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

THE DIRECTOR

November 18, 2013

M-14-04

MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Sylvia M. Burwell
Director

SUBJECT: Fiscal Year 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management

The attached memorandum provides instructions for meeting your agency's Fiscal Year (FY) 2013 reporting requirements under the Federal Information Security Management Act of 2002 (FISMA) (Title III, Pub. L. No. 107-347). It also includes reporting instructions on your agency's privacy management program.

The Office of Management and Budget (OMB) identified cybersecurity as one of 14 Cross Agency Priority (CAP) Goals for FY 2013 and FY 2014, which were established in accordance with the Government Performance and Results Modernization Act to build on the statutory requirements provided for in FISMA. The CAP goals are available at http://goals.performance.gov/. The cybersecurity CAP goals, which build upon work from prior years, are helping agencies improve cybersecurity performance by focusing efforts on what data and information are entering and exiting their networks, who is on their systems, and what components are on their information networks as well as when their security status changes. To accomplish these goals the Administration is prioritizing: (1) measuring agency implementation of Trusted Internet Connections; (2) focusing on strong authentication through the use of multi-factor authentication in accordance with Homeland Security Presidential Directive-12; and (3) performing monitoring of security controls in federal information systems and environments in which those systems operate on a continuous basis. The FY 2013 FISMA metrics issued by the Department of Homeland Security established minimum and target levels of performance for these priorities, as well as metrics for other key performance areas.

As discussed in OMB Memorandum 10-28, *"Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security (DHS),"* DHS is exercising primary responsibility within the Executive Branch for the operational aspects of Federal agency cybersecurity with respect to the Federal information systems that fall within FISMA under 44 U.S.C. §3543. As stated in previous FISMA guidance issued by OMB, agencies are required to adhere to Department of Homeland Security (DHS) direction to report data through CyberScope. Additionally, OMB requires that the head of each agency submit, as part of the agency's annual report, 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.

I ask for your help in overseeing your agency's implementation of the reporting guidance outlined in the attachments.

Questions for OMB may be directed to Carol Bales at 202-395-9915 or fisma@omb.eop.gov. Questions regarding FISMA metrics and Cyberscope reporting may be directed to the Cybersecurity Performance Management Office, Federal Network Security Branch, DHS, at FISMA.FNS@dhs.gov or (703) 235-5045.

Attachments

Attachment: Fiscal Year (FY) 2013 FISMA Reporting Guidance

The FY 2013 FISMA metrics are classified into three categories as follows:

Administration Priorities (AP)	The AP metrics highlight three areas: Trusted Internet Connection (TIC) capabilities and utilization, mandatory authentication with Personal Identity Verification (PIV), and Continuous Monitoring.
Key FISMA Metrics (KFM)	Key metrics are the additional metrics outside of the Administration priorities that are measured (scored).
Baseline (BASE)	Baseline FISMA metrics are not scored, but used to establish current baselines against which future performance may be measured.

The FY 2013 FISMA metrics are located on the Department of Homeland Security (DHS) website at: http://www.dhs.gov/federal-network-resilience

Required Action

To comply, agencies will carry out the following activities:

• **Submit monthly data feeds.** The Chief Information Officers (CIO) of CIO Council member agencies will submit monthly data feeds through CyberScope. Agencies must load data from their automated security management tools into CyberScope on a monthly basis for a limited number of data elements. For more information, refer to the Frequently Asked Questions related to data feeds.[1]

• **Respond to security posture questions on a quarterly/annual basis.** In addition to providing the data feeds described above, agency CIOs, Inspectors General, and Senior Agency Officials for Privacy are also required to answer a set of information security questions in CyberScope. These questions address areas of risk and are designed to assess the implementation of security capabilities and measure their effectiveness. The CIOs of CIO Council member agencies report on a quarterly basis, and Inspectors General and Senior Agency Officials for Privacy report on an annual basis.

DHS will continue to provide agencies with the status of their current cybersecurity posture, based on CyberScope data, and ask agencies to complete a Plan of Action for improving specific cybersecurity capabilities. Agencies will provide quarterly and FY targets and demonstrate progress toward those targets as they mature their programs.

• **Participate in CyberStat accountability sessions and agency interviews.** Equipped with the reporting results from CyberScope and agency Plans of Action, DHS, along with the Office of Management and Budget (OMB) and the White House National Security Staff, 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.

DHS will continue the annual interviews with agencies' CIO and Chief Information Security Officers (CISO) based on their agency's security posture. Each interview session has three distinct goals:
- Assessing progress towards the administration cybersecurity priorities and other FISMA compliance and challenges.
- Identifying security best practices and raising awareness of FISMA reporting requirements.
- Establishing meaningful dialogue with the agency's senior leadership.

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

[1] Frequently asked questions related to data feeds can be found on the CyberScope information page within the OMB MAX Portal. The URL for the page is https://max.omb.gov/community/display/Egov/Data+Feeds.

• **Submit Privacy documents.** As part of the annual report, Senior Agency Officials for Privacy are to submit the following documents through CyberScope:

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

OMB is requiring agencies to submit these four documents whether or not the documents have changed from versions submitted in previous years.

Reporting deadlines

Monthly Data Feeds:	Agencies are required to submit information security data to CyberScope by close of business on the 5th of each month. Small and micro agencies are not required to submit monthly reports, although they are highly encouraged to do so.
Quarterly Reporting:	CIO Council agencies are expected to submit metrics data for first, second and third quarters. For first quarter, agencies must submit their updates to CyberScope between January 1-15. For second quarter, agencies must submit their updates to CyberScope between April 1-15. For third quarter, agencies must submit their updates to CyberScope between July 1-15. Agencies are not expected to submit metrics data for the fourth quarter, other than what is required for the annual report.
Annual Report:	The due date for all agencies to submit their annual FY 2013 FISMA report through CyberScope is December 2, 2013.

Additional Requirements

• Agencies shall review their performance of the administration's FISMA cybersecurity priorities with their Performance Improvement Officer, as these priorities will receive additional emphasis in FY 2014 as the Administration reports agency progress towards the cybersecurity Cross Agency Priority (CAP) goals. The cybersecurity CAP goals consist of the following activities: Continuous Monitoring; Trusted Internet Connections (TIC) capabilities and traffic consolidation; and strong authentication using HSPD-12 Personal Identity Verification (PIV) cards for logical access.

• Agencies should note that a PIV card, compliant with Homeland Security Presidential Directive (HSPD) 12, is required for access to CyberScope. FISMA submissions will not be accepted outside of CyberScope. For information related to CyberScope, please visit: https://max.omb.gov/community/display/Egov/CyberScope+Documentation

• As part of the annual report, agencies are also asked to submit an electronic copy of an official letter to CyberScope, signed by the head of the agency, 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.

Points of Contact

Please direct questions regarding FISMA to the Cybersecurity Performance Management Office, Federal Network Security Branch, DHS, at FISMA.FNS@dhs.gov or (703) 235-5045.

For OMB policy related questions, please contact Carol Bales, (202) 395-9915 or fisma@omb.eop.gov.

Attachment: Fiscal Year (FY) 2013 Frequently Asked Questions on Reporting for the Federal Information Security Management Act and Agency Privacy Management

Sending Reports to Congress and GAO

1. When should my agency send its annual report to Congress and the Government Accountability Office (GAO)?
After review by and notification from OMB, agencies shall forward their transmittal letter with a report generated by CyberScope to the appropriate Congressional Committees. Transmittal of agency reports to Congress shall be made by, or be consistent with guidance from, the agency's Congressional or Legislative Affairs office to the following: Committees on Oversight and Government Reform and Science and Technology of the House, the Committees on Government Affairs and Commerce, Science, and Transportation of the Senate, and the Congressional authorization and appropriations committees for each individual agency. In prior years, the Committees have provided to OMB specific points of contact for receiving the reports. As in the past, if such are provided to OMB, we will notify the agencies. In addition, agencies must forward a copy of their printed reports to the GAO.

