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

THE DIRECTOR

November 18, 2013

M-14-03

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Sylvia M. Burwell
Director

SUBJECT: Enhancing the Security of Federal Information and Information Systems

Our nation's security and economic prosperity depend on ensuring the confidentiality, integrity and availability of Federal information and information systems. To strengthen the nation's cybersecurity posture, the Office of Management and Budget (OMB) identified cybersecurity as one of 14 Cross Agency Priority (CAP) Goals,[1] established in accordance with the Government Performance and Results Modernization Act.[2] This memorandum provides agencies with guidance for managing information security risk on a continuous basis and builds upon efforts towards achieving the cybersecurity CAP goal.[3] The requirement to manage information security risk on a continuous basis includes the requirement to monitor the security controls in Federal information systems and the environments in which those systems operate on an ongoing basis—one of six steps in the National Institute of Standards and Technology (NIST) Risk Management Framework.[4] This allows agencies to maintain ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.[5]

By strengthening the underlying information technology infrastructure through the application of state-of-the-art architectural and engineering solutions, and leveraging automation to support the implementation of the Risk Management Framework (which includes the ongoing monitoring of security controls), agencies can improve the effectiveness of the safeguards and countermeasures protecting federal information and information systems in order to keep pace with the dynamic threat landscape. Another important benefit of having a robust program for managing information security risk on a continuous basis is the support it provides for ongoing authorization—that is, the ongoing determination and acceptance of information security risk. Rather than enforcing a static, point-in-time reauthorization process, agencies shall conduct ongoing authorizations of their information systems and environments in which those systems

---

[1] The CAP goal helps 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 statuses change*. It accomplishes this by measuring agency implementation of Trusted Internet Connections; strong authentication through the use of multi-factor authentication in accordance with Homeland Security Presidential Directive-12; and monitoring information systems' security controls on a continuous basis.

[2] See http://goals.performance.gov/goals_2013.

[3] The direction included in this memorandum applies to non-national security systems.

[4] See NIST Special Publication 800-37 at: http://csrc.nist.gov/publications/PubsSPs.html.

[5] See NIST Special Publication 800-137 at: http://csrc.nist.gov/publications/PubsSPs.html.

operate, including common controls,[6] through the implementation of their risk management programs. Enhancing the security of information systems can also play an important role in protecting privacy by more thoroughly safeguarding the information in those systems.

During the past year, the Federal Government has undertaken the following actions to support and accelerate agency implementation of effective risk management programs. In coordination with OMB, the Federal Chief Information Officer's Council (CIOC) and the Committee on National Security Systems (CNSS) established the Joint Continuous Monitoring Working Group (JCMWG), which developed the *United States Government Concept of Operations (CONOPS) for Information Security Continuous Monitoring*. This CONOPS supplements NIST guidelines by providing a roadmap and more specific implementation guidance to stakeholders across the Federal government. Agencies shall implement continuous monitoring of security controls[7] (step 6 in the Risk Management Framework) as part of a phased approach through Fiscal Year (FY) 2017.[8]

In conjunction with this effort, the Department of Homeland Security (DHS) has established a Continuous Diagnostics and Mitigation (CDM) Program.[9] Under this program, DHS coordinated with the General Services Administration (GSA) to establish a government-wide Blanket Purchase Agreement (BPA) under Multiple Award Schedule 70, which Federal, State, local and tribal governments can leverage to deploy a basic set of capabilities to support continuous monitoring of security controls in Federal information systems and environments of operation. The BPA, awarded on August 12th, 2013, provides a consistent, government-wide set of information security continuous monitoring (ISCM) tools to enhance the Federal government's ability to identify and respond, in real-time or near real-time, to the risk of emerging cyber threats. It also capitalizes on strategic sourcing to minimize the costs associated with implementing requirements of the Risk Management Framework.

To fully implement ISCM across the Government, agencies shall:

1) Develop and maintain, consistent with existing statutes, OMB policy, NIST guidelines[10] and the CONOPS, an ISCM strategy, and establish an ISCM program that:
    a. Provides a clear understanding of organizational risk and helps officials set priorities and manage such risk consistently throughout the agency; and
    b. Addresses how the agency will conduct ongoing authorizations of information systems and the environments in which those systems operate, including the agency's use of common controls.[11]

---

[6] As defined in NIST Special Publication 800-37 located at: http://csrc.nist.gov/publications/PubsSPs.html.
[7] Refers to the ongoing monitoring of security controls in Federal information systems and environments of operation.
[8] Phase 1 focus areas are discussed in the CONOPS and on page 10 of this document.
[9] The DHS CDM Program is one of the key components in a comprehensive ISCM program and is based upon NIST standards and guidelines.
[10] NIST Special Publications 800-37; 800-39; 800-53; 800-53A; and 800-137 provide guidance on ISCM and are available at: http://csrc.nist.gov/publications/PubsSPs.html.
[11] "Common Control" refers to a security control that is inherited by one or more organizational information systems. Refer to NIST SP 800-39 at: http://csrc.nist.gov/publications/PubsSPs.html.

2) Establish plans, in coordination with DHS, to implement an agency ISCM program;[12]

3) Standardize, to the extent practicable, the requirement to establish ISCM as an agency-wide solution, deploying enterprise ISCM products and services instead of developing multiple, disparate services across agency bureaus and components;[13]

4) Establish plans, to the extent practicable, to migrate to the GSA BPA as contract terms expire for acquisition vehicles currently used to acquire ISCM products and services. If an agency determines that it cannot use the GSA BPA, the agency Chief Operating Officer or the Deputy Secretary must submit a letter of attestation to the OMB Deputy Director for Management (and send a copy to egov@omb.eop.gov) with a justification as to why they cannot use the BPA, and demonstrate that the total cost to implement ISCM products and services from agency-specific or other contract vehicles is less than pricing available from the BPA;

5) Submit specified security-related information to the Federal ISCM dashboard maintained by DHS;

6) Evaluate and upgrade information systems and deploy new products, as needed, including agency and component ISCM dashboards, to support ISCM and the need to submit security-related information, as requested by OMB and DHS;

7) Require that external service providers hosting Federal information meet Federal information security requirements for ISCM.[14] This includes FedRAMP requirements for cloud computing;[15] and

8) Ensure adequate staff and training to meet the objectives of the ISCM program.

In addition to the general agency responsibilities described above:

1) OMB will continue to oversee agency information security practices, in accordance with the Federal Information Security Management Act of 2002;[16]

---

[12] These plans can fully leverage the DHS CDM Program, provide for an agency–specific ISCM implementation or leverage a hybrid between the two.

[13] These actions should be consistent with the OMB Memoranda M-11-29 and M-13-09. See http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-29.pdf and http://www.whitehouse.gov/sites/default/files/omb/memoranda/2013/m-13-09.pdf.

[14] Federal Acquisition Regulation Part 7, Subpart 7.1 requires that agency planners of information technology acquisitions comply with the requirements in the Federal information Security Management Act, OMB's implementing policies, and NIST standards and guidelines. See http://www.acquisition.gov/far.

[15] See https://cio.gov/wp-content/uploads/2012/09/fedrampmemo.pdf.

[16] See Public Law 107-347, Title III, Subchapter III, Section 3543 at http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf

2) DHS shall work with each agency to establish an ISCM implementation program that capitalizes on the processes established in the CONOPS and leverages, to the extent practicable, the BPA;

3) DHS, in consultation with OMB, shall establish a Federal dashboard for ISCM, which will provide a government-wide view of ISCM, as well as the technical specifications and guidance for agencies on the requirements for submitting information to this Federal dashboard;

4) DHS, in coordination with OMB, shall monitor the implementation of agencies ISCM strategies and programs in conjunction with PortfolioStat[17] and through CyberStat;[18]

5) The JCMWG, in coordination with stakeholders, shall update the CONOPS at least annually; and

6) NIST shall issue additional guidance on conducting ongoing authorizations.

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.

The attachment provides more specific direction and timelines for agencies to implement ISCM. For additional information on the DHS CDM Program, please contact cdm.fns@dhs.gov. For additional information regarding the GSA BPA, please contact cdm@gsa.gov or refer to http://www.gsa.gov/cdm. Questions relating to this policy may be directed to OMB at egov@omb.eop.gov.

Attachment

[17] See http://www.whitehouse.gov/sites/default/files/omb/memoranda/2012/m-12-10_1.pdf and http://www.whitehouse.gov/sites/default/files/omb/memoranda/2013/m-13-09.pdf.
[18] See http://www.whitehouse.gov/sites/default/files/omb/memoranda/2012/m-12-20.pdf.

Attachment: This attachment outlines specific actions for agencies to follow in establishing their information security continuous monitoring (ISCM) programs. Additional guidance will be provided, as needed, as the DHS Continuous Diagnostics and Mitigation (CDM) and agency programs mature.

Contents

Coordinate Federal ISCM Efforts
The Federal Chief Information Officer Council's Information Security and Identity Management Committee (ISIMC) along with the Committee on National Security Systems (CNSS) have established the Joint Continuous Monitoring Working Group (JCMWG) to provide consistent guidance for the ISCM[19] of both non-national security and national security systems.

In support of ISCM, the JCMWG developed the *United States Government Concept of Operations (CONOPS) for Information Security Continuous Monitoring.*[20] To support ISCM and the implementation of the DHS CDM Program, the JCMWG will continue to collaborate and coordinate with agencies and appropriate stakeholders to define the strategic and operational guidance for the successful implementation of ISCM throughout the federal government.

Develop, Maintain, and Implement ISCM Strategy
Agencies are required to develop and maintain an ISCM strategy and implement an ISCM program in accordance with NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach,* NIST Special Publication 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, and* NIST Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations.*[21] Agencies should also follow implementation guidance outlined in the CONOPS.

The ISCM strategies shall address all security controls selected and implemented by agencies, including the frequency of and degree of rigor associated with the monitoring process.[22] ISCM strategies, which must be approved by the appropriate agency authorizing official, shall also include all common controls inherited by organizational information systems. Additionally, all strategies must address the agencies' plans for transitioning to and maintaining consistency with Federal information security policies, standards, and guidelines. Agency officials shall monitor the security state of their information systems and the environments in which those systems operate 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.[23]

---

[19] ISCM is one part of a 3-tiered Risk Management Framework process as defined by NIST in Special Publication 800-39. See http://csrc.nist.gov/publications/PubsSPs.html.
[20] While the CONOPS applies to national security systems and non-national security systems, this memorandum applies only to non-national security systems. The CONOPS is available at: https://max.omb.gov/community/x/7YFaE.
[21] Agencies can develop either overarching (agency-wide/bureau/component/etc.) ISCM strategies that address all information systems or ISCM strategies for each agency information system. Such continuous strategies shall include the monitoring of all security controls (including common controls) at agency defined frequencies.
[22] Security control selection and implementation refer to steps 2 and 3 of the NIST Risk Management Framework (RMF) which includes any tailoring activities applied by agencies to the initial security control baselines. Security controls selected and implemented by agencies (including common controls, hybrid controls, and system-specific controls) are documented in associated security plans.
[23] Rather than enforcing a static, three-year reauthorization process, agencies are expected to conduct ongoing authorizations of information systems. This includes the ongoing authorization of common controls inherited by organizational information systems. ISCM programs fulfill the three-year security reauthorization requirement required by Circular A-130 (dated November 2000), so a separate reauthorization process is not necessary.

Required Action	Deadline	Responsible Entity
Develop ISCM strategy (or strategies)	February 28, 2014	All agencies

Assess and Develop Staff and Resources

Agencies shall ensure adequate staff and training are in place to meet the objectives of the ISCM program. To support agencies' implementations, DHS will coordinate interagency advisory and user groups and provide training and mentoring to agency managers on how to implement ISCM. For those agencies obtaining ISCM services offered through the DHS CDM Program, contract support will be provided to help implement sensors across multiple agencies to reduce the learning curve and provide consistent implementation. Agencies shall ensure any additional budget needs are addressed during the development of their annual budget.

Required Action	Deadline	Responsible Entity
Identify resource and skill requirement gaps (if any) to manage and coordinate the internal ISCM program	April 30, 2014	All agencies
Identify specific individuals to manage the agency ISCM program	April 30, 2014	All agencies

Procure Products and Services

DHS has worked with GSA to make available products and services (including ISCM dashboards) to support the implementation of ISCM through strategic sourcing. Unless agencies have already procured ISCM products and services to support Phase 1 focus areas,[24] procurements for the timelines below apply to all agencies regardless of whether or not they use the GSA BPA for ISCM products and services. Agencies shall identify capability gaps and procure products and services, as needed, to implement their ISCM strategy. In addressing gaps, agencies should leverage, to the extent practicable, the GSA BPA. The initial suite of products available on the GSA BPA covers hardware asset management, software asset management (including malware management), configuration setting management, and common vulnerability management (from the National Vulnerability Database).[25] The suite of products will eventually be expanded to cover additional capabilities, to support future phases as outlined in the CONOPS and NIST security controls. Services may include operation and maintenance of these products as well as integration of security-related information gathered through the ISCM process into the appropriate dashboards.

To the extent that agencies reduce their ISCM costs by leveraging the GSA BPA and participating in the DHS CDM program, those agencies shall reinvest the savings to improve their risk management processes. As agencies transition from traditional static (i.e., point-in-time driven) assessment and authorization processes to ongoing assessment and authorization

[24] Phase 1 focus areas are discussed in the CONOPS and on page 10 of this document.
[25] See http://nvd.nist.gov/.

processes, they are expected to leverage their existing funding to implement ISCM. The DHS CDM program funding may be used to address gaps in products and services for civilian agencies.[26]

Required Action	Deadline	Responsible Entity
Complete CDM foundational survey and return to DHS	Immediately, if not already completed	All civilian agencies
Sign Memorandum of Agreement (MOA) with DHS	Immediately, if not already completed	All civilian agencies receiving DHS CDM services
Begin to procure products and services to support Phase 1 focus areas (as described in the CONOPS)	February 28, 2014	All agencies

Deploy Products

Agencies shall evaluate capability gaps, upgrade their infrastructure and deploy new products, as needed, to support ISCM and the requirement to automate the submission of security-related information to OMB and DHS. As outlined in the CONOPS, agencies have a variety of options when implementing their ISCM technical architecture, which include:

a. Leveraging the services and products offered by the DHS CDM Program;
b. Leveraging the agency's existing products and services; and/or
c. Implementing a hybrid approach where agencies can leverage the DHS CDM Program to procure products, for example, but implementing it using their own hardware.

Required Action	Deadline	Responsible Entity
Begin to deploy products to support ISCM of all systems	May 30, 2014	All agencies
Ensure all information systems are authorized to operate in accordance with Federal requirements prior to initiating ISCM for those systems	May 30, 2014	All agencies

Deploy ISCM Dashboards

Beginning in FY 2014, all agencies must submit security-related information to an extensible ISCM dashboard for agency-level and Federal government-wide views. A standard set of dashboards will help agencies use the security-related information on a daily basis to identify and address their highest priority security issues. DHS shall establish the Federal dashboard through

[26] DHS CDM program funding may only be used to assist the Executive branch civilian agencies, excluding DOD and the intelligence community. Please see Public Law 113-6, Division D, Title V, Section 558, subsection (e) at http://www.gpo.gov/fdsys/pkg/BILLS-113hr933enr/pdf/BILLS-113hr933enr.pdf.

which agencies shall report security-related information. The Federal dashboard will be maintained by DHS, and will be focused on managing the highest priority and most serious risks based on risk assessment information and the risk tolerance established by individual agencies. DHS, in consultation with OMB, will provide guidance for security-related information and associated technical specifications required to be reported to the Federal dashboard.

The Federal dashboard, maintained by DHS, shall provide information on specific vulnerabilities identified that could lead to adverse impacts to missions/business functions.[27] It will also supply data on agency performance for use by oversight entities to help identify the level of risk reduction which is both possible and beneficial for agencies (depending on their risk-based needs). Data gathered from the Federal dashboard will be used by DHS to develop guidance for agencies with the intent of improving decision making regarding risk/cost tradeoffs.

For agencies obtaining services offered by the DHS CDM Program, integration of products with DHS supplied dashboards shall be provided. In the event an agency uses sensor products other than those offered through the GSA BPA as part of the CDM Program, the agency shall be responsible for providing required security-related information to the DHS-supplied dashboard. Once the DHS-supplied dashboard is integrated with the products (e.g., sensors), it is the expectation of the DHS CDM Program that minimal agency effort will be required to provide the necessary security-related information to the Federal dashboard.

Regardless of the implementation approach, all agencies shall deliver security-related information to the DHS supplied dashboard(s) in accordance with requirements provided by DHS, in coordination with OMB. Additionally, it is the sole responsibility of the agency to respond to risks identified as a result of the ISCM program.[28]

Required Action	Deadline	Responsible Entity
Publish technical specifications for agency data feeds for Phase 1 focus areas to the Federal dashboard	3 months prior to deployment of the Federal dashboard	DHS
Ensure that all Phase 1 products necessary to meet DHS reporting requirements provide data compatible with the Federal dashboard maintained by DHS	Within 3 months of the Federal dashboard being deployed	All agencies
Complete installation of agency and bureau/component-level dashboards	Within 6 months of the Federal dashboard being deployed	All agencies

[27] As noted on page 10, the security-related information gathered for input to the Federal dashboard will not provide the comprehensive information required for agencies to make risk-based decisions regarding the effectiveness of all selected and implemented security controls. Additional security-related information will be needed to make fully-informed, risk-based decisions.

[28] In accordance with NIST Special Publication 800-39, agency risk responses can include accepting, rejecting, mitigating, transferring, or sharing information security risk.

Required Action	Deadline	Responsible Entity
Begin submitting automated data feeds for Phase 1 focus areas to the Federal dashboard	Within 6 months of the Federal dashboard being deployed	All agencies

Implement ISCM
In accordance with the CONOPS, the Phase 1 FY 2014 focus areas for the DHS CDM Program, including the Federal dashboard, include automating the following subset of information security capabilities:

- Hardware Asset Management;
- Software Asset Management (including malware management);
- Configuration Setting Management; and
- Common Vulnerability Management;

While four initial information security capability areas have been identified on which agencies must automate and automatically report to DHS for integration to the Federal dashboard, this does not eliminate the need for agencies to monitor *all* security controls documented in their security plans and implemented within agency information systems and environments of operation. The security-related information gathered for input to the Federal dashboard will not provide the comprehensive information required to make risk-based decisions about the effectiveness of all selected and implemented security controls. Additional security-related information will be needed to make fully informed risk-based decisions regarding specific information systems. In accordance with NIST guidelines, agencies are expected to automate the monitoring of security controls whenever feasible. Agencies are also expected to document risk response decisions.

For additional information on Phase 1 priorities for the DHS CDM Program, refer to the CONOPS. Timelines for subsequent phases shall be provided by the JCMWG in updates to the CONOPS. Agencies shall complete all ISCM requirements described in this memorandum by the end of FY 2017.

Required Action	Deadline	Responsible Entity
Analyze, and respond to vulnerabilities identified on the local dashboards[29]	Starting immediately upon activation of local dashboards	All agencies

Provide for Ongoing Authorization and Re-authorization
When fully implemented in accordance with NIST guidelines and the CONOPS, ISCM programs will support the process of ongoing authorization by providing authorizing officials with sufficient information regarding the current security state of their information systems and environments of operation, including the effectiveness of the security controls employed within, and inherited by, the systems. A well-designed and well-managed ISCM program can

[29] Agencies may choose to accept, reject, share, transfer or mitigate risks that arise from the identified vulnerabilities. These risk response decisions should be appropriated documented.

effectively transform an otherwise static security control assessment and authorization process into a dynamic process that provides essential, near real-time security-related information to agencies. Senior leaders can use this information to take appropriate risk response actions and make cost-effective, risk-based decisions regarding the operation of their information systems. Once established, a robust ISCM program will allow agencies to track the security state of their information systems on an ongoing basis and maintain the security authorizations for those systems over time. These ISCM and ongoing authorization processes meet the security assessment and authorization requirements defined in OMB Circular A-130.[30]

ISCM programs should begin enabling the transition to ongoing authorization—that is, the ongoing determination and acceptance of information security risk. The complete transition to ongoing authorization should be implemented in accordance with the specific transition criteria established by agencies, including such considerations as the maturity and effectiveness of their ISCM programs, organizational risk tolerance, and the concerns of authorizing officials and other agency officials responsible and accountable for managing information security risk.

Continuous monitoring-generated, security-related information is used to determine whether continued operation of the information system is acceptable, based on ongoing risk determinations. If such risk is not acceptable, the continuous monitoring-generated information helps guide and inform authorizing officials as to which steps in the Risk Management Framework[31] need to be revisited and/or what actions need to be initiated within the three risk management tiers described in NIST Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, in order to adequately respond to the additional risk.

In accordance with NIST guidelines and subject to agency policy, information systems that have completed the Risk Management Framework and have been granted an initial authorization to operate are subsequently eligible to transition into an ongoing authorization process, assuming the agency has a comprehensive and effective ISCM program in place. Formal reauthorization actions may still be conducted based on the risks identified by ISCM and/or may be initiated at the discretion of authorizing officials in accordance with Federal or agency policies. This may include, for example, revisiting all the steps in the Risk Management Framework similar to the initial authorization.

Continuous monitoring-generated information can also be leveraged as assessment evidence in formal reauthorization actions, as in stated in NIST Special Publication 800-37. Continuous monitoring-generated information used to support ongoing authorizations must satisfy the independence requirements defined in NIST Special Publication (SP) 800-37; SP 800-53; and SP 800-137. In addition to following NIST guidelines, agencies can obtain additional guidance on ongoing authorization in the CONOPS.

---

[30] See http://www.whitehouse.gov/omb/circulars_default

[31] Refer to NIST Special Publication 800-37 at: http://csrc.nist.gov/publications/PubsSPs.html.

Required Action	Deadline	Responsible Entity
Publish guidance establishing a process and criteria for agencies to conduct ongoing assessments and authorizations	March 31, 2014	NIST
Update ISCM strategies to describe the process for performing ongoing authorizations	Within 3 months of receiving additional guidance in this area (either from the NIST, DHS, and/or the JCMWG)	All agencies

Perform Independent Evaluations

As part of the annual Federal Information Security Management Act (FISMA) reporting process, agency Inspectors General will conduct annual reviews of agency implementation of ISCM.

Required Action	Deadline	Responsible Entity
Determine whether agencies have documented their ISCM strategy	November 15, 2014 (and each year thereafter)	Inspectors General
Assess whether agencies have implemented ISCM for information technology assets	November 15, 2014 (and each year thereafter)	Inspectors General
Evaluate agencies' risk assessments used to develop their ISCM strategy	November 15, 2014 (and each year thereafter)	Inspectors General
Verify that agencies conduct and report on ISCM results in accordance with their ISCM strategy	November 15, 2014 (and each year thereafter)	Inspectors General

Additional Information

1. Nothing in this memorandum shall be interpreted to mean that agencies must mitigate every vulnerability resulting in organizational risk identified as part of the ISCM effort. Each agency must assess organizational risk and justify risk responses including risk acceptance decisions.

2. Over time, ISCM programs may identify new and emerging vulnerabilities and the potential mission/business risks resulting from the exploitation of such vulnerabilities. ISCM programs are designed to facilitate the prioritization of risk response actions in order to manage risk appropriately.

3. 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 Federal Information Processing Standard (FIPS) Publication 199, and use the results of that categorization to select one of the three security control baselines described in NIST Special Publication 800-53. Agencies are subsequently expected to:

    a. Use the baselines as a starting point in the security control selection process;
    b. Apply the tailoring guidance in Special Publication 800-53, eliminating or adding controls as necessary, based on an assessment of risk; and
    c. 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.

4. Agencies are required to monitor all selected and implemented controls in their security plans on an ongoing basis in accordance with NIST Special Publication (SP) 800-39; SP 800-37; SP 800-137; and their ISCM 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 Committee on National Security Systems (CNSS) Instruction 1253.

5. FISMA (Section 3544(b)(5)) requires each agency to perform, for all information 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 review 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. FISMA, however, does not require an annual assessment of *all* security controls employed in agency information systems. To satisfy the annual FISMA assessment requirement, agencies 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 to 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.

Summary of Required Actions

Required Action	Deadline	Responsible Entity
Develop ISCM strategy (or strategies)	February 28, 2014	All agencies
Identify resource and skill requirement gaps (if any) to manage and coordinate the internal ISCM program	April 30, 2014	All agencies
Identify specific individuals to manage the agency ISCM program	April 30, 2014	All agencies
Complete CDM foundational survey and return to DHS	Immediately, if not already completed	All civilian agencies
Sign Memorandum of Agreement (MOA) with DHS	Immediately, if not already completed	All civilian agencies receiving DHS CDM services
Begin to procure products and services to support Phase 1 focus areas (as described in the CONOPS)	February 28, 2014	All agencies
Begin to deploy products to support ISCM for all systems	May 30, 2014	All agencies
Ensure all information systems are authorized to operate in accordance with Federal requirements prior to initiating ISCM for those systems	May 30, 2014	All agencies
Publish technical specifications for agency data feeds for Phase 1 focus areas to the Federal dashboard	3 months prior to deployment of the Federal dashboard	DHS

Required Action	Deadline	Responsible Entity
Ensure that all Phase 1 products necessary to meet DHS reporting requirements provide data compatible with the Federal dashboard maintained by DHS	Within 3 months of the Federal dashboard being deployed	All agencies
Complete installation of agency and bureau/component-level dashboards	Within 6 months of the Federal dashboard being deployed	All agencies
Begin submitting automated data feeds for Phase 1 focus areas to the Federal dashboard	Within 6 months of the Federal dashboard being deployed	All agencies
Analyze, and respond to vulnerabilities identified on the local dashboards	Starting immediately upon activation of local dashboards	All agencies
Publish guidance establishing a process and criteria for agencies to conduct ongoing assessments and authorizations	March 31, 2014	NIST
Update ISCM strategies to describe the process for performing ongoing authorizations	Within 3 months of receiving additional guidance in this area (either from the NIST, DHS, and/or the JCMWG)	All agencies
Determine whether agencies have documented their ISCM strategy	November 15, 2014 (and each year thereafter)	Inspectors General
Assess whether agencies have implemented ISCM for information technology assets	November 15, 2014 (and each year thereafter)	Inspectors General
Evaluate agencies' risk assessments used to develop their ISCM strategy	November 15, 2014 (and each year thereafter)	Inspectors General
Verify that agencies conduct and report on ISCM results in accordance with their continuous monitoring strategy	November 15, 2014 (and each year thereafter)	Inspectors General