OFFICE OF
INSPECTOR GENERAL
U.S. DEPARTMENT OF THE INTERIOR

INDEPENDENT AUDITORS' PERFORMANCE AUDIT REPORT ON THE U.S. DEPARTMENT OF THE INTERIOR FEDERAL INFORMATION SECURITY MODERNIZATION ACT FOR FISCAL YEAR 2016

This is a revised version of the report prepared for public release.

OFFICE OF
INSPECTOR GENERAL
U.S.DEPARTMENT OF THE INTERIOR

MAR 10 2017

Memorandum

To: Sylvia Burns
Chief Information Officer

From: Mary L. Kendall
Deputy Inspector General

Subject: Independent Auditors' Performance Audit Report on the U.S. Department of the Interior Federal Information Security Modernization Act for Fiscal Year 2016
Report No. 2016-ITA-062

This memorandum transmits the KPMG LLP (KPMG) Federal Information Security Modernization Act (FISMA) audit report of the U.S. Department of the Interior (DOI) for fiscal year (FY) 2016. FISMA (Public Law 113-283) requires Federal agencies' Offices of Inspectors General (OIG) to independently evaluate their agencies' information security programs and practices and determine their effectiveness, or designate an independent external auditor to do so.

KPMG, an independent public accounting firm, performed the DOI FY 2016 FISMA audit under a contract issued by DOI and monitored by OIG. As required by the contract, KPMG asserted that it conducted the audit in accordance with Generally Accepted Government Auditing Standards to obtain sufficient, appropriate evidence to provide a reasonable basis for its findings and conclusions based on the audit objectives. KPMG is responsible for the findings and conclusions expressed in the audit report. OIG does not express an opinion on the report, nor on KPMG's conclusions regarding DOI's compliance with laws and regulations.

FISMA reporting has been completed in accordance with Office of Management and Budget Memorandum M-17-05, "Fiscal Year 2016-2017 Guidance on Federal Information Security and Privacy Management Requirements," dated November 04, 2016.

KPMG reviewed information security practices, policies, and procedures at the DOI Office of the Chief Information Officer and 12 DOI bureaus and offices:

- Bureau of Indian Affairs;
- Bureau of Land Management;
- Bureau of Reclamation;
- Bureau of Safety and Environmental Enforcement;
- Fish and Wildlife Service;
- Interior Business Center;
- National Park Service;
- Office of Inspector General;

- Office of The Secretary;
- Office of Surface Mining Reclamation and Enforcement;
- Office of the Special Trustee for American Indians; and
- U.S. Geological Survey.

To ensure the quality of the audit work, we—

- reviewed KPMG's approach and planning of the audit;
- evaluated the auditors' qualifications and independence;
- monitored the audit's progress at key milestones;
- engaged in regularly scheduled meetings with KPMG and DOI management to discuss audit progress, findings, and recommendations;
- reviewed KPMG's supporting work papers and audit report; and
- performed other procedures as deemed necessary.

KPMG identified needed improvements in most areas audited, including contractor systems, configuration management, identity and access management, information security continuous monitoring, incident response and contingency planning. KPMG made 21 recommendations related to these control weaknesses intended to strengthen the respective bureaus and offices, as well as the Department's information security program. In its response to the draft report, the Office of the Chief Information Officer fully concurred with 19 and partially concurred with 2 recommendations, and stated it was either in the process of taking or planned to take corrective actions. The corrective actions for the two partially concurred recommendations, however, will depend on the implementation of other programs.

We will refer KPMG's recommendations to the Office of Financial Management for audit follow-up. The legislation creating OIG requires that we report to Congress semiannually on all audit, inspection, and evaluation reports issued; actions taken to implement recommendations; and recommendations that have not been implemented.

We appreciate the cooperation and assistance of DOI personnel during the audit. If you have any questions regarding the report, please contact me at 202-208-5745.

Attachment

The United States Department of the Interior
Office of Inspector General
Federal Information Security Modernization Act of 2014
Fiscal Year 2016 Performance Audit

February 10, 2017

KPMG LLP
1676 International Drive
McLean, Virginia 22102

KPMG LLP
1676 International Drive
McLean, VA 22102

February 10, 2017

Ms. Mary L. Kendall
Deputy Inspector General
U.S. Department of the Interior
Office of Inspector General
1849 C Street, NW MS 4428
Washington, DC 20240-0001

Dear Ms. Kendall:

This report presents the results of our work conducted to address the performance audit objectives relative to the Fiscal Year (FY) 2016 Federal Information Security Modernization Act of 2014 (FISMA) Audit for information systems**.** We performed our work during the period of May 24 to September 30, 2016 and our results are as of February 10, 2017.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The audit objective(s) of our work were to for the year ending September 30, 2016:

- Perform the annual independent FISMA audit of DOI's information security programs and practices related to the financial and non-financial information systems in accordance with the FISMA, Public Law 113-283, 44 USC 3554.
- Assess the implementation of the security control catalog contained in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision (Rev) 4. We utilized criteria and guidance, including Federal Information Processing Standard (FIPS) Publication (PUB) 199, FIPS PUB 200, and NIST SP 800-37 Rev 1. Criteria and guidance were used to evaluate DOI's implementation of the risk management framework and the extent of implementation of select security controls.
- Prepare responses for each of the Department of Homeland Security (DHS) FISMA Reporting Metrics on behalf of the DOI Office of Inspector General (OIG) to support documented conclusions with appropriate rationale/justification as to the effectiveness of the information security program and practices of the DOI for each area evaluated and overall.

Our procedures tested security control areas identified in NIST SP 800-53 and additional security program areas identified in the 2016 FISMA Reporting Metrics for the OIG. Our sample was selected from information systems distributed across 12 Bureaus/Offices. These Bureaus/Offices are Bureau of Indian Affairs (BIA), Bureau of Land Management (BLM), Bureau of Reclamation (BOR), Bureau of Safety and Environmental Enforcement (BSEE),National Park Service (NPS), Office of the Chief Information Officer (OCIO), Office of Inspector General (OIG), Office of the Secretary (OS), Office of Surface Mining Reclamation and Enforcement (OSMRE), the Office of the Special Trustee for American Indians (OST), U.S. Fish and Wildlife Service (FWS), and U.S. Geological Survey (USGS). At the conclusion of our test

procedures, we aggregated the individual bureau and information system results by control area to produce results at the Department level.

As part of the FISMA performance audit of the subset of DOI information systems, we assessed the effectiveness of the Department's information security program and practices and the implementation of the security controls in NIST SP 800-53 Revision 4. We identified needed improvements in most areas audited including contractor systems, configuration management, identity and access management, information security continuous monitoring, incident response and contingency planning.

The following table summarizes the control areas tested and the control deficiencies identified in the fiscal year 2016 FISMA Reporting Metrics for the OIG.

Cybersecurity Framework Security Functions[1]	Summary of Results
1. Identify (Contractor System Oversight)	DOI has established a contractor system oversight program. However, DOI has not fully: • defined and documented roles, responsibilities and procedures for government oversight, monitoring, and reporting.
2. Protect (Configuration Management and Identity and Access Management)	DOI has established configuration management and identity and access management programs. However, DOI has not fully: • Ensured that [redacted] are fully implemented in accordance with DOI policy; • Tested and implemented the [redacted] for one information system; • disabled vulnerable [redacted]; • completed post-implementation activities to verify [redacted] compliance for one system; • implemented a process for the review of [redacted] accounts; • performed and documented [redacted], to include users with [redacted]; • implemented a process to identify [redacted] on the network; and • enforced the requirement to enable [redacted] for one Bureau.
3. Detect (Information Security	DOI has established an information security continuous monitoring program. However, DOI has not fully:

[1] Metrics organized around the five information security functions outlined in the NIST Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework): Identify, Protect, Detect, Respond, and Recover.

Continuous Monitoring)	• documented how the information security continuous monitoring activities integrate with organizational risk management activities and shared with individuals with significant security responsibilities; • defined and documented qualitative and quantitative performance measures to assess the effectiveness of the program; • documented how automation will be used to [redacted] on the DOI network; and • validated implementation of the [redacted] application on all servers on one information system.
4. Respond (Incident Response)	DOI has establish an incident response program. However, DOI has not fully: • updated relevant incident response policies and procedures; • defined qualitative and quantitative performance measures to assess effectiveness of incident response program; and • developed a process to determine how technology is to be used to [redacted] for users and information systems.
5. Recover (Contingency Planning)	DOI has established a contingency planning program. However, DOI has not fully: • reviewed and updated information system contingency plans; and • tested information system contingency plans in accordance with Departmental security policy.

We have made 21 recommendations related to these control weaknesses intended to strengthen the respective Bureaus, Offices, and the Department's information security program. Also, the report includes six appendices, Appendix I summarizes the program areas in which bureaus and offices have control deficiencies, Appendix II list of acronyms, Appendix III provides the status of FY15 recommendations; Appendix IV lists the NIST Special Publication 800-53 security controls cross-referenced to the FY2016 OIG FISMA metrics, Appendix V provides the FY2016 OIG FISMA Reporting metrics, and Appendix VI provides the description of the information security continuous monitoring model for FY2016.

This performance audit did not constitute an audit of financial statements in accordance with *Government Auditing Standards*. KPMG was not engaged to, and did not; render an opinion on the U.S. Department of the Interior's internal controls over financial reporting or over financial management systems. KPMG cautions that projecting the results of our evaluation to future periods is subject to the risks that controls may become inadequate because of changes in conditions or because compliance with controls may deteriorate.

KPMG LLP

Table of Contents

`

Background

Mission of the DOI and its Bureaus/Offices

The U.S. Department of the Interior (DOI) protects America's natural resources and heritage, honors our cultures and tribal communities, and supplies the energy to power our future. DOI is composed of a number of Bureaus and a number of additional Offices that fall under the Office of the Secretary, the Assistant Secretary for Policy, Management and Budget, Solicitor's Office and Office of Inspector General. Of those, the following 12[2] Bureaus and Offices are included within the scope of the Office of Inspector General's (OIG) FISMA reporting for 2016:

1 The **Bureau of Indian Affairs (BIA)** is responsible for the administration and management of 55 million surface acres and 57 million acres of subsurface minerals estates held in trust by the United States for American Indian, Indian tribes, and Alaska Natives.

2 The **Bureau of Land Management (BLM)** administers 262 million surface acres of America's public lands, located primarily in 12 Western States. The BLM sustains the health, diversity, and productivity of the public lands for the use and enjoyment of present and future generations.

3 The **Bureau of Reclamation (BOR)** manages, develops, and protects water and related resources in an environmentally and economically sound manner in the interest of the American public.

4 The **Bureau of Safety and Environmental Enforcement (BSEE)** is responsible for overseeing the safe and environmentally responsible development of energy and mineral resources on the Outer Continental Shelf.

5 The **U.S. Fish and Wildlife Service (FWS)** was created to conserve, protect, and enhance fish, wildlife, and plants and their habitats for the continuing benefit of the American people.

6 The **National Park Service (NPS)** supports to preserve unimpaired the natural and cultural resources and values of the national park system, a network of nearly 400 natural, cultural, and recreational sites across the nation, for the enjoyment, education, and inspiration of this and future generations.

7 The **Interior Business Center** provides the executive leadership, policy, guidance, independent program evaluation, and coordination needed to manage the diverse, complex, nationally significant programs that are DOI's responsibility.

8 The **Office of Inspector General (OIG)** accomplishes its mission by performing audits, investigations, evaluations, inspections, and other reviews of the DOI's programs and operations. They independently and objectively identify risks and vulnerabilities that directly affect, or could impact, DOI's mission and the vast responsibilities of its bureaus and entities. Their objective is to improve the accountability of DOI and their responsiveness to Congress, the Department, and the public.

9 The **Office of the Secretary (OS)** is primarily responsible for providing quality services and efficient solutions to meet DOI business needs through its most important asset – its people.

10 The **Office of Surface Mining (OSMRE)** carries out the requirements of the Surface Mining Control and Reclamation Act in cooperation with States and Tribes. Their primary objectives are to ensure that coal

[2]. Our sample resulted in a subset of information systems distributed over 12 Bureaus/Offices.

mines are operated in a manner that protects citizens and the environment during mining and assures the land is restored to beneficial use following mining, and to mitigate the effects of past mining by aggressively pursuing reclamation of abandoned coal mines.

11 The **Office of the Special Trustee for American Indians (OST)** improves the accountability and management of Indian funds held in trust by the federal government.

12 The **U.S. Geological Survey (USGS)** serves the nation by providing reliable scientific information to describe and understand the earth; minimize loss of life and property from natural disasters; manage water, biological, energy, and mineral resources; and enhance and protect our quality of life.

Information Technology (IT) Organization

The Office of the Chief Information Officer (OCIO) heads the security management program for the Department. The Chief Information Security Officer (CISO) serves as the head of the OCIO's Information Management and Assurance Division, assumed responsibility of all Information Assurance (IA) functions within the OCIO as CISO. The Bureaus/Offices have an Associate Chief Information Officers. Many Bureaus/Offices also have Bureau Chief Information Security Officers (BCISOs) that are responsible for the local implementation of the Department's information security program.

FISMA

Federal Information Security Modernization Act of 2014: (1) reestablish the oversight authority of the Director of the Office of Management and Budget (OMB) with respect to agency information security policies and practices, and (2) set forth authority for the Secretary of Homeland Security (DHS) to administer the implementation of such policies and practices for information systems.

Objective, Scope, and Methodology

The objectives for this performance audit were to for the year ending September 30, 2016:

- Perform the annual independent Federal Information Systems Security Modernization Act of 2014 (FISMA) audit of DOI's information security programs and practices related to the financial and non-financial information systems in accordance with the FISMA, Public Law 113-283, 44 USC.
- Assess the implementation of the security control catalog contained in the NIST SP 800-53 Rev 4. We utilized criteria and guidance, including FIPS 199, FIPS 200, and NIST SP 800-53 Rev 4, to evaluate the implementation of the risk management framework and the extent of implementation of security controls selected from the security control catalog. The table in Appendix IV lists the NIST SP 800-53 revision 4 controls[3] considered during the performance audit.
- Prepare responses for each of the OMB/Department of Homeland Security (DHS) FISMA Reporting Metrics on behalf of the DOI OIG to support documented conclusions on the effectiveness of the information security program and practices of the DOI for each area evaluated.

[3] The Department is in the process of formally approving and fully implementing relevant information security policies and procedures in accordance with NIST SP 800-53 revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, with an anticipated completion date of December 31, 2016.

The scope of our audit included the following:

- An inspection of relevant information security practices and policies established by the DOI Office of the Chief Information Officer (OCIO) as they relate to the FY2016 OIG FISMA reporting metrics; and
- An inspection of the information security practices, policies, and procedures in use across 12 Bureaus and Offices identified by the DOI OIG, specifically, BIA, BLM, BOR, BSEE, FWS, NPS, IBC, OIG, OS, OSMRE, OST, and USGS.

Specifically, our approach followed two steps:

Step A: Department and Bureau level Compliance – During this step we gained Department and Bureau understanding of the FISMA-related policies and guidance established by the DOI OCIO. We examined the policies, procedures, and practices established to the applicable Federal laws and criteria to evaluate whether the Department and Bureaus are generally consistent with FISMA.

Step B: Assessment of the implementation of select security controls from the NIST SP 800-53 revision 4. During this process, we assessed the implementation of a selection of security controls from the NIST SP 800-53 Rev 4, for our representative subset (10 %) of DOI's information systems.[4]
The controls selected addressed areas covered by the DHS FY2016 Inspector General Federal Information Security Modernization Act Reporting Metrics.

The DOI Statement of Work (SOW) for the FISMA audit required us to perform our procedures on a subset of systems defined by the Department as at least 10% of the information systems in the DOI's authoritative information system inventory in the Cyber Security Assessment and Management (CSAM) application. The table below identifies the information systems audited.

Table 1. DOI Information Systems Audited

BUREAU OF INDIAN AFFAIRS					
System Name	**Acronym**	**CSAM ID**	**FIPS 199 Category**	**Type**	**Location**
[redacted]	[redacted]	[redacted]	Moderate	[redacted]	[redacted]

[4] In accordance with the Request for Quotation (RFQ) No. D11PS40153 for Financial Audit Services for the U.S. Department of the Interior, Office of the Inspector General RFQ# D 11PD40 153 Financial Audit Services, dated January 26, 2011; we employed a random sampling approach to determine a representative subset of 10 percent of the DOI information systems. That representative subset includes Major Applications and General Support Systems with Federal Information Processing Standard (FIPS) 199 security categorizations of "Low," "Moderate," and "High". The FIPS 199 ratings are defined by the DOI system owner and authorizing official. We randomly selected 13 of 123 operational systems, which represents 10 percent of the total DOI information systems recorded in CSAM.

BUREAU OF LAND MANAGEMENT					
System Name	**Acronym**	**CSAM ID**	**FIPS 199 Category**	**Type**	**Location**
[redacted]	[redacted]	[redacted]	Moderate	[redacted]	[redacted]

BUREAU OF RECLAMATION					
System Name	**Acronym**	**CSAM ID**	**FIPS 199 Category**	**Type**	**Location**
[redacted]	[redacted]	[redacted]	Moderate	[redacted]	[redacted]

BUREAU OF SAFETY AND ENVIRONMENTAL ENFORCEMENT					
System Name	**Acronym**	**CSAM ID**	**FIPS 199 Category**	**Type**	**Location**
[redacted]	[redacted]	[redacted]	Moderate	[redacted]	[redacted]

U.S. FISH AND WILDLIFE SERVICE					
System Name	**Acronym**	**CSAM ID**	**FIPS 199 Category**	**Type**	**Location**
[redacted]	[redacted]	[redacted]	Moderate	[redacted]	[redacted]

INTERIOR BUSINESS CENTER					
System Name	**Acronym**	**CSAM ID**	**FIPS 199 Category**	**Type**	**Location**
[redacted]	[redacted]	[redacted]	Moderate	[redacted]	[redacted]

NATIONAL PARKS SERVICE					
System Name	**Acronym**	**CSAM ID**	**FIPS 199 Category**	**Type**	**Location**
[redacted]	[redacted]	[redacted]	Moderate	[redacted]	[redacted]

OFFICE OF THE CHIEF INFORMATION OFFICER					
System Name	**Acronym**	**CSAM ID**	**FIPS 199 Category**	**Type**	**Location**
[redacted]	[redacted]	[redacted]	Moderate	[redacted]	[redacted]

OFFICE OF INSPECTOR GENERAL					
System Name	**Acronym**	**CSAM ID**	**FIPS 199 Category**	**Type**	**Location**
[redacted]	[redacted]	[redacted]	Moderate	[redacted]	[redacted]

OFFICE OF THE SECRETARY					
System Name	**Acronym**	**CSAM ID**	**FIPS 199 Category**	**Type**	**Location**
[redacted]	[redacted]	[redacted]	Moderate	[redacted]	[redacted]

OFFICE OF SURFACE MINING RECLAMATION AND ENFORCEMENT					
System Name	**Acronym**	**CSAM ID**	**FIPS 199 Category**	**Type**	**Location**
[redacted]	[redacted]	[redacted]	Low	[redacted]	[redacted]

OFFICE OF THE SPECIAL TRUSTEE FOR AMERICAN INDIANS					
System Name	**Acronym**	**CSAM ID**	**FIPS 199 Category**	**Type**	**Location**
[redacted]	[redacted]	[redacted]	Moderate	[redacted]	[redacted]

U.S. GEOLOGICAL SURVEY					
System Name	**Acronym**	**CSAM ID**	**FIPS 199 Category**	**Type**	**Location**
[redacted]	[redacted]	[redacted]	Moderate	[redacted]	[redacted]

Results of Review

We identified needed improvements in most areas audited including contractor systems, configuration management, identity and access management, information security continuous monitoring, incident response and contingency planning.

1. Implementation of the Contractor System Oversight

KPMG noted the following control deficiencies in the Office of the Secretary contractor system oversight program.

The Office of the Secretary (OS) and Office of the Chief Information Officer (OCIO) manages [redacted] operational contractor-operated systems and relies on contractors to operate these information systems on their behalf.

OS and OCIO's processes and procedures for monitoring contractor-operated systems are not formally documented, consistently performed, and not consistently reported to appropriate levels of management.

KPMG inquired of OS and the OCIO management, and was informed that procedures have not been documented for OS/OCIO system owners and Information System Security Officers (ISSO) to routinely monitor and report to appropriate levels of management contractor performance or non-performance of required security controls.

KPMG inspected documentation, including the [redacted] *for U.S. Department of the Interior* v1.2, and noted that contractor requirements and responsibilities were documented, but government oversight roles and responsibilities were not fully defined. Similarly, the [redacted], dated October 1, 2011, describes contractor performance requirements, but not government oversight roles and responsibilities.

NIST SP 800-53 Rev 4, SA-9 External Information System Services states:

Control: The organization:

a. Requires that providers of external information system services comply with organizational information security requirements and employ [*Assignment: organization-defined security controls*] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;

b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and

c. Employs [*Assignment: organization-defined processes, methods, and techniques*] to monitor security control compliance by external service providers on an ongoing basis.

OS/OCIO have not formally defined and documented government oversight procedures and assigned roles and responsibilities for monitoring of contractor provided systems and services to ensure contractors are performing, monitoring and reporting required security controls in accordance with contractual requirements.

Contractor information security controls may not be implemented and operating effectively in accordance with DOI information security policies and procedures, which could lead to increased risk to DOI data and information.

We recommend that DOI:

1. Ensure OS and OCIO define and document roles, responsibilities and procedures for government oversight, monitoring and reporting of contractor provided systems and services to ensure contractors are performing, monitoring and reporting required security controls in accordance with contractual requirements.

2. Implementation of the Configuration Management Program

KPMG noted the following weaknesses at eight of 12 bureaus and offices, BIA, BLM, BOR, BSEE, FWS, NPS, OIG, and USGS configuration management programs. Similar control weaknesses were identified during the fiscal year 2015 FISMA audit.

BIA:

KPMG conducted a vulnerability assessment over the Bureau of Indian Affairs (BIA)'s [redacted]

KPMG tested 13 of 13 [redacted] and noted that 43 [redacted] were not consistently implemented in accordance with Departmental security policies.

[redacted] KPMG informed BIA management of the condition and provided detailed results of testing.

BLM:

KPMG conducted a vulnerability assessment over the BLM [redacted] Network devices were judgmentally selected and KPMG identified 5,383 [redacted] and noted that 28,817 [redacted] consistently implemented in accordance with Departmental security policies. However, it was determined that [redacted] identified were unique to the environment.

Vulnerabilities identified were related to [redacted]

Additionally, [redacted] KPMG informed BLM management of the condition and provided detailed results for testing. Upon notification, BLM proactively coordinated remediation efforts [redacted]

During the testing period, the Department of the Interior (DOI) mandated the use of their [redacted] to a new client solution allowing BLM to [redacted] in a timely manner.

[5] Risk ratings were determined by the manufacture of the vulnerability assessment tool.

[6] [redacted]

Management informed KPMG and provided evidence that remediation was ongoing around the items noted during the testing period, but KPMG was unable to confirm the extent of the remediation.

BOR:

KPMG conducted a vulnerability assessment over the [redacted]. KPMG tested 39 of 47 [redacted] and noted that 397 [redacted]s were not consistently implemented in accordance with Departmental security policies. [redacted]

[redacted]

Additionally, [redacted] KPMG noted that management is in the process of upgrading the systems to the latest [redacted] Furthermore, KPMG noted two of five sampled software in the [redacted].

KPMG informed BOR management of the condition and provided detailed results of testing. Management informed KPMG that there was an issue with the [redacted] Furthermore, management informed KPMG that the [redacted] has since been remediated, in addition to other remediation efforts ongoing around the items noted from the testing period, but KPMG was unable to confirm the extent of the remediation.

BSEE:

KPMG performed a vulnerability assessment over selected networked devices on the BSEE's [redacted]. Network devices were judgmentally selected and included 878 network devices across the [redacted] and supporting networks and noted that 3,142[8] [redacted] were not fully implemented, although they were deployed in accordance with Departmental security policies.

[redacted]

Additionally, [redacted], unless otherwise approved by the Office of the Chief Information Officer (OCIO).

[redacted] KPMG informed BSEE management of the condition and provided detailed results of testing. Management informed

[7] Risk ratings were determined by the manufacture of the vulnerability assessment tool.
[8] Vendor released [redacted] may count each version as an individual item.

KPMG that six (6) Plan of Action and Milestones (POA&Ms) were created for the conditions described above, all with a completion [redacted]

- POA&M [redacted]
- POA&M [redacted];
- POA&M [redacted];
- POA&M [redacted];
- POA&M [redacted] and
- POA&M [redacted].

BSEE management took immediate action when notified of security weaknesses.

[redacted]

KPMG validated that [redacted], and obtained evidence of the removal to support the remediation. KPMG also validated that [redacted] were updated. Remediation efforts around the remaining [redacted] were noted during the testing period, but KPMG was unable to confirm the extent of the [redacted] remediation.

FWS:

KPMG conducted a vulnerability assessment over the Fish and Wildlife Service (FWS)'s [redacted] and noted that information technology [redacted] were not consistently implemented in accordance with policy. KPMG evaluated 13 of 13 devices and noted 147 [redacted]

Management informed KPMG that remediation was ongoing around the items noted during the audit. In particular, [redacted] were scheduled for replacement shortly after completion of KPMG testing. FWS management had not attempted to [redacted] and instead focused on their replacement. [redacted]

NPS:

KPMG conducted a vulnerability assessment on over the [redacted]

KPMG tested 155 of 190 [redacted] and noted 1,996 [redacted] consistently remediated in accordance with Departmental security policies.

[redacted]

[9] Risk ratings were determined by the manufacture of the vulnerability assessment tool.

Additionally, [redacted]. KPMG informed management of the condition and provided detailed results for testing. Management informed KPMG that correction actions were taken to [redacted] and validated by KPMG. Furthermore, KPMG was informed that additional remediation efforts were ongoing around the remaining items noted from the testing period but KPMG was unable to confirm the extent of the remediation.

OIG:

KPMG conducted a vulnerability assessment over the [redacted] Network devices were judgmentally selected for testing and KPMG identified 249 of 276 network devices [redacted] and noted that 357 [redacted] were not consistently implemented in accordance with Departmental security policies.

[redacted]

Additionally, [redacted], unless otherwise approved by the Office of the Chief Information Officer (OCIO). KPMG informed OIG management of the condition and provided detailed results of testing. KPMG validated management's corrective actions [redacted]. Management informed KPMG and provided evidence that additional remediation efforts were ongoing around the items noted during the testing period, but KPMG was unable to confirm the extent of the remediation.

USGS:

KPMG conducted a vulnerability assessment over [redacted], and noted that information technology [redacted] consistently implemented timely. KPMG identified 309 of 384 network devices [redacted] and noted 702 [redacted] consistently implemented in accordance with Departmental security policies.

[redacted]

[redacted] unless otherwise approved by the Office of the Chief Information Officer (OCIO). Management informed KPMG that [redacted] has been approved internally for usage [redacted], however Departmental approval was not obtained. Furthermore, it was noted that monthly credentialed vulnerability scans are performed by the Information

[10] Risk ratings were determined by the manufacture of the vulnerability assessment tool.

[redacted], which exceeds the Department's defined standard of scanning on a quarterly basis. However, it was noted that [redacted] failed to properly [redacted] to management's security scans.

Furthermore, [redacted] onfiguration file that is used to implement STIG settings did not completely configure the server.

USGS management took immediate action when notified of the security weaknesses, and provided evidence of remediation efforts around the items noted from the testing period; however, KPMG was unable to re-perform the internal vulnerability assessment to confirm and validate the extent of the remediation.

Table 1 below summarizes the number of [redacted] for each information system evaluated.

Table 1. Summary of vulnerability assessment results

Bureau/ Office	System	Number of network devices [redacted]	Number of [redacted] identified	Number of [redacted]
BIA	[redacted]	13 of 13	43	1
BLM	[redacted]	5,383 of 6,685	28,817	244
BOR	[redacted]	39 of 47	397	28
BSEE	[redacted]	878 of 1,052	3,142	48
FWS	[redacted]	13 of 13	147	15
NPS	[redacted]	155 of 190	1,996	60
OIG	[redacted]	249 of 276	357	8
OCIO	[redacted]	70 of 70	151	4
OS	[redacted]	2 of 2	5	0
OS-IBC	[redacted]	6 of 6	11	2
OSMRE	[redacted]	2 of 2	10	0
OST	[redacted]	14 of 14	128	1
USGS	[redacted]	309 of 384	702	42

[11] [redacted] is a configuration methodology for standardizing configuration security settings and protocols to improve security.

[12] [redacted]

Department of the Interior, Security Control Standard, Risk Assessment version 1.3, dated December 2012, RA-5 Vulnerability Scanning states:

"Control: The organization:

a. Scans for vulnerabilities in the information system and hosted applications quarterly for operating system(s), web application(s), and database(s) (as applicable) and when new vulnerabilities potentially affecting the system/applications are identified and reported;

b. Employs vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for:

- Enumerating platforms, software flaws, and improper configurations;
- Formatting and making transparent, checklists and test procedures; and
- Measuring vulnerability impact;

c. Analyzes vulnerability scan reports and results from security control assessments;

d. Remediates legitimate vulnerabilities within thirty days for high-risk vulnerabilities; within ninety days for moderate risk vulnerabilities in accordance with an organizational assessment of risk; and

e. Shares information obtained from the vulnerability scanning process and security control assessments with designated personnel throughout the organization to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies)."

Department of the Interior, Security Control Standard, System and Information Integrity version 1.2, dated December 2012, SI-2 Flaw Remediation states:

"Control: The organization:

a. Identifies, reports, and corrects information system flaws;

b. Tests software updates related to flaw remediation for effectiveness and potential side effects on organizational information systems before installation; and

c. Incorporates flaw remediation into the organizational configuration management process."

Department of the Interior, Security Control Standard, Configