EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

October 3, 2014

M-15-01

MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shaun Donovan
Director

SUBJECT: Fiscal Year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices

Purpose

This memorandum identifies current Administration information security priorities, provides agencies with Fiscal Year (FY) 2014-2015 Federal Information Security Management Act (FISMA) and Privacy Management reporting guidance and deadlines, as required by the *Federal Information Security Management Act of 2002* (P.L. 107-347), and establishes new policy guidelines to improve Federal information security posture. This memorandum, as it applies to FY 2015, updates and expands the scope of Office of Management and Budget (OMB) Memoranda M-06-19, *"Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments"* and M-07-16, *"Safeguarding Against and Responding to the Breach of Personally Identifiable Information."* As discussed in Section III of this memorandum, OMB is making these updates to streamline agency reporting of information security incidents to the Department of Homeland Security's (DHS) U.S. Computer Emergency Readiness Team (US-CERT), and to improve DHS US-CERT's ability to respond to information security incidents effectively. OMB will pilot these updates for one year (FY 2015) as it considers the most effective way to permanently update M-06-19 and M-07-16.

This memorandum also introduces new requirements based on assessments of emerging threat activities, to include the introduction of: enhanced FISMA metrics; a proactive vulnerability scanning process; and updated incident response procedures. The remainder of this memorandum describes the background for these requirements, along with associated guidelines.

This memorandum is only applicable to Federal civilian agency networks, and does not impact classified or national security systems and/or networks.

Background

FISMA was enacted to protect Federal resources by providing a comprehensive framework for supporting the effectiveness of information security controls. OMB, National Security Council (NSC) staff, the DHS, and each Federal agency all play a role in ensuring the security of Federal information, information systems, and networks. In accordance with FISMA requirements, OMB, in coordination with NSC staff and DHS, oversees Federal agencies' information technology (IT) programs through the collection and review of annual FISMA metrics (to include the cybersecurity Cross Agency Priority (CAP) goal[1]); the CyberStat process[2]; the annual FISMA report to Congress; and the budget process. Federal agencies are responsible for managing the security of their information and information systems through a variety of risk-based security controls and initiatives, and Senior Agency Officials are responsible for ensuring that information security management processes are integrated with agency strategic and operational planning processes.

Key Initiatives and Policy Updates

While the processes noted above have led to improvements in the governmentwide IT security posture, as reflected in the FY 2013 FISMA Report[3], cyber threats have continued to evolve. This memorandum emphasizes and provides guidance on the following new initiatives which OMB and DHS, in coordination with NSC staff and in collaboration with the National Institute of Standards and Technology (NIST) and other Federal agencies, have developed within the previous year to address these evolving threats and improve government wide information security:

- **OMB Memorandum M-14-03 and the Continuous Diagnostics and Mitigation (CDM) Program**

  Instead of requiring agencies to provide point-in-time assessments of information systems, OMB Memorandum M-14-03, *"Enhancing the Security of Federal Information and Information Systems"* requires agencies to assess information security risks on an ongoing basis. Additionally, the CDM program, led by DHS, provides a central blanket purchase agreement (BPA) for use by Federal agencies and state, local, and tribal governments to procure a standard set of cybersecurity tools and services to improve the monitoring and defense of their networks. Ultimately, these tools will provide near real-time risk information to aid Federal agency officials in rapidly detecting and then responding to information security events.

  M-14-03 also required agencies to develop an Information Security Continuous Monitoring (ISCM) strategy which supports the implementation of a program to continuously monitor and defend their network(s) from cyber security risks, threats and malicious activity by February 28, 2014. **Agencies are required to submit the ISCM strategy to OMB via CyberScope by November 14, 2014.**

- **FY 2015 FISMA Metrics**

[1] Established by the Government Performance and Results Modernization Act of 2010, these Cross-Agency Priority Goals are a tool used by leadership to accelerate progress on a limited number of Presidential priority areas where implementation requires active collaboration between multiple agencies. Additional information is available at: www.performance.gov/cap-goals-list?view=public.

[2] CyberStat reviews are face-to-face, evidence-based meetings to ensure agencies are accountable for their cybersecurity posture, while at the same time assisting them in developing focused strategies for improving their information security posture.

[3] The FY 2013 FISMA Report is available at: www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fy_2013_fisma_report_05.01.2014.pdf.

OMB and NSC staff use annual FISMA metrics to assess the implementation of agency information security capabilities and to measure overall program effectiveness in reducing risks. To better assess Federal agency information security programs, OMB and DHS, in coordination with NSC staff, worked across the Federal Government and applied feedback from agencies to enhance FISMA reporting by including outcome-oriented measures to better assess the true status of Federal agencies' information security posture.

OMB, NSC staff, and DHS have taken the following approach in developing the enhanced FY 2015 FISMA metrics: 1) assessed the quality and validity of each metric by soliciting input from over 100 cybersecurity professionals from more than 24 Federal agencies who made over 200 recommendations to the metrics; 2) where possible, removed metrics that had completed their lifecycle or did not add sufficient value to the expanded assessment process; 3) developed outcome-oriented metrics to complement existing compliance-oriented metrics, to include anti-phishing and malware defense metrics aimed at reducing the risk of malware introduced through email and malicious or compromised websites; and 4) where possible, used existing Federal agency data feeds to automate responses to improve the quality and timeliness of reported data. **Federal agencies must assess their information security capabilities against these enhanced FISMA metrics at the beginning of FY 2015.**

- **FY 2015 Cybersecurity CAP Goal**
  The *Government Performance and Results Modernization Act of 2010* (P.L. 111-352) established CAP goals as tools used by agency leadership to accelerate progress on a limited number of Presidential priority areas. NSC staff and OMB identified cybersecurity as one of 14 *CAP goals* for FY 2014 to build on the statutory requirements of FISMA, and to provide senior government officials with greater visibility and accountability for this issue. Cybersecurity CAP goal initiatives and metrics are a subset of the FISMA metrics. As referenced in the *President's FY 2015 Budget* and published on *www.Performance.gov,* OMB and NSC staff led an interagency working group to develop cybersecurity CAP goal priorities for FY 2015 to FY 2017.

  As with the previous cybersecurity CAP goal, OMB and NSC staff will maintain focus on ISCM and Identity, Credential, and Access Management (ICAM). Additionally, for the first time, OMB and NSC staff have identified "Anti-Phishing and Malware Defense" as an additional priority area. Data reported to the DHS US-CERT by Federal agencies shows a preponderance of phishing attacks, and shows the number of phishing attacks is steadily increasing. By elevating this new priority, OMB and NSC staff will combat the number one threat vector affecting Federal systems and information.

- **Formalized Process for Proactive Scans of Public Facing Agency Networks**
  Given the rapid agility of those seeking to compromise Federal systems and data, the Federal Government needs a consistent, central, and repeatable method for identifying cybersecurity threats and vulnerabilities. Consistent with OMB Memorandum M-10-28, *"Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security,"* this memorandum identifies DHS

as the agency responsible for performing regular and proactive scans of public facing segments of Federal civilian agency networks. This memorandum also identifies the responsibilities of Federal agencies, to include providing DHS with an authorization for scanning internet accessible addresses and systems. Section II of this memorandum provides a more extensive explanation of the responsibilities and expectations of both DHS and Federal agencies.

- **Updated DHS US-CERT Incident Notification Guidelines**
  Pursuant to FISMA, 44 U.S.C. § 3544(b)(7), agencies are required to report information security incidents to US-CERT. In conjunction with the release of this OMB memorandum, DHS US-CERT will release its updated incident notification guidelines. These guidelines establish the following: 1) a standard set of data elements for reporting incidents; 2) updated incident notification requirements; 3) impact classifications; and 4) threat vectors used to categorize and address incidents.

