# Proposed FY 2010 FISMA Performance Metrics

Please send comments to:

OMB-Metrics@nist.gov

By January 4, 2010

# System Inventory

- Please provide the number of agency-owned and contractor systems by component with the following information
  - FIPS 199 risk category
  - Certification and accreditation status
  - Whether annual testing occurred
  - Whether a tested contingency plan exists
  - The number of systems assessed at E-Authentication levels 3 or 4

# Hardware Inventory

- Can the agency provide a real-time data feed of its asset inventory of all devices connected to its network?

# Hardware Inventory

**Sub questions:**

- How frequently updated is the D/A's asset inventory of all devices connected to the network and the network devices themselves, recording at least the network address, device name(s), purpose of each system, and an asset owner responsible for each device?
- Is this capability manual, partially automated or fully automated for all D/A devices?
- Does the D/A have the technical ability to block introduction of unauthorized hardware to any device connected to the network? Is there a process to respond if detected?
- Does the D/A regularly test this capability by attaching devices not already in the inventory to the network?
- Does the D/A technically scan and discover/inventory all devices connected to the enterprise network?
- If the D/A does not currently maintain such an inventory, what are its plans to do so and by when?

# Software Inventory

- Can the agency provide a real-time data feed of its asset inventory of all software installed on all devices connected to its networks?

# Software Inventory

**Sub-questions:**

- How frequently updated is the D/A's asset inventory of all software installed on devices connected to the network, recording at least the operating system, version number, patch level, and the applications installed on it?
- Is this capability manual, partially automated or fully automated for all D/A devices?
- Does the D/A technically scan and discover/inventory all software on devices connected to the enterprise network?
- If the D/A does not currently maintain such an inventory, what are its plans to do so and by when?
- Does the D/A have the technical ability to block introduction of unauthorized software to any device connected to the network? Is there a process to respond if detected?
- Does the D/A regularly test this capability by attempting to install unapproved software on D/A devices?

# Connections Inventory

- Can the agency provide a real-time data feed of all of its external connections as defined in the TIC architecture?

# Connections Inventory

**Sub-questions:**

- How frequently updated is the D/A's inventory of all external connections as defined in the TIC architecture?
- Is this capability manual, partially automated or fully automated for all D/A connections?
- Does the D/A technically block connections of unauthorized devices to the network?
- Does the D/A employ technical means to scan and map all IPs on each enclave?
- If the D/A does not currently maintain a connections inventory, what are its plans to do so and by when?

# Configuration Management

**For various hardware and software, agencies will be asked the following questions:**

- Standard baseline configuration defined
- Checklist Used
- Number of instances that can be and the number that are technically scanned for compliance with standard baseline
- Frequency of scanning of all instances (Average number of days)
- Number of instances with settings found to be compliant with standard baseline
- Average time to apply high security criticality patch to 95% of machines
- What technology is used for scanning?

# Integration of Security into SDLC

- What number of new systems (by 199 level) went live during the reporting period?
- What number of new systems used 800-53 controls as system design requirements?
- What number of new systems used 800-53A in the process of system acceptance testing?
- What number of contract systems have the FISMA requirements in the contract or equivalent language?

# Remote Access Management

- Can the agency provide a real-time data feed of all of its external connections?

# Remote Access Management

**Sub-questions:**

- For GFE, do you automatically mitigate deviations from the minimum D/A configurations before allowing connection to proceed?
- For personally-owned equipment (if permitted for use), do you require the user's system to meet minimum D/A configurations before allowing the connection to proceed?
    - If you are unable to prohibit connections when minimum D/A configuration standards are not met, when do you plan to have that functionality in place?
    - If you are unable to actively validate that remotely connected devices meet D/A configuration standards upon connection, when do you plan to have that functionality in place?
- What percentage of remote access connections to the D/A network do you monitor?
- Does your D/A monitor for: (a) intrusions, (b) malware, (c) data loss, (d) data flows (e.g., source/destination IP), (e) authorized user information (e.g., user ID), (f) resource(s) accessed, (g) other

# Remote Access Management, cont.

- Does the D/A's remote access policy require two-factor authentication for remote access (including VPN, dial-up, and other forms)?
    - If the agency does not have a remote access policy, what are the plans to develop and implement one and by when, respectively?
- What number of users have remote access to the D/A networks?
    - What number of those use two-factor authentication for remote access?
    - What number of those use HSPD-12 cards?
- What percentage of connections prohibit split tunneling (as defined by NIST)?
- Is D/A information permitted to be stored on the local device?
- What percentage of remote access solutions (e.g., the cryptographic portions, if any) use FIPS 140-2 validated cryptographic modules?
- Does your D/A use a "time-out" function for remote access and mobile devices requiring user re-authentication after 30 minutes of inactivity?

