (12.1a) where the tools generated output compliant with:

12.1b(1). Common Vulnerabilities and Exposures (CVE)

12.1b(2). Common Weakness Enumeration (CWE)

12.1b(3). Common Vulnerability Scoring System (CVSS)

12.1b(4). Open Vulnerability and Assessment Language (OVAL)

13. CONTINUOUS MONITORING

13.1. What percentage of data from the following potential data feeds are being monitored at appropriate frequencies and levels in the Agency:

13.1a. IDS/IPS

13.1b. AV/Anti-Malware/Anti-Spyware

13.1c. System Logs

13.1d. Application logs

13.1e. Patch Status

13.1f. Vulnerability Scans

13.1g. DNS logging

13.1h. Configuration/Change Management system alerts

13.1i. Failed Logins for privileged accounts

13.1j. Physical security logs for access to restricted areas (e.g. data centers)

13.1k. Data Loss Prevention data

13.1l. Remote Access logs

13.1m. Network device logs

13.1n. Account monitoring

13.1n(1). Locked out

13.1n(2). Disabled

13.1n(3). Terminated personnel

13.1n(4). Transferred personnel

13.1n(5). Dormant accounts

13.1n(6). Passwords that have reached the maximum password age

13.1n(7). Passwords that never expire

13.1o. Outbound traffic to include large transfers of data, either unencrypted or encrypted.

13.1p. Port scans

13.1q. Network access control lists and firewall rule sets.

13.2 To what extent is the data collected, correlated, and being used to drive action to reduce risks? Please provide a number on a scale of 1-5, with 1 being that “All continuous monitoring data is correlated”.