Summary of Federal Agency FY 2014-2015 Requirements

As noted above, this memorandum establishes new policy guidelines to improve the Federal information security posture, and provides guidance to agencies on complying with FY 2014-2015 FISMA and Privacy Management reporting requirements. This includes a detailed listing of what agencies are required to provide by the November 14, 2014 deadline. The contents of this memorandum are organized as follows:

Section I: Information Security Program Oversight Requirements

Requires that agencies participate in regular CyberStat sessions and Chief Information Officer (CIO) interviews. These sessions are a key oversight tool used by OMB and NSC staff, in coordination with DHS, to assess the status of Federal agency information security programs, develop plans for addressing any identified shortcomings, and identify any agency-specific challenges in fulfilling cyber mandates.

Section II: Formalized Process for Proactive Scans of Public Facing Agency Networks

Provides detailed requirements for DHS and Federal agencies to implement the process for regular and proactive scans of public facing segments of Federal civilian agency networks.

Section III: FY 2014-2015 FISMA Reporting and Privacy Management Guidance

- Provides Federal agencies with deadlines and requirements for monthly, quarterly, and annual reporting requirements.
- Establishes detailed instructions for preparing the annual Federal agency FISMA report, to include privacy documents, which must be submitted to DHS through CyberScope **no later than Friday, November 14, 2014.**
- Identifies changes, applicable for one year (FY 2015), to OMB Memoranda M-06-19, *"Reporting Incidents Involving Personally Identifiable Information Incorporating the Cost for Security in Agency Information Technology Investments"* and M-07-16, *"Safeguarding Against and Responding to the Breach of Personally Identifiable Information."*
- Updates DHS US-CERT Incident Notification Guidelines for reporting information security incidents to DHS US-CERT.

Section IV: Updates to Frequently Asked Questions

This section provides updates on Frequently Asked Questions regarding these instructions.

I ask for your help in overseeing your agency's implementation of the guidance established in the memorandum.

Questions for OMB may be directed to fisma@omb.eop.gov. Questions regarding FISMA metrics and CyberScope reporting may be directed to the DHS Federal Network Resilience Division, Cybersecurity Performance Management Branch at FNR.FISMA@hq.dhs.gov.

Section I: Information Security Program Oversight Requirements

In addition to the reporting requirements outlined below in Section III, Federal agencies must carry out the following activities to comply with FY 2014 FISMA requirements:

Participate in CyberStat accountability sessions and agency interviews. Equipped with the reporting results from CyberScope and agency Plans of Action, OMB, in coordination with NSC staff and DHS, will continue to conduct CyberStat reviews of selected agencies. CyberStat reviews are face-to-face, evidence-based meetings to ensure agencies are accountable for their cybersecurity posture, while at the same time assisting them in developing focused strategies for improving information security posture.

As in prior years, DHS will provide agencies with the status of their current cybersecurity posture based on CyberScope data. DHS will continue the annual interviews with agencies' CIO and Chief Information Security Officers (CISO) to discuss their agency's security posture. Each interview session has four distinct goals:

- Assessing progress towards the Administration's cybersecurity priorities and other governance, information security risk management, and FISMA compliance issues and challenges.
- Identifying security best practices and raising awareness of FISMA reporting requirements.
- Identifying any agency-specific challenges with meeting cyber mandates and/or operational security requirements.
- Establishing meaningful dialogue with the agency's senior leadership.

Agencies should complete and maintain a Plan of Action for improving specific cybersecurity capabilities. Agencies will provide FY targets and demonstrate progress toward those targets as they mature their programs.

The information collected in these interviews will also inform OMB's annual FISMA Report to Congress.

Section II: Formalized Process for Proactive Scans of Public Facing Agency Networks

Recent cybersecurity events have demonstrated that the Federal Government needs a mechanism for conducting regular and proactive scans of public facing segments of Federal civilian agency networks. This mechanism should supplement existing agency information security operations, to include network scans, and is intended to provide a consistent scanning methodology that can quickly identify threats and vulnerabilities that may have governmentwide implications.

In accordance with the authorities established in OMB Memorandum *M-10-28, "Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security (DHS),"* OMB directs DHS to take the following actions in the interest of improving Federal information security. These responsibilities are subject to OMB oversight and applicable FISMA requirements and limitations. **In furtherance of those responsibilities and consistent with applicable law, regulation, policy, and existing Memoranda of Agreement with agencies, DHS shall:**

- Scan internet accessible addresses and public facing segments of Federal civilian agency systems for vulnerabilities on an ongoing basis as well as in response to newly discovered vulnerabilities on an urgent basis, to include without prior agency authorization on an emergency basis where not prohibited by law;
- Maintain a mechanism for the reporting of Federal department and agency website and system vulnerabilities. Contracted third parties and cloud service providers, in accordance with agency and provider incident response plans (IRP) and FedRAMP requirements, should report vulnerabilities to the relevant agencies who should in turn report to DHS;
- Continue to deploy consolidated intrusion detection and prevention capabilities to protect Federal department and agency information and information systems;
- Develop and periodically update guidance for the reporting of cybersecurity incidents involving Federal department and agency information systems to DHS US-CERT, which serves as the Federal Information Security Incident Center as established in 44 U.S.C. § 3546;
- Report to OMB on the identification and mitigation of risks and vulnerabilities across Federal agency information systems;
- Provide Federal agencies with the agency-specific results of DHS scanning and reports on the identification risks and vulnerabilities across the department or agency's internet accessible addresses, systems and external access points; and,
- Offer additional risk and vulnerability assessment services upon the request of individual Federal agencies.

Federal agencies, consistent with applicable law, regulation, policy, and existing Memoranda of Agreement with DHS, shall provide the following by Friday, November 14, 2014, unless otherwise stated, to coincide with agency FISMA reporting requirements referenced below in Section III:

- Provide DHS with an authorization for scanning of internet accessible addresses and systems. Ensure that such an authorization is reviewed on a semiannual basis and remains on file with DHS;
- Provide DHS, on a semiannual basis, with a complete list of all internet accessible addresses and systems, including static IP addresses for external websites, servers and other access points and domain name service names for dynamically provisioned systems[4], and provide DHS with at least five business days advanced notice of changes to IP ranges by emailing federal@us-cert.gov;[5]
- Enter into a legally sufficient Memorandum of Agreement with DHS relating to the deployment of EINSTEIN (an intrusion detection and prevention capability operated by DHS);
- Provide DHS with names of vendors who manage, host, or provide security for internet accessible systems, including external websites and servers, and ensure that those vendors have provided any necessary authorizations for DHS scanning of agency systems, by emailing federal@us-cert.gov;
- Provide DHS with a technical point of contact to facilitate DHS scanning and protective activities within the scope of this memorandum, and update that contact information as necessary by emailing federal@us-cert.gov;
- Work collaboratively with OMB and DHS to mitigate risks and vulnerabilities in internet accessible addresses and systems identified by OMB or DHS; and,
- Promptly report cybersecurity incidents involving department or agency information systems to DHS US-CERT in accordance with current Incident Notification Guidelines.
- Agencies may consider providing the results of the DHS scans to their Office of Inspector General, as appropriate.

[4] The term "dynamically provisioned system" refers to systems which are virtually hosted and operated from multiple sites, such that network traffic to the systems is distributed across multiple, discrete IP ranges or autonomous system numbers (ASNs).

[5] This requirement only applies to Federal civilian agencies.

Section III: FY 2014-2015 FISMA Reporting and Privacy Management Guidance

Consistent with previous OMB FISMA guidance, agencies are required to adhere to DHS direction to report data through CyberScope. Additionally, as part of each Federal agency's annual report to OMB and Congress, OMB requires that the head of each agency submit a signed electronic copy of an official letter to CyberScope providing a comprehensive overview reflecting his or her assessment of the adequacy and effectiveness of information security policies, procedures, and practices, and compliance with the requirements of FISMA for the agency.

Reporting Requirements and Deadlines

OMB, NSC staff, and DHS worked collaboratively with agencies to develop metrics to assess the implementation of agency information security capabilities and to measure their overall program effectiveness in reducing risks. Agency success in achieving these measures is conveyed to Congress in OMB's annual FISMA report.

As in previous years, Federal agencies shall adhere to the following reporting requirements and deadlines:

FY 2014 Annual FISMA Reporting Deadline

Annual FISMA Report*:	**CyberScope will be open for agencies to submit their annual report beginning Monday, October 6, 2014.** **The due date for all CFO Act agencies to submit their annual FY 2014 FISMA data through CyberScope is Friday, November 14, 2014.** All agencies, except for micro agencies (agencies with fewer than 100 full time equivalents), should complete the CIO, Inspector General, and Senior Agency Official for Privacy questions in CyberScope no later than this date.

ISCM CyberScope Reporting Deadline

ISCM CyberScope Reporting*:	Agencies are required to submit their ISCM strategy, developed in accordance with M-14-03, to CyberScope by 5pm EST on November 14, 2014.

***Use of personal identity verification (PIV) card to access CyberScope.** Agencies should note that a PIV card, compliant with Homeland Security Presidential Directive 12, is required for access to CyberScope. FISMA submissions will not be accepted outside of CyberScope.

FY 2015 Monthly and Quarterly Information Security Metrics CyberScope Reporting Deadlines

Monthly CyberScope Data Feeds*:	Agencies are required to submit information security data to CyberScope by 5pm EST on the 5th day of each month. Small and micro agencies are not required to submit monthly reports, although they are highly encouraged to do so. Agency Inspectors General, and Senior Agency Officials for Privacy are not required to submit monthly reports.
Quarterly CyberScope Reporting*:	CFO Act agencies are required to submit metrics data to CyberScope for the first, second and third quarters of each fiscal year. Quarterly reporting dates are as follows: • Quarter 1: Between January 1-15, 2015 • Quarter 2: Between April 1-15, 2015 • Quarter 3: Between July 1-15, 2015. Fourth quarter data should be included in their annual FISMA report, and therefore agencies are not required to submit separate metrics data during the fourth quarter. Agency Inspectors General and Senior Agency Officials for Privacy are not required to submit quarterly reports, but must submit an annual report. As in previous years, agencies are encouraged to set an internal cut-off date for data collection to permit adequate time for review and resolution of disputes prior to submission of the agency's annual FISMA report.

***Use of personal identity verification (PIV) card to access CyberScope.** Agencies should note that a PIV card, compliant with Homeland Security Presidential Directive 12, is required for access to CyberScope. FISMA submissions will not be accepted outside of CyberScope.

FY 2014 Agency Reports to OMB and Congress

In accordance with Section 301 § 3544 of FISMA, agencies are required to submit an annual report to OMB, the Committees on Oversight and Government Reform and Science, Space, and Technology of the House of Representatives, the Committees on Homeland Security and Government Affairs and Commerce, Science, and Transportation of the Senate, the appropriate authorization and appropriations committees of Congress, and the Comptroller General. **The due date for all CFO Act agencies to submit their annual FY 2014 FISMA data through CyberScope is Friday, November 14, 2014.**

These reports must address all of the requirements of Section 301 § 3544. Each report must have an executive summary, and that summary should include the following information:

- **Agency head assessment -** An official letter, signed by the head of the agency, providing a comprehensive overview reflecting his or her assessment of the adequacy and effectiveness of their agency's information security policies, procedures, and practices. Specifically, this assessment must include the following information:

- **Progress towards meeting FY 2014 FISMA Metrics -** Agency-specific metrics data reported through CyberScope showing agency progress towards meeting the FY 2014 FISMA metrics established by OMB, DHS, NSC staff, and the CIO Council.[6]

- **Progress towards meeting the Cybersecurity CAP goal.** Agencies shall review their performance with regards to the Administration's cybersecurity priorities with their Performance Improvement Officer. Agencies shall include in their annual report information pertaining to the agency's performance in this area. These priorities will receive additional emphasis as the Administration reports on agency progress in FY 2014 towards meeting the Cybersecurity CAP goal.

- **Information on incidents reported to DHS US-CERT** – Agencies shall include information regarding computer security incidents reported to the DHS US-CERT through the DHS US-CERT Incident Notification System.

Agencies shall upload this letter to CyberScope as part of their annual reporting requirements.

FY 2014-2015 Privacy Management Requirements

As in previous years, the Senior Agency Officials for Privacy are required to report on an annual basis and must submit the following documents through CyberScope as part of the annual data submission:

- Description of the agency's privacy training for employees and contractors;
- Breach notification policy;
- Progress update on eliminating unnecessary use of Social Security Numbers; and,
- Progress update on the review and reduction of holdings of personally identifiable information (PII).

Agencies are required to submit these four documents whether or not the documents have changed from versions submitted in previous years.

FY 2015 FISMA Metrics

Agencies must assess their information security capabilities against the FY 2015 FISMA metrics established by OMB, NSC staff, and DHS. The FY 2015 FISMA metrics are classified according to the following three categories:

Cross Agency Priorities (CAP)	The CAP metrics highlight three areas: ISCM, Strong Authentication (HSPD-12), and Anti-Phishing and Malware

[6] FY 2014 FISMA metrics are available at: www.dhs.gov/publication/fy14-fisma-documents.

	Defense.
Key FISMA Metrics (KFM)	KFMs are additional priority metrics outside of the CAP metrics. These metrics score the following performance areas: system inventory; hardware and software asset management; secure configuration management; vulnerability and weakness management; identity credential and access management; anti-phishing and malware defense; data protection; network defense; boundary protection; training and education; and incident response management.
Baseline (BASE)	BASE metrics are derived from NIST guidelines. They are not scored, but are used to establish current baselines against which future performance may be measured. BASE metrics include areas such as: system inventory; asset and access management; boundary protection; and user training and education.

Additional details regarding the FY 2015 FISMA metrics are available at: www.dhs.gov/federal-information-security-management-act-fisma.

Updated DHS US-CERT Incident Notification Guidelines

OMB Memoranda M-06-19, *"Reporting Incidents Involving Personally Identifiable Information Incorporating the Cost for Security in Agency Information Technology Investments"* and M-07-16, *"Safeguarding Against and Responding to the Breach of Personally Identifiable Information"* established requirements for agencies to report incidents involving PII to DHS US-CERT. M-06-19 required that agencies report all incidents involving PII to DHS US-CERT within one hour of discovering the incident. M-07-16 further clarified this requirement by stating that incidents involving the breach of PII must be reported to US-CERT whether in electronic or paper format.

The release of this memorandum coincides with the release of updated DHS US-CERT Incident Notification Guidelines, which DHS US-CERT developed in coordination with OMB and NSC staff. Specifically, this memorandum updates and expands the scope of M-06-19 and M-07-16 and requires Federal agencies to notify DHS US-CERT of all cyber related (electronic) incidents with confirmed loss of confidentiality, integrity or availability **within one hour of reaching the agency's top-level Computer Security Incident Response Team (CSIRT), Security Operations Center (SOC), or IT department**. All non-cyber related (paper) incidents should be reported to the agency's privacy office within one hour of a confirmed breach. As previously noted, these changes will be in effect for FY 2015 while OMB determines the most effective way to permanently update M-06-19 and M-07-16. Agencies should review the updated DHS US-CERT Incident Notification Guidelines for additional details on incident reporting requirements.

The DHS US-CERT guidelines are only applicable to Federal civilian agency networks, and do not impact classified or national security systems and/or networks. **The modified DHS US-CERT guidelines will be effective beginning October 1, 2014, however, all Federal agencies are permitted to continue reporting incidents using the legacy incident reporting category system until September 30, 2015**.

To ensure the guidelines remain up to date in addressing dynamic cybersecurity challenges while consistently providing timely and actionable incident information, DHS US-CERT will establish a schedule for reviewing and updating the incident notification guidelines at regular intervals in coordination with OMB and the Federal CIO Council.

Section IV: Updates to Frequently Asked Questions on Reporting for the Federal Information Security Management Act and Agency Privacy Management

The Frequently Asked Questions (FAQs) listed below are only those questions that are either new or updated from guidance issued in OMB Memorandum M-14-04, *"Fiscal Year 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management."* The information conveyed in the FAQs and definitions from the FY 2013 FISMA guidance is still applicable to Federal agencies. Those FAQs and definitions are listed on the OMB MAX site located here: *https://max.omb.gov/community/x/eodcKw*.

What's New?

1. Is there anything new in this year's guidance?

Yes. OMB has added two sections to this year's guidance that address critical cybersecurity areas. Section II provides detailed requirements for DHS and other Federal agencies to formalize the process for regular and proactive scans of agency networks. The Federal Government's response to the "Heartbleed" security vulnerability highlighted the need to formalize this process, and ensure that Federal agencies are proactively scanning networks for vulnerabilities. This year's guidance clarifies what is required of DHS and Federal agencies in this area.

Additionally, Section III clarifies changes to agency requirements for reporting security incidents to DHS US-CERT. These changes will clarify what constitutes a security incident, when and what information Federal agencies should report to DHS US-CERT, and provide greater consistency in information reported by Federal agencies. Consistent reporting using common metrics will better enable OMB to identify the frequency of various security incidents across the Federal Government, assess vulnerabilities within agencies, and assess the capability of agencies to address those vulnerabilities.

Mobile Devices

2. Are there specific security requirements for mobile devices (e.g. smartphones and tablets)?

All existing Federal requirements for data protection and remote access are applicable to mobile devices. For example, the security requirements in OMB Circular A-130, NIST FIPS 140-2, "*Security Requirements for Cryptographic Modules*," NIST FIPS 199, "*Standards for Security Categorization of Federal Information and Information Systems*," NIST FIPS 200, "*Minimum Security Requirements for Federal Information and Information Systems*," and NIST FIPS 201-2, "*Personal Identification Verification of Federal Employees and Contractors*," apply to mobile devices (including appropriate security controls specified in NIST SP 800-53). Agencies are also required to follow NIST SP 800-124, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*, and NIST SP 800-037, *Guide for Applying the Risk Management Framework for Federal Information Systems*. Agencies should specify security requirements during the acquisition process and ensure that procurements capture the requirements of the Federal Acquisition Regulation (e.g. 52.225-5, Trade Agreements), OMB policy (e.g. M-07-16), and NIST standards and guidelines.

In May 2013, the Federal CIO Council issued the Federal Mobile Security Baseline, Mobile Computing Decision Framework, and Mobile Security Reference Architecture in order to further assist Federal agencies with securing mobile devices and help integrate effective security and privacy measures into the design and adoption of mobile technologies.

The initial version of the Federal Mobile Security Baseline provides a baseline set of controls for Mobile Device Management and Mobile Application Management, and notional controls for Identity and Access Management and Data. The Federal CIO Council is developing more comprehensive control sets for Identity and Access Management and Data which is expected to be included in the Federal Mobile Security Baseline at a later time. This baseline focuses on the most common Federal mobility use case: Federal employees operating agency-controlled mobile devices to access moderate impact systems on a Federal network.

Additionally, the Mobile Computing Decision Framework is designed to assist agencies in making decisions regarding mobile devices, applications, and infrastructure. The Mobile Security Reference Architecture presents the architectural components necessary to provide secure mobile services, while providing the data confidentiality, integrity, and availability critical to agency mission success.

CIOs and agency procurement officials should work together to ensure that all new purchases of mobile devices and infrastructure support the technical controls in these documents.

Security Incident Reporting

3. Why are the number and classification of reported incidents by DHS US-CERT different than those reported in my agency's submission?

There may be some differences between the DHS US-CERT Reported Incident totals for agencies in the Federal FISMA Report and the data provided by agencies in their own FISMA reports. According to DHS US-CERT, small variations in the number of reported incidents is not abnormal. Additionally, DHS US-CERT often re-categorizes incidents based upon its methodology after incidents are processed internally. This is a result of different viewpoints among the respective information security professionals as to how a particular incident should be categorized. Each agency has unique challenges that influence their reported numbers to varying degrees. DHS US-CERT continues to work with agencies to address disparities on a case-by-case basis and ensure greater consistency in classification.

Protection of Agency Information

4. How will DHS protect agencies' vulnerability information?

DHS is taking multiple steps to ensure the information is protected once it is collected from agencies. The equipment utilized by DHS meets security standards as identified in the DHS IT Services and Hardware Catalog, and analysts follow DHS and industry best practices for securing the data appropriately. During the course of the scan, data from an agency's public facing internet accessible systems is collected pertaining to security vulnerabilities and risks on systems and information. The type of data collected and stored during the external scanning is publicly accessible system related information (such as open ports, services and versions running on the open ports, security issues and potential vulnerabilities), as well as configuration and patch levels. The data is derived from publicly accessible information via the Internet. The data generated from the scans is encrypted in an automated report template before being transferred to the agency that owns the network. Additionally, DHS generally defers to the agency in question in response to any external requests for information (e.g. Congressional requests, FOIA, etc.) before releasing any agency vulnerability information.

Ongoing Authorizations

5. What is expected of agencies and authorizing officials with regard to the full transition to ongoing authorization?
The transition from the static, three-year reauthorization approach to ongoing authorization should be carried out in accordance with the level of maturity and effectiveness of agency ISCM programs, organizational risk tolerance, and subject to the final decision of agency Authorizing officials.[7] Agencies are expected to define specific criteria (e.g. risk tolerance, agreed upon documentation frequencies) depending on the maturity level of their ISCM programs to assist authorizing officials in determining when information systems and common controls are ready to transition to the full ongoing authorization approach for managing information security risk.

6. Are there specific conditions that must be satisfied before an information system is considered for transition to ongoing authorization?
Yes. Before a transition to ongoing authorization is considered, two conditions must be satisfied: (1) an organizational ISCM program is in place that has the capability to monitor *all* implemented security controls with the appropriate degree of rigor and at the appropriate frequencies specified by the organization in accordance with their ISCM strategy and NIST guidance; and (2) the information system has been granted an initial authorization to operate based on a complete (zero-base) review of the system and has entered the operations/maintenance phase of the system development life cycle.

7. Do all agency information systems and common controls have to transition to ongoing authorization at the same time?
No. Agencies may consider employing a phased implementation approach to ongoing authorization, for example: (1) by transitioning information systems to ongoing authorization according to security categorizations or system impact levels; or (2) by partitioning their information systems into well-defined subsystems or system components and subsequently transitioning those subsystems and/or system components to ongoing authorization one segment at a time until the entire system is ready for the full transition.

8. Are authorizing officials required to formally acknowledge the transition of an information system and common controls to ongoing authorization for systems and controls that are currently following the static, three-year reauthorization process?
Yes. Authorizing Officials must formally acknowledge that an information system and/or common controls are now being managed by an ongoing authorization process informed by an ISCM program and accept the responsibility for performing all necessary activities associated with that process.

[7] Authorizing officials are senior management officials responsible for ensuring the organization's ISCM program is applied with respect to a given information system and ensuring the security posture of the information systems is maintained. Additional responsibilities are described in NIST Special Publication 800-137, "Information Security Continuous Monitoring for Federal Information Systems and Organizations," and NIST "Supplemental Guidance on Ongoing Authorization: Transitioning to Near Real-Time Risk Management."