# Incident Management

- **During the D/A's controlled network penetration testing, what percentage of incidents were detected by NOC/SOC?**
    - For detected incidents, what is the mean-time to incident recovery?
    - What tools, techniques, technologies, does the Agency use for incident detection?
    - How many systems (or networks of systems) are protected using the tools, techniques, and technologies listed above?
    - If the agency has not performed controlled network penetration testing, when will it have the capability to do so?

# Incident Management cont.

- Does your D/A have an Incident Response Capability (whether in-house or as part of managed security services contract)?
    - If not, does the D/A have a Security Operations Center operating as the incident response center?
- Does your D/A participate in US-CERT threat briefings? (E.g., JACKE)
    - If not, why and what are the D/A's plans to participate?
- Does your D/A have access to GFIRST information?
    - If not, why and what are the D/A's plans to obtain access?
- Does your D/A have access to US-CERT publications? (E.g., SARS)
    - If not, why and what are the D/A's plans to obtain access?

# Training

Can the agency provide a real-time data feed with the information in the chart below?

| # of employees and contractors with log-in privileges | # of employees and contractors given annual security awareness training | # of employees and contractors with significant security responsibilities | # of employees with significant security responsibilities provided specialized security training | Cost of providing security awareness training | Cost of providing specialized security training |
|---|---|---|---|---|---|
| | | | | | |

Does the D/A security awareness training:

- Address phishing?
- Cover the subject of remote access?
- Cover the subject of Web 2.0 technologies?
- Cover the subject of Peer-to-Peer technologies?

# Training, cont.

- Is the training automated or in person? Or both?
- How many employees/contractors have security related certifications?
- How many employees/contractors with significant security responsibilities have security-related certifications?
- Please identify the types of security-related certifications for each.
- List the titles of Agency official(s) that determine the employees with SISR.
- Provide the criteria to determine who has SISR. (E.g., privileged access, data focused, decision-making/managerial focused, OPM job descriptions, etc.)
- Provide the number of employees and contractors with system privileges.
  - Provide the number of these that were given appropriate security and privacy awareness training during the reporting year.

# Identity & Access Management

- **What is the percentage of employees and contractors with valid HSPD-12 credentials?**
  - Please upload a progress update for your HSPD-12 logical access plan.
- How many systems in your reported system inventory use two-factor authentication?
  - How many of these systems are enabled to use Personal Identity Verification (PIV) credentials for user authentication?
- Of the systems assessed at E-authentication levels 3 or 4, what percentage of those require two-factor or multi-factor authentication for non-Federal users (e.g. citizens, business partners)?
- What is the D/A number of privileged users (e.g. system administrators)?
- What percentage of privileged users are required to use two-factor authentication for all privileged authentications?

# Data Leakage Prevention

- **What products/technologies does the D/A use for Data Leakage Prevention (DLP) or equivalent on its network to technically prevent the sending of unencrypted sensitive information outside the perimeter?**
    - If the D/A does not have any products/technologies in use, when will these be in place?
- What products/technologies does the D/A use for DLP or equivalent on its network to technically prevent the sending of unencrypted sensitive information to mobile media and USB devices?
    - If the D/A does not have any products/technologies in use, when will these be in place?

# Data Leakage Prevention

- Does the D/A have the following in place:
  - data sensitivity based labeling scheme
  - a technical based labeling scheme
  - security controls invoked based on sensitivity based labeling
  - the capability to disable compromised mobile devices (i.e. lost or stolen devices)
- What is the percentage of portable computers (laptops) which have all user data encrypted with FIPS validated encryption?
- What is the percentage of Personal Digital Assistants which have all user data encrypted with FIPS validated encryption?

# Real-Time Security Status & Management

- **Does the D/A have an automated capability (e.g. via a SIM or SIEM tool) to provide real to near real time enterprise-wise cybersecurity situational awareness?**
  - Does it integrate the following:
  - Note: If your answer is no to any of the following, please provide the date by which your agency will have this capability in place.
    - Intrusion Detection/Prevention Sensor Data
    - Anti-Virus/Anti-Malware/Anti-Spyware
    - System Log Data
    - Application Log Data
    - Patch Status
    - Vulnerability Scans
    - Security Configuration Management Scans of:
      - » Operating Systems
      - » Databases
      - » Servers
      - » Network Devices (firewalls, routers, switches)

# Real-Time Security Status & Management

- If your agency does not have the automated capability to provide real to near real-time enterprise-wide cybersecurity situational awareness, please provide the date by which your agency will have this capability in place.