Submission Instructions and Templates

2. Which set of questions should my agency fill out in CyberScope?
All agencies, except for micro agencies, should complete the Chief Information Officer (CIO), Inspector General (IG) and Senior Agency Official for Privacy (SAOP) questions in CyberScope for submission no later than December 2, 2013.

Micro agencies (i.e. agencies employing 100 or fewer full time equivalents (FTEs)) should answer the abbreviated questions for their annual report. Micro agencies will be automatically presented with the correct questions within CyberScope.

Please note that only submissions through CyberScope will be accepted.

3. When should program officials, CIOs, IGs, and SAOPs share the results of their reviews?
While the goal of FISMA is stronger agency- and government-wide security, information regarding an agency's information security program should be shared as it becomes available. This helps promote timely correction and resolution of issues in the agency's information systems.

As in previous years, the Agency Head should submit a signed letter that provides a comprehensive overview of the adequacy and effectiveness of information security policies, procedures, and practices, and compliance with the requirements of FISMA for the agency. CyberScope will require that agencies upload a portable document format (PDF) of this letter with the Agency Head's signature prior to accepting the agency's FY 2013 report submission.

4. Should agencies set an internal FISMA reporting cut-off date?
Yes. Agencies should set an internal cut-off date for data collection and report preparation. A cut-off date should permit adequate time for meaningful internal review and comment and resolution of any disputes before finalizing the agency's report. With respect to an IG's review of the CIO's or SAOP's work product, such review does not in itself fulfill FISMA's requirement

for IGs to independently evaluate an agency's program including testing the effectiveness of a representative subset of the agency's information systems.

5. Why are there questions in CyberScope that do not correspond to a security control in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*?
Not all FISMA questions relate to security controls in NIST SP 800-53. OMB and the Department of Homeland Security (DHS) are continuously improving the FISMA metrics and reporting process, including the addition of baseline security metrics to assess the current status and maturity level of Cybersecurity in the agencies, not just specific control implementations. The FISMA metrics continue to evolve as Cybersecurity matures.

6. Is the use of CyberScope mandatory?
Yes. Submissions will only be accepted through CyberScope. Full instructions for the use of the tool as well as additional information, and detailed CyberScope Frequently Asked Questions (FAQs), are available on the Max portal at: https://max.omb.gov/community/x/EgQrFQ.

Security Reporting

7. Must agencies report at both an agency wide level and by individual component?
Yes. Agencies must provide an overall agency view of their security and privacy program but most of the topic areas also require specific responses for each of the major components (e.g., bureaus or operating divisions).

Please note that CyberScope will require reporting by component in several areas as well as at the agency level.

8. Should all of my agency's information systems be included as part of our FISMA report?
Yes. Section 3544(a)(1)(A) of FISMA states: "*The head of each agency shall be responsible for providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of (i) information collected or maintained by or on behalf of the agency; and (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.*"

Your agency's annual FISMA report, therefore, summarizes the performance of your agency's program to secure all of your agency's information and information systems, in any form or format, whether automated or manual. NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, provides guidance on establishing information system boundaries which can help you identify your systems.

9. Must the Department of Defense (DoD) and the Office of the Director of National Intelligence (ODNI) follow OMB policy and NIST standards/guidelines?
Yes, for non-national security systems, DOD and ODNI are to incorporate OMB policies and NIST guidelines into their internal policies.

For national security systems, the Joint Task Force Transformation Initiative (JTFTI) Interagency Working Group with representatives from the Civil, Defense and Intelligence Communities (IC) started an on-going effort in FY2009 to produce a unified information security framework for the Federal Government. Under this effort, the DoD and ODNI jointly developed with NIST the following publications:

- NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013.

- NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach,* February 2010.

- NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans*, June 2010.[1]

- NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View,* March 2011.

- NIST SP 800-30, *Guide for Conducting Risk Assessments*, September 2012.

Because these guidelines are jointly developed, DOD, ODNI, and CNSS policies for national security systems should incorporate these guidelines. Additional guidance for national security systems is provided in Committee on National Security Systems (CNSS) Instruction 1253.

10. What reporting is required for national security systems?
FISMA requires annual reviews and reporting of all systems, including national security systems. Agencies can choose to provide responses to the questions in the template either in aggregate or separate from their non-national security systems.

Agencies shall describe how they are implementing the requirements of FISMA for national security systems. When management and internal control oversight of an agency's national security programs and systems are handled differently than non-national security programs, a description of and explanation for the differences is required. DoD and the ODNI shall report on compliance with their policies and guidance. Note that SP 800-30, SP 800-37, SP 800-53, and SP 800-53A, 800-39 were developed jointly by NIST, DoD and the IC through the Joint Task Force Transformation Initiative Interagency Working Group.

The CIO for the ODNI reports on systems processing, storing, or transmitting sensitive compartmentalized information (SCI) across the Intelligence Community and those other systems for which the DNI is the principal accrediting authority. Agencies shall follow the Intelligence Community reporting guidance for these systems. SCI systems shall only be reported via the Intelligence Community report. However, this separate reporting does not alter an agency head's responsibility for overseeing the security of all operations and assets of the agency or component. Therefore, copies of separate reporting must also be provided to the agency head for their use.

[1] NIST SP 800-53A is in the process of being updated for consistency with SP 800-53 Revision 4.

To assist oversight by appropriate national security authorities, it is important to specify where practicable which portion of the agency report pertains to national security systems.

NIST Standards and Guidelines

11. Is use of NIST Federal Information Processing Standards (FIPS) required?
Yes. FIPS are issued by NIST after approval by the Secretary of Commerce pursuant to Section 5131 of the Information Technology Reform Act of 1996 (Public Law 104-106) and FISMA. With the passage of FISMA, there is no longer a statutory provision to allow for agencies to waive Federal Information Processing Standards (FIPS).

12. Is use of NIST guidelines required?
Yes. For non-national security programs and information systems, agencies must follow NIST guidelines unless otherwise stated by OMB.

13. How soon after release of final NIST publications (standards and guidelines) must agencies be compliant?
For legacy information systems, agencies are expected to be in compliance with NIST standards and guidelines within one year of the publication date unless otherwise directed by OMB. The one year compliance date for revisions to NIST publications applies only to the new and/or updated material in the publications. For information systems under development or for legacy systems undergoing significant changes, agencies are expected to be in compliance with the NIST publications immediately upon deployment of the information system.

14. Are NIST guidelines flexible?
Yes. While agencies are required to follow NIST guidelines in accordance with OMB policy, there is flexibility within NIST's guidelines in how agencies apply them. Unless specified by additional implementing policy by OMB, NIST guidelines generally allow agencies latitude in their application. Consequently, the application of NIST guidelines by agencies can result in different security solutions that are equally acceptable and consistent with the guidelines.

15. Are agencies required to select and implement all security controls in NIST SP 800-53?
No. Agencies are required to use a risk-based approach in developing security plans for federal information systems and for common controls that are inherited by those systems. A risk-based approach requires agencies to perform a security categorization of their information and information systems in accordance with FIPS Publication 199 and use the results of that categorization to select one of the three security control baselines described in NIST SP 800-53. Agencies are subsequently expected to: (i) use the baselines as a starting point in the security control selection process; (ii) apply the tailoring guidance in SP 800-53, eliminating or adding controls as necessary (based on an assessment of risk); and (iii) produce a security plan with appropriate justification and rationale that, when implemented, will meet the requirements of FIPS Publication 200 and provide adequate protection for organizational operations and assets, individuals, other organizations, and the Nation. Although agencies are not required to select and implement all security controls in SP 800-53, they are required to monitor all selected and implemented controls in their security plans on an ongoing basis in accordance with NIST SP

800-39, SP 800-37, SP 800-137, and their information security continuous monitoring (ISCM)[2] strategies to effectively manage information security risk over time. Additionally, every security control from the initial security control baselines must be accounted for in security plans. If particular security controls are tailored out of those baselines, then the associated rationale is recorded in security plans (or references/pointers to other relevant documentation provided). For national security systems, guidance for security categorization, security control baselines, and tailoring is provided in CNSS Instruction 1253.

General

16. Are the security requirements outlined in the Federal Information Security Management Act of 2002 (44 U.S.C. 3544) limited to information in electronic form?
No. Section 3541 of FISMA provides the Act's security requirements apply to "*information and information systems*" without distinguishing by form or format; therefore, the security requirements outlined in FISMA apply to Federal information in all forms and formats (including electronic, paper, audio, etc.).

17. Does OMB give equal weight to the assessments by the agency and the IG? What if the two parties disagree?
OMB gives equal weight to both assessments. In asking different questions of each party, OMB and DHS seek complementary and not conflicting reporting. While government-wide reporting guidelines require a single report from each agency, the report should represent the consolidated views of the agency and not separate views of various reviewers.

18. FISMA, OMB policy, and NIST standards and guidelines require agency security programs to be risk-based. Who is responsible for deciding the acceptable level of risk (e.g., the CIO, program officials and system owners, or the IG)? Are the IGs' independent evaluations also to be risk-based? What if they disagree?
The agency head ultimately is responsible for deciding the acceptable level of risk for their agency. System owners, program officials, and CIOs provide input for this decision. Such decisions must reflect policies from OMB and standards and guidelines from NIST (particularly FIPS Publication199, *Standards for Security Categorization of Federal Information and Information Systems*, and FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, as well as NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*). An information system's Authorizing Official[3] takes responsibility for accepting any residual risk, thus they are held accountable for managing the security for that system.

IG evaluations are intended to independently assess if the agency is applying a risk-based approach to their information security programs and the information systems that support the conduct of agency missions and business functions. For example, when reviewing the assessment in support of an individual security authorization, the IG would generally assess whether: 1) the assessment was performed in the manner prescribed in NIST guidelines and

[2] Refers to the ongoing monitoring of security controls in Federal information systems and environments of operation.

[3] As defined in NIST Special Publication 800-39 located at: http://csrc.nist.gov/publications/PubsSPs.html.

agency policy; 2) controls are being implemented as stated in any planning documentation; and 3) ISCM is adequate given the system impact level of the system and information.

19. Could you provide examples of high impact systems?
Determining the impact level of organizational information systems is unique to each agency and dependent on its mission requirements. At the same time, some examples are relatively obvious and common to all agencies. As a rebuttable presumption, all cyber critical infrastructure and key resources identified in an agency's Homeland Security Policy Directive 7 (HSPD-7), *Critical Infrastructure Identification, Prioritization, and Protection*, plans are high impact, as are all systems identified as necessary to support agency continuity of operations.

As discussed in OMB Memorandum 05-16, *Regulation on Maintaining Telecommunications Service During Crisis or Emergency in Federally-owned Buildings*, issued June 2005, systems necessary for continuity of operations purposes include, for example, telecommunications systems identified in agency reviews implementing Section 414 the Transportation, Treasury, Independent Agencies, and General Government Appropriations Act, 2005 (Division H of Public Law 108-447.)

Additionally, information systems used by agencies to provide services to other agencies such as under E-Government initiatives and lines of business, could also be high impact, but are at least moderate impact. The decision as to information system impact level in this circumstance must be agreed to by the provider and all of its customers. Please see NIST FIPS Publication 199 and NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, for further guidance.

20. If my IG says the agency's inventory of information systems is less than 100% complete, how do I reconcile the differing lists?
Agencies should be provided the list of systems the IG has identified as not being part of the agency's inventory.

21. When OMB asks if an agency has a process, are you also asking if the process is implemented and is effective?
Yes. OMB wants to know whether processes are implemented and working effectively to safeguard information and information systems. An ineffective process cannot be relied upon to achieve its information security and privacy objectives. To gauge the effectiveness of a particular Information Technology (IT) security program process, we rely on responses to questions asked of the agency IG.

22. We often find security weaknesses requiring additional and significant resources to correct, yet such discoveries seldom coincide with the budget process. Can we delay correction until the next budget cycle?
No. However, agencies should integrate security requirements as they develop new and operate existing systems and as security weaknesses are identified.

OMB's policies regarding information security funding were articulated in OMB Memorandum M-00-07, *Incorporating and Funding Security in Information Systems Investments*, dated

February 2000. They remain in effect, were repeated in OMB Memorandum M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, dated July 2006. Any additional resources should be included in the materials submitted for OMB's budget guidance, when there is enough time. Resources that need to be included outside of the budget process will need to follow the reprogramming request process. In brief, agencies must do two specific things. First, they must integrate security into and fund it over the lifecycle of each system as it is developed. This requirement was codified in section 3544(b)(2)(C) of FISMA. Second, the operations of legacy (steady-state) systems must meet security requirements (as stated in OMB policy, NIST standards, etc.) before funds are spent on new systems (development, modernization or enhancement).

As an example of this policy in practice, if an agency has a legacy system without a current security authorization, or for which a contingency plan has not been tested, these actions must be completed before spending funds on a new system. A simple way to accomplish this is to redirect the costs of security risk management activities (e.g., weakness (risk) mitigation, security assessment and authorization, or contingency plan testing) from the funds intended for development, modernization or enhancement.

OMB recognizes that other unanticipated security needs may arise from time-to-time. In such cases, agencies should prioritize available resources to correct the most significant weaknesses.

23. You are no longer asking agencies to report significant deficiencies in the annual FISMA report. Don't we have to report them?

Not in your annual FISMA report. However, agencies must maintain all documentation supporting a finding of a significant deficiency and make it available in a timely manner upon request by OMB or other oversight authorities.

FISMA requires agencies to report a significant deficiency as: 1) a material weakness under the Federal Managers Financial Integrity Act (FMFIA) and 2) an instance of a lack of substantial compliance under FFMIA, if related to financial management systems. (See OMB Circular A-123, *Management's Responsibility for Internal Control*, for further information on reporting significant deficiencies.) All security weaknesses that are to be remediated must be included in and tracked on your plan of action and milestones (POA&M.).

A significant deficiency is defined as a weakness in an agency's overall information systems security program or management control structure, or within one or more information systems that significantly restricts the capability of the agency to carry out its mission or compromises the security of its information, information systems, personnel, or other resources, operations, or assets. In this context, the risk is great enough that the agency head and other agencies must be notified and immediate or near-immediate corrective action must be taken.

24. What about weaknesses for which an agency accepts the risk?

Identified weaknesses that are to be accepted (residual) risks are tracked in the Security Assessment Report and are documented with the rationale for acceptance in the System Security Plan. Agencies factor accepted risks into ISCM strategies to ensure that the risk remains acceptable over the course of time.

25. Should I apply FISMA and privacy requirements to my agency's regulatory and information collection activities?

Yes. Federal regulatory and information collection activities depend upon quality information protected from unauthorized access, use, disclosure, disruption, modification, or destruction.

Federal regulatory and information collection activities often require Federal agencies, and entities (e.g., contractors, private companies, non-profit organizations) which operate on behalf of Federal agencies, to collect, create, process, or maintain Federal government information. When developing regulations, agencies must ensure information security and privacy law and policy are applied where appropriate. Your agency's information collection activities (subject to the Paperwork Reduction Act and OMB's rule providing implementing guidance found at 5 CFR 1320, *Controlling Paperwork Burdens on the Public*), including those activities conducted or sponsored by other entities on behalf of your agency, must also ensure procedures for adequately securing and safeguarding Federal information are consistent with existing law and policy.

If your agency promulgates regulations requiring entities which operate on behalf of your agency to collect, create, process, or maintain Federal information, then procedures established by the regulation for adequately securing and safeguarding this information must be consistent with existing law and policy (e.g. FISMA, the Privacy Act, the E-Government Act, OMB information security and privacy policy, and NIST standards and guidelines), regardless of whether the information is being held at the agency or with the entity collecting, processing, or maintaining the information on behalf of the agency.

26. Are agencies allowed to utilize data services provided by the private sector, including "software as a service," “platform as a service,” “infrastructure as a service" and software subscription type solutions?

Yes. Agencies are permitted to use these types of agreements and arrangements, provided appropriate security controls are implemented, tested, and monitored as part of the agency’s information security program. We encourage agencies to seek out and leverage private sector, market-driven solutions resulting in cost savings and performance improvements – provided agency information is protected to the degree required by FISMA, FISMA implementation standards (i.e. FIPS), and associated policy and guidelines. As with other contractor services and relationships, agencies should include these software solutions and subscriptions as they complete their annual security assessments.

As of December 8, 2011, all agencies were required to follow Federal Risk and Authorization Management Program (FedRAMP)[4] requirements for cloud computing.

[4] See https://cio.gov/wp-content/uploads/2012/09/fedrampmemo.pdf and http://www.fedramp.gov.

27. How do agencies ensure FISMA compliance for connections to non-agency systems? Do Statement of Auditing Standards No. 70 (SAS 70) audits meet the requirements of FISMA and implementing policies and guidance?
NIST Special Publication 800-47, Security Guide for Interconnecting Information Technology Systems, provides a management approach for interconnecting IT systems, with an emphasis on security. The document recommends development of an Interconnection Security Agreement (ISA) and a Memorandum of Understanding (MOU). The ISA specifies the technical and security requirements of the interconnection, and the MOU defines the responsibilities of the participating organizations. The security guide recommends regular communications between the organizations throughout the life cycle of the interconnection. One or both organizations shall review the security controls for the interconnection at least annually or whenever a significant change occurs to ensure the controls are operating properly and are providing appropriate levels of protection.

Security reviews may be conducted by designated audit authorities of one or both organizations, or by an independent third party. Both organizations shall agree on the rigor and frequency of reviews as well as a reporting process.

SAS 70 audits compliance does not necessarily ensure FISMA compliance. The private sector relies on SAS 70, to ensure compliance with Section 404 of the Sarbanes-Oxley Act of 2002, requiring management assessment of internal controls. While SAS 70 reports may be sufficient to determine contractor compliance with OMB Circular A-123 and financial statement audit requirements, it is not a pre-determined set of control objectives or control activities, and therefore is not in itself sufficient to meet FISMA requirements. In addition, the extent to which specific systems supporting the Government activity or contract are actually reviewed as part of a particular audit is not always clear. In determining whether SAS 70 reports provide sufficient evidence of contractor system FISMA compliance, it is the agency's responsibility to ensure that:

- The scope of the SAS 70 audit was sufficient and fully addressed the specific contractor system requiring FISMA review.
- The audit encompassed all controls and requirements of law, OMB policy and NIST standards and guidelines.

To reduce burden on agencies and service providers and increase efficiency, agencies and IGs should share with their counterparts at other agencies any assessment described above.

28. Are there security requirements specific 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*, and NIST FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, apply (including appropriate security controls specified in NIST SP 800-53) to mobile devices. Agencies are also required to follow 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.

To further assist agencies with securing mobile devices, in May 2013, the Federal Chief Information Officer (CIO) Council issued the Federal Mobile Security Baseline, Mobile Computing Decision Framework, and Mobile Security Reference Architecture. 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. 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. The above referenced documents will serve as tools to help integrate effective security and privacy measures into the design and adoption of mobile technologies. CIOs and agency procurement officials should work together to ensure that all new purchases of mobile devices and infrastructure support the technical controls in the Federal Mobile Security Baseline.

29. How can organizations leverage the concept of overlays to develop specialized security plans that address specific protection needs?

Overlays are developed when there is divergence from the assumptions used to create the initial security control baselines identified in NIST Special Publication 800-53. Organizations can use overlays to develop a set of security controls for community-wide use (e.g., health care, intelligence, transportation), to address specialized requirements, technologies, or unique missions/environments of operation (e.g., mobile devices, counterterrorism, weapons systems, space-based systems, industrial control systems), or to address specific threats (e.g., insider threats, advanced persistent threats, supply chain threats). When developing an overlay, organizations begin by applying the security categorization process to determine the impact level of the information/information system to be addressed by the overlay and select the appropriate initial security control baseline from NIST Special Publication 800-53. The selected baseline is then tailored to align the controls with the specific conditions associated with the particular technology, threat, mission/environment of operation, etc. to be addressed by the overlay. Organizations then identify and characterize the overlay, provide information on the applicability/scope of the overlay, summarize the overlay, define overlay control specifications, provide definitions and information about tailoring the overlay, and include any additional information or instructions. The overlay is then applied to information/information systems that fall with the scope defined in the overlay. As an example, an overlay for federal agencies wishing to employ cloud computing provided by the private sector was developed by an interagency working group and has been implemented as the FedRAMP. Another example of an overlay developed by an interagency working group is the Federal Mobile Security Baseline. NIST Special Publication 800-53 provides guidance on overlays in Section 3.3 and Appendix I.

Risk Management

30. Why is implementation of the risk management framework (RMF) important?
The RMF is a holistic process, consistent with the system development life cycle, that allows agencies to manage information security commensurate with risk through the application of six distinct but interrelated and mutually reinforcing steps:

- Step 1: **Categorize** the information system and the information processed, stored, and transmitted by that system based on an impact analysis.
- Step 2: **Select** an initial set of baseline security controls for the information system based on the security categorization; tailoring the security control baseline as needed based on an organizational assessment of risk and local conditions.
- Step 3: **Implement** the security controls and describe how the controls are employed within the information system and its environment of operation.
- Step 4: **Assess** the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
- Step 5: **Authorize** information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable.
- Step 6: **Monitor** the security controls in the information system on an ongoing basis including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials.

31. Why must agency information systems be authorized to operate (Step 5 of the RMF)?
The act of authorizing an information system to operate (including the common controls inherited by the system), ensures that senior organizational officials are aware of and understand the actual information security risks and, armed with that information, are able to determine if the risk to agency operations, assets, individuals, other agencies, or the Nation is acceptable. The explicit acceptance of risk is the responsibility of the Authorizing Official and balancing security considerations with mission and operational needs is paramount to achieving an acceptable authorization decision.

32. Is a security authorization required for all information systems? OMB Circular A-130 requires a security authorization to operate only for general support systems and major applications.
Yes. Security authorizations are required for all Federal information systems. Section 3544(b)(3) of FISMA refers to "*subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems*" and does not distinguish between major or other applications. Smaller "systems" and "applications" may be included as part of the assessment of a larger system—as allowable in NIST guidelines and provided an appropriate risk

assessment is completed and security controls are implemented. Security authorizations are also required for all common controls inherited by Federal information systems.

33. Does OMB recognize interim authority to operate for security authorizations?
No. Security authorization has been required for many years, and it is important to measure the implementation of this process to improve consistency and quality government-wide. Introducing additional inconsistency to the Government's security program would be counter to FISMA's goals.

34. Is a security reauthorization still required every 3 years or when an information system has undergone significant change as stated in OMB Circular A-130?
No. Rather than enforcing a static, three-year reauthorization process, agencies are expected to make ongoing authorization decisions for information systems by leveraging security-related information gathered through the implementation of ISCM programs. The implementation of ISCM and ongoing authorization thus fulfill the three-year security reauthorization requirement, so a separate re-authorization process is not necessary.[5] In an effort to implement a more dynamic, risk-based security authorization process, agencies should follow the guidance in NIST Special Publication 800-37. Agencies will be required to report the security state of their information systems and results of their ongoing authorizations through CyberScope in accordance with the data feeds defined by DHS.

35. How can my agency use ISCM to inform ongoing authorization decisions?
Agencies should develop and implement ISCM strategies for all information systems which address all security controls implemented, including the frequency and degree of rigor associated with the monitoring process. ISCM strategies should also include all common controls inherited by organizational information systems. ISCM strategies should be developed in accordance with NIST SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*, and approved by appropriate authorizing officials. Agency officials should monitor the security state of their information systems on an ongoing basis with a frequency sufficient to make ongoing risk-based decisions on whether to continue to operate the systems within their organizations. ISCM programs and strategies should address: (i) establishment of metrics to be monitored; (ii) establishment of frequencies for monitoring/assessments; (iii) ongoing security control assessments to determine the effectiveness of deployed security controls; (iv) ongoing security status monitoring; (v) correlation and analysis of security-related information generated by assessments and monitoring; (vi) response actions to address the results of the analysis; and (vii) reporting the security status of the organization and information system to senior management officials consistent with guidance in NIST SP 800-137.

Testing (Assessments)

36. Why is information system testing and evaluation important?
Assessing and monitoring security controls helps to determine their overall effectiveness, that is, the extent to which operational, technical, and management security controls are implemented

[5] The transition from the three-year reauthorization approach to ongoing authorization should be in accordance with the level of maturity and effectiveness of agency ISCM programs, organizational risk tolerance, and subject to the final decision of authorizing officials.

correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Understanding the overall effectiveness of the security controls implemented in the information system is essential in determining the risk to the organization's operations and assets, to individuals, to other organizations, and to the Nation resulting from the use of the system.

37. Must all agency information systems be tested and evaluated annually?
Yes, all information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency must be tested at least annually. FISMA (Section 3544(b)(5)) requires each agency to perform for all systems "*periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually.*" This testing and evaluation shall include the assessment of management, operational, and technical controls selected and implemented by agencies in accordance with the NIST Risk Management Framework, which includes any associated tailoring activities applied to the initial security control baselines.

38. How can agencies meet the annual testing and evaluation (assess) requirement?
To satisfy the annual FISMA assessment requirement, organizations can draw upon the security control assessment results from any of the following sources, including but not limited to:

- Security assessments conducted as part of an information system security authorization or re-authorization process;
- ISCM activities supporting ongoing authorization; or
- Testing and evaluation of the information system as part of the ongoing system development life cycle process (provided that the testing and evaluation results are current and relevant to the determination of security control effectiveness).

Agencies are required to use NIST Special Publication 800-37 and NIST Special Publication 800-53A for the assessment of security control effectiveness. Existing security assessment results can be reused to the extent that they are still valid and are supplemented with additional assessments as needed. Reuse of assessment information is critical in achieving a broad-based, cost-effective, and fully integrated security program capable of producing the needed evidence to determine the actual security status of the information system.

FISMA does not require an annual assessment of all security controls employed in an organizational information system. In accordance with OMB policy, organizations must determine the necessary depth and breadth of an annual assessment and assess a subset of the security controls based on several factors, including: (i) the NIST FIPS Publication 199 security categorization of the information system; (ii) the specific security controls selected and employed by the organization to protect the information system; (iii) the relative comprehensiveness of the most recent past assessment, (iv) the adequacy and successful implementation of the plan of action and milestone (POA&M) for weaknesses in the system, (v) advice from IGs or United States Computer Emergency Readiness Team (US-CERT) on threats and vulnerabilities at your agency, and (vi) the level of assurance (or confidence) that the organization must have in determining the effectiveness of the security controls in the information system, among others.

Agencies are expected to conduct ongoing authorizations of information systems through the implementation of ISCM programs in accordance with NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems* and NIST SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*.

39. What NIST guidelines must agencies use for their annual testing and evaluations?
Agencies are required to use NIST FIPS Publication 200/NIST SP 800-53, for the specification of security controls and NIST SP 800-37 and NIST SP 800-53A for the assessment of security control effectiveness.

While NIST guidelines do not apply to national security systems, DoD and ODNI participated in the Joint Task Force Transformation Initiative Working Group to produce a unified information security framework that DoD and ODNI are implementing.[6]

40. Why should agencies conduct continuous monitoring of their security controls?
Continuous monitoring of security controls is a cost-effective and important part of managing organizational risk and maintaining an accurate understanding of the security risks related to your agency's information systems. Continuous monitoring of security controls (including system-specific, hybrid, and common controls) is required as part of the Risk Management Framework described in NIST SP 800-37 and across the three tiers of the organization described in NIST SP 800-39 to ensure that the implemented controls remain effective over time (i.e., after the initial security authorization) in the face of changing threats, missions, environments of operation, and technologies.

Agencies should develop an organization-wide strategy for monitoring security controls on an ongoing basis. A robust and effective ISCM program will ensure important procedures included in an agency's security authorization package (e.g., as described in system security plans, security assessment reports, and POA&Ms) are updated as appropriate and contain the necessary information for authorizing officials to make credible risk-based decisions regarding the security posture of the information system on an ongoing basis. This will help make the security authorization process more dynamic and responsive to today's federal missions and rapidly changing conditions. NIST SP 800-37, NIST SP 800-53, and NIST SP 800-137, provide guidance on ISCM programs.

41. Do agencies need to test and evaluate (assess) security controls on low impact information systems?
Yes. While the depth and breadth of security controls testing and evaluation (review) will vary based on information system risk and system impact level, agencies are required to do annual testing and evaluation (review) of *all* systems. NIST SP 800-37 and NIST SP 800-53A provide guidance on assessment of security controls in low-impact information systems.

[6] Additional guidance for national security systems is provided in Committee on National Security Systems (CNSS) Instruction 1253.

Configuration Management[7]

42. What are minimally acceptable system configuration requirements?

FISMA (Section 3544(b)(2)(D)(iii)) requires each agency to develop minimally acceptable system configuration requirements and ensure compliance with them. Common security configurations provide a baseline level of security, reduce risk from security threats and vulnerabilities, and save time and resources. This allows agencies to improve system performance, decrease operating costs, and ensure public confidence in the confidentiality, integrity, and availability of Government information.

In FY 2007, OMB issued policy for agencies to adopt security configurations for Windows XP and VISTA, as well as policy for ensuring new acquisitions include common security configurations. For more information, see OMB Memorandum M-07-11, *Implementation of Commonly Accepted Security Configurations for Windows Operating Systems*, at: http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-11.pdf and OMB Memorandum M-07-18, *Ensuring New Acquisitions Include Common Security Configurations*, at: http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-18.pdf, respectively.

The acquisition language in OMB Memorandum 07-18 was published in the Federal Register, FAR Case 2007-004, *Common Security Configurations*. For all contracts, the following language from Division A, Section 101(h), Title VI, Section 622 of the Omnibus Appropriations and Authorization Act (P.L. 105-277), Part 39 – Acquisition of Information Technology, Section 39. 101 Policy, should be included to encompass Federal Desktop Core Configurations (FDCC):

> *"(d) In acquiring information technology, agencies shall include the appropriate information technology security policies and requirements, including use of common security configurations available from the National Institute of Standards and Technology's website at http://checklists.nist.gov. Agency contracting officers should consult with the requiring official to ensure the appropriate standards are incorporated."*

In FY 2010, the CIO Council announced the creation of the United States Government Configuration Baselines (USGCB) which is maintained by the CIO Council's Technology Infrastructure Subcommittee. Baselines developed by the USGCB should be applied to Federal systems. See http://usgcb.nist.gov/ for information.

43. Why must agencies explain their performance metrics in terms of NIST FIPS Publication 199 categories?

FISMA directed NIST to develop a standard to categorize all information and information systems based upon the need to provide appropriate levels of information security according to a range of risk levels. FIPS Publication 199 defines three levels of potential impact on organizations or individuals in the case of a breach of security (i.e., a loss of confidentiality, integrity, or availability). These impact levels are: low, moderate, and high. Agencies must categorize their information and information systems using one of these three categories in order

[7] NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*, provide guidelines for implementation of security-focused configuration management programs.

to comply with the minimum security requirements described in FIPS Publication 200 and to determine which security control baseline from NIST SP 800-53 to use as a starting point. While NIST guidelines do not apply to national security systems, DoD and ODNI participated in the Joint Task Force Transformation Initiative Interagency Working Group to produce a unified information security framework that DoD and ODNI are implementing.

Plan of Action and Milestones (POA&M)

44. What is required of agency POA&Ms?

As outlined in previous guidance (OMB Memorandum 04-25, *FY 2004 Reporting Instructions for the Federal Information Security Management Act*) Agency POA&Ms must:

1) Be tied to the agency's budget submission through the Unique Project Identifier[8]of a system. This links the security costs for a system to the security performance of a system.

2) Include all security weaknesses found, and in need of remediation, during any other assessment done by, for, or on behalf of the agency, including GAO audits, financial system audits, and critical infrastructure vulnerability assessments. These plans should be the authoritative agency-wide management tool, inclusive of all evaluations.

3) Be shared with the agency IG to ensure independent verification and validation of identified weaknesses and completed corrective actions.

4) Be submitted to OMB upon request.

While agencies are no longer required to follow the exact format prescribed in the POA&M examples in OMB Memorandum 04-25, they must still include all of the associated data elements in their POA&Ms. POA&Ms can be incorporated into the new automated processes that agencies are putting in place as part of their ISCM programs. To facilitate compliance with POA&M reporting requirements, agencies may choose to utilize the FISMA reporting services of a Shared Service Center as part of the Information Systems Security Line of Business. Please note that these FISMA reporting services are not mandatory.

45. Can a POA&M process be effective even when correcting identified weaknesses is untimely?

Yes. The purpose of a POA&M is to identify and track remediation plans for security weaknesses. A POA&M permits agency officials and oversight authorities to identify when documented corrective actions are both timely and untimely. In either circumstance, the POA&M has served its intended purpose. Agency managers can use the POA&M process to focus resources to resolve delays.

[8] Beginning with Budget Year (BY) 2013 submissions, the "Unique Project Identifier" (UPI) has been renamed to "Unique Investment Identifier" (UII). For additional information, refer to the Circular A-11 guidance for BY 2014.

Contractor Monitoring and Controls

46. Must Government contractors abide by FISMA requirements?

Yes. Each agency must ensure their contractors are abiding by FISMA requirements. Section 3544(a)(1)(A)(ii) describes Federal agency security responsibilities as including "information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency." Section 3544(b) requires each agency to provide information security for the information and "information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source." This includes services which are either fully or partially provided, including agency hosted, outsourced, and software-as-a-service (SaaS) type solutions.

Because FISMA applies to both information and information systems used by the agency, contractors, and other organizations and sources, it has somewhat broader applicability than prior security law. That is, agency information security programs apply to all organizations (sources) which process, store, or transmit Federal information – or which operate, use, or have access to Federal information systems (whether automated or manual) – on behalf of a Federal agency. Other organizations may include contractors, grantees, State and Local Governments, industry partners, providers of software subscription services, etc. FISMA, therefore, underscores the longstanding OMB policy concerning sharing Government information and interconnecting systems.

Therefore, Federal security requirements continue to apply and the agency is responsible for ensuring appropriate security controls (see OMB Circular A-130, Appendix III). Agencies must develop policies for information security oversight of contractors and other users with privileged access to Federal data. Agencies must also review the security of other users with privileged access to Federal data and systems.

Finally, because FISMA applies to Federal information and information systems, in certain limited circumstances its requirements also apply to a specific class of information technology that the Clinger-Cohen Act of 1996 (40 U.S.C. § 1401(3)) did not include, i.e., "equipment that is acquired by a Federal contractor incidental to a Federal contract." Therefore, when Federal information is used within incidentally acquired equipment, the agency continues to be responsible and accountable for ensuring FISMA requirements are met.

47. Could you provide examples of "incidental" contractor equipment which is not subject to FISMA?

In considering the answer to this question, it is essential to remember FISMA requires agencies to provide security protections "...commensurate with the risk and magnitude of harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the agency; and information systems used or operated by an agency or other organization on behalf of an agency." This includes services which are either fully or partially provided by another source, including agency hosted, outsourced, and SaaS type solutions.

A corporate human resource or financial management system acquired solely to assist managing corporate resources assigned to a government contract could be incidental provided the system does not use agency information or interconnect with an agency system.

48. Could you provide examples of agency information security responsibilities concerning contractors and other sources?
FISMA requires agencies to provide security protections "...commensurate with the risk and magnitude of harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the agency; and information systems used or operated by an agency or other organization on behalf of an agency." This includes full or partial operations.

While we cannot anticipate all possible combinations and permutations, there are five primary categories of contractors as they relate to securing systems and information: 1) service providers; 2) contractor support; 3) Government Owned, Contractor Operated facilities (GOCO); 4) laboratories and research centers; and 5) management and operating contracts.

1) Service providers -- this encompasses typical outsourcing of system or network operations, telecommunications services, or other managed services (including those provided by another agency and subscribing to software services).

Agencies are fully responsible and accountable for ensuring all FISMA and related policy requirements are implemented and reviewed and such must be included in the terms of the contract. Agencies must ensure identical, not "equivalent," security procedures. For example, annual testing and evaluation, risk assessments, security plans, control assessments, contingency planning, and security authorization must, at a minimum, explicitly meet NIST guidelines. Additionally, IGs shall include some contractor systems in their "representative subset of agency systems," and not doing so presents an incomplete independent evaluation.

Agencies and IGs should, to the maximum extent practicable, consult with other agencies using the same service provider, share security assessment results, and avoid the unnecessary burden on the service provider and the agencies resulting from duplicative assessments and re-assessments. Additionally, provided they meet FISMA and policy requirements, agencies and IGs should accept all or part of the results of industry-specific security assessments performed by an independent auditor on the commercial service provider.

In the case of agency service providers, they must work with their customer agencies to develop suitable arrangements for meeting all of FISMA's requirements, including any special requirements for one or more particular customer agencies. Any arrangements should also provide for an annual evaluation by the IG of one agency. Thereafter, the results of that IG evaluation would be shared with all customer agencies and their respective IGs.

2) Contractor support -- this encompasses on- or off-site contractor technical or other support staff.

Agencies are fully responsible and accountable for ensuring all FISMA and related policy requirements are implemented and reviewed and such must be included in the terms of the contract. Agencies must ensure identical, not "equivalent," security procedures. Specifically, the agency is responsible for ensuring the contractor personnel receive appropriate training (i.e., user awareness training and training on agency policy and procedures).

3) Government Owned, Contractor Operated (GOCO) -- For the purposes of FISMA, GOCO facilities are agency components and their security requirements are identical to those of the managing Federal agency in all respects. Security requirements must be included in the terms of the contract.

4) Laboratories and research facilities -- For the purposes of FISMA, laboratories and research facilities are agency components and their security requirements are identical to those of the managing Federal agency in all respects. Security requirements must be included in the terms of the contract or other similar agreement.

5) Management and Operating Contracts – For the purposes of FISMA, management and operating contracts include contracts for the operation, maintenance, or support of a government-owned or -controlled research, development, special production, or testing establishment.

49. Should agencies include FISMA requirements in grants and contracts?
Yes. Agency contracts including but not limited to those for IT services must reflect FISMA requirements.

The Federal Acquisition Regulation, Part 7, *Acquisition Planning*, Subpart 7.1, *Acquisition Plans*, requires heads of agencies to ensure agency planners on information technology acquisitions comply with the information technology security requirements in the Federal Information Security Management Act, OMB's implementing policies including Appendix III of OMB Circular A-130, and NIST standards and guidelines.

When applicable, agencies must also include FISMA's security requirements in the terms and conditions of grants.

50. How deeply into contractor, state, or grantee systems must a FISMA review reach? To the application, to the interface between the application and their network, or into the corporate network/infrastructure?
This question has a two-part answer. First, FISMA's requirements follow agency information into any system which processes, stores, or transmits such information on behalf of the agency. Second, with respect to system interconnections, as a general rule, OMB assumes agency responsibility and accountability extends to the interface between government systems (or contractor systems performing functions on behalf of the agency) and corporate systems and networks. For example, a corporate network, human resource, or financial management system would not be covered by FISMA requirements, provided the agency has confirmed appropriate security of the interface between them and any system using government information or those

operating on behalf of the agency. See also the discussions concerning interconnection agreements and security authorization boundaries.

51. Must all information systems operated by a contractor on behalf of an agency apply the RMF process the same as agency-operated systems?
Yes. They must be addressed in the same way. As with agency-operated systems, the level of effort applied to implementation of the RMF depends on the impact level of the information contained on each system. Risk Management tasks for a system with an impact level of low will be less rigorous and costly than a system with a higher impact level. More information on system security categorization is available in NIST FIPS Publication 199 and NIST Special Publication (SP) 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*.

FISMA is unambiguous regarding the extent to which contractor-owned or managed systems must comply with FISMA requirements. To the extent that contractor, state, or grantee systems process, store, or transmit Federal information (for which the agency continues to be responsible for maintaining control), the RMF must be applied using the same NIST standards and guidelines as if they were a government-owned or -operated system. The security authorization boundary for these systems must be carefully mapped to ensure that Federal information: (a) is adequately protected, (b) is segregated from the contractor, state or grantee corporate infrastructure, and (c) there is an interconnection security agreement in place to address connections from the contractor, state, or grantee system containing the agency information to systems external to the security authorization boundary.

52. Who is responsible for the POA&M process for contractor systems owned by the contractor?
The agency is responsible for ensuring the contractor corrects weaknesses discovered through self-assessments and independent assessments. Any weaknesses requiring remediation are to be reflected in the agency's POA&M.

Training

53. Do employees who never access electronic information systems need annual security and privacy awareness training?
Yes. FISMA and OMB policy require all employees to receive annual security and privacy awareness training, and they must be included as part of your agency's training totals. When administering your security and privacy awareness training programs, it is important to remember: (i) all employees collect, process, access and/or maintain government information, in some form or format, to successfully perform their duties and support the agency's mission; and (ii) information is processed in various forms and formats, including paper and electronic, and information systems are defined as a discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual.

OMB Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information,* requires that agencies must initially train employees (including managers) on their privacy and security responsibilities before permitting access to agency information and information systems. Thereafter, agencies must provide at least annual refresher training to ensure employees continue to understand their responsibilities. Additional or advanced training should also be provided commensurate with increased responsibilities or change in duties.

Both initial and refresher training must include acceptable rules of behavior and the consequences when the rules are not followed. For agencies implementing telework and other authorized remote access programs, training must also include the rules of such programs.

54. OMB asks agencies whether they have provided information security training and awareness to all employees, including contractors. Is it the agency's responsibility to ensure contractors have security training if they are hired to perform IT security functions? Wouldn't they already be trained by their companies to perform this work?
Per FISMA, each agency shall develop, document and implement an agency-wide information security program that includes security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of: (a) information security risks associated with their activities; and (b) their responsibilities in complying with agency policies and procedures designed to reduce these risks.

Agencies should include in its contracts the requirements for level of skill and experience; however, contractors must be trained on agency-specific security policies and procedures, including rules of behavior.

55. What resources are available to assist agencies in providing annual information security and privacy training to their employees?
The DHS Information System Security Line of Business (ISSLOB) works with agencies on developing standardized curricula, and selecting information security Shared Service Centers (SSC). The ISSLOB SSC's provide agencies with efficient and cost-effective solutions for procuring general information security training for employees and contractors. For more information on this program contact the ISSLOB program management office at isslob@hq.dhs.gov.

Privacy

56. Which agency official should complete the privacy questions in this FISMA report?
These questions shall be completed or supervised by the Senior Agency Official for Privacy (SAOP). Since privacy management may fall into areas of responsibility likely held by several program officials, e.g., the CIO, the Privacy Act Officer, etc., the SAOP shall consult with these officials when responding to these questions, and to those who contributed and/or reviewed the responses to the questions.

57. Must agencies publish a SORN for all systems?
No. As required by the Privacy Act (5 U.S.C. § 552a), agencies must publish a SORN for systems with records about individuals maintained in a system of records covered by the Privacy Act.

58. Are agencies required to conduct a privacy impact assessment (PIA) for IT systems that contain or administer information in identifiable form strictly about Federal employees (including contractors)?
The legal and policy requirements addressing Federal agency computer security apply equally to Federal IT systems containing identifiable information about members of the public and to systems containing identifiable information solely about agency employees (or contractors). That is, as a practical matter, all systems containing information in identifiable form fall subject to the same technical, administrative and operational security controls. Although neither Section 208 of the E-Government Act, nor OMB's implementing guidance mandate agencies conduct PIAs on electronic systems containing information about Federal employees (including contractors), OMB encourages agencies to scrutinize their internal business processes and the handling of identifiable information about employees to the same extent they scrutinize processes and information handling procedures involving information collected from or about members of the public (OMB Memorandum 03-22, Section II.B.3.a.).

59. If an agency chooses to conduct a PIA on systems which only contain information about Federal employees (including contractors), should these be included in the total number of systems reported?
No. Agencies should count only those systems which require a PIA under the E-Government Act. OMB recognizes some agencies choose to conduct a PIA on systems containing information about Federal employees (including contractors), or conduct a "threshold analysis" to determine whether a formal PIA is required for the system. While OMB applauds this level of dedication to privacy awareness and encourages agencies to continue pursuing these efforts, including these additional assessments inhibits meaningful evaluation of agency compliance with Section 208 of the E-Government Act of 2002.

60. Are agencies expected to implement the privacy controls contained in NIST SP 800-53, Appendix J?
Yes. Agencies are expected to implement the privacy controls in Appendix J to satisfy the privacy requirements set forth in the Privacy Act of 1974 and any privacy-related policies published by OMB. Implementing the privacy controls in Appendix J will address some of the issues in the privacy-related questions above.

61. Who has the lead on agency implementation of NIST SP 800-53, Appendix J?
Senior Agency Officials for Privacy (SAOP) are responsible for the implementation of Appendix J. SAOPs will consult with other agency officials, including program mangers/information system owners, Authorizing Officials, Chief Information Officers, and Chief Information Security Officers in fulfilling this responsibility. However, the authority for selection and assessment of privacy controls ultimately rests with SAOPs.

62. Can any NIST SP 800-53, Appendix J privacy controls be treated as common controls?
Yes, privacy controls may be considered as common controls consistent with the agency's particular mission/business needs and risk tolerance. The determination of which controls to treat as common controls must be made by the SAOP, in collaboration and consultation with other agency officials involved in risk management decisions.

63. How does NIST SP 800-53, Appendix J affect agency risk management processes, including the implementation of the Risk Management Framework (RMF) and authorizations to operate for agency information systems?
An assessment of compliance with applicable Appendix J privacy controls must be conducted by the SAOP or the SAOP's designated representative. SAOP approval is required as a precondition for the issuance of an authorization to operate.

64. When are agencies required to implement NIST SP 800-53, Appendix J privacy controls?
The implementation timeframe for NIST 800-53, Appendix J privacy controls is consistent with that established for all other new controls included in SP 800-53, Revision 4 (i.e., immediately for new information systems and one year for legacy systems). SAOPs and agencies' Privacy Officers should be aware, however, that the publication of Appendix J does not relieve agencies from any existing responsibilities for privacy risk management and compliance established by federal privacy legislation, directives, policies, or regulations.

Electronic Authentication

65. What is Electronic Authentication (e-authentication)?
In December 2003, OMB issued Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*, which requires agencies to review new and existing electronic transactions to ensure the authentication processes provide the appropriate level of assurance. It establishes and describes four levels of identity assurance for electronic transactions requiring authentication. Specifically, agencies are to determine assurance levels using the following steps:

1. Conduct an e-authentication risk assessment of the e-government system.
2. Map identified risks to the appropriate assurance level.
3. Select technology based on e-authentication technical guidance.
4. Validate that the implemented system has achieved the required assurance level.
5. Periodically reassess the system to determine technology refresh requirements.

An e-authentication application is an application that meets the following criteria:

1. Is web-based;
2. Requires authentication; and
3. Extends beyond the borders of your enterprise (e.g. multi-agency, government-wide, or public facing)

For additional e-authentication requirements, please refer to NIST SP 800-63, *Electronic Authentication Guidance*, at http://csrc.nist.gov/publications.

Homeland Security Presidential Directive 12 (HSPD-12)

66. When reporting how many Personal Identity Verification (PIV) credentials are being used for authentication to systems, does my agency include only those implementations where the PIV authentication (PIVAUTH) certificate is being used for authentication?

When reporting how many PIV credentials are being used for logical access to systems, agencies should include the following implementations:

- Remote or networked logical access system implementations are PIV-enabled when the implementation uses the Public Key Infrastructure (PKI) Authentication method described in FIPS 201. This includes the PIN, cryptographic challenge response, and full path validation for the PIV Authentication Certificate. Certificate validation may be performed by an intermediary service such as a Server-based Certificate Validation Protocol (SCVP) server. The certificate must be valid at time of access, including the full certificate path to the Common Policy CA. Certificate revocation information can be cached until the next update time included in each Certificate Revocation List (CRL).

- Local workstation logical access system implementations are PIV-enabled when the BIO, BIO-A, CHUID, or PIV Authentication credentials and authentication protocols are in conformance with authentication mechanisms defined in FIPS 201 and NIST SP 800-73, digital signatures on data objects used are verified, and full path validation is performed on any certificates used, including certificates for keys used to sign data objects.

- System implementations protected by an Identity and Access Management solution that adheres to the principles above are also considered PIV-enabled.

For additional information, refer to FIPS 201 at http://csrc.nist.gov/publications/PubsFIPS.html, NIST SP 800-73 at http://csrc.nist.gov/publications/PubsSPs.html, and Federal PKI Policy and FICAM Roadmap and Implementation Guidance at www.idmanagement.gov.

67. What guidance does my agency follow when implementing the use of the PIV credentials for physical access control?

NIST SP 800-116, "*A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)*," provides guidance concerning the use of the PIV credential for physical access. OMB M-06-18 states agencies "must ensure that only approved products/services from the Approved Products List are acquired and incorporated into system solutions and ensure compliance with other federal standards and requirements for systems used to implement HSPD-12. In order to ensure government-wide interoperability, this applies for the lifecycle of products, services, and/or systems being acquired." Agencies should not include in the count of PIV-enabled physical access control any situations where the PIV credential is being used to support legacy systems, including but not limited to situations where physical access control systems use PIV credential modifications (such as additional legacy antennas, MAG Stripe, 3D Barcode, 2D Barcode, etc.) Nor should agencies count manual physical access control (i.e. using the PIV credential as a "flash-pass"). Full path validation must be performed for any content signer of a PIV container that is used for authentication.

68. For the purposes of HSPD-12 implementation, what is meant by "federal facilities" or "systems?"

You may refer to Page 3 of OMB Memorandum 05-24, "*Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors,*" for a definition of federally controlled facilities and information systems. Each agency is expected to have identified all of its facilities and is to report on whether all the physical access control systems and card readers controlling access to these facilities have been upgraded to be HSPD-12 compliant in accordance with NIST and General Services Administration (GSA) guidance. When reporting the number of FISMA systems enabled to use PIV credentials, it is expected that all applications included as part of the FISMA system use the PIV credential as the means to gain access. Additionally, physical access control systems which include servers, databases, workstations and appliances in either shared or isolated networks are to be included in the count of reported systems.

For additional information regarding HSPD-12, please visit http://www.idmanagement.gov.

Definitions

Adequate Security (defined in OMB Circular A-130, Appendix III, (A)(2)(a))
Security is commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls.

Capital Planning and Investment Control Process (as defined in OMB Circular A-130, (6)(c))
A management process for ongoing identification, selection, control, and evaluation of investments in information resources. The process links budget formulation and execution, and is focused on agency missions and achieving specific program outcomes.

The Federal Risk Authorization Management Program
FedRAMP will provide a cost-effective, risk-based approach for the adoption and use of cloud services by making available to Executive departments and agencies: (1) Standardized security requirements for the authorization and ongoing cybersecurity of cloud services for selected information system impact levels; (2) A conformity assessment program capable of producing consistent independent, third-party assessments of security controls implemented by CSPs; (3) Authorization packages of cloud services reviewed by a Joint Authorization Board (JAB) consisting of security experts from the DHS, DOD, and GSA; (4) Standardized contract language to help Executive departments and agencies integrate FedRAMP requirements and best practices into acquisition; and 5) A repository of authorization packages for cloud services that can bc leveraged government-wide.

Information Security (defined by FISMA, section 3542(b)(1)(A-C))
Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide: (A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity; (B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and (C) availability, which means ensuring timely and reliable access to and use of information.

Information System (defined in OMB Circular A-130, (6)(q))
The term "information system" means a discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual.

Information Technology (defined by the Clinger-Cohen Act of 1996, sections 5002, 5141 and 5142)
Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. For purposes of this definition, equipment is used by an agency whether the agency uses the equipment directly or it is used by a

contractor under a contract with the agency which (1) requires the use of such equipment or (2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. Information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. It does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract.

Major Acquisition/Investment (defined in OMB Circular A-11, section 300)
Major acquisition/investment means a system or project requiring special management attention because of its importance to the mission or function of the agency, a component of the agency or another organization; is for financial management and obligates more than $500,000 annually; has significant program or policy implications; has high executive visibility; has high development, operating or maintenance costs or is defined as major by the agency's capital planning and investment control process.

National Security System (defined in FISMA, section 3542 (b)(2)(A-B))
(A) The term "national security system" means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency--

(i) the function, operation, or use of which--

(I) involves intelligence activities;
(II) involves cryptologic activities related to national security;
(III) involves command and control of military forces;
(IV) involves equipment that is an integral part of a weapon or weapons system; or
(V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or

(ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

(B) Subparagraph (A)(i)(V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

Plan of Action and Milestone (POA&M) (defined in OMB Memorandum M-02-01)
A POA&M, also referred to as a corrective action plan, is a tool that identifies tasks that need to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates for the milestones. The purpose of the POA&M is to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems.

Privacy Impact Assessment (PIA) (See OMB Memorandum 03-22)
A process for examining the risks and ramifications of using information technology to collect, maintain and disseminate information in identifiable form from or about members of the public, and for identifying and evaluating protections and alternative processes to mitigate the impact to privacy of collecting such information.

Security Controls (defined in NIST FIPS Publication 199)
Security controls are defined as the management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

Security Program (defined by FISMA, Section 3544(b)(1-8))
Each agency shall develop, document, and implement an agency wide information security program, approved by the Director under section 3543(a)(5), to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

Significant Deficiency
A significant deficiency is a weakness in an agency's overall information systems security program or management control structure, or within one or more information systems, that significantly restricts the capability of the agency to carry out its mission or compromises the security of its information, information systems, personnel, or other resources, operations, or assets. In this context, the risk is great enough that the agency head and outside agencies must be notified and immediate or near-immediate corrective action must be taken.

As required in FISMA (section 3544(c)(3)), agencies are to report any significant deficiency in policy, procedure, or practice as a material weakness in reporting under FMFIA and if relating to financial management systems, as an instance of a lack of substantial compliance under FFMIA.

Security Control Assessment
The testing and/or evaluation of the management, operational, and technical security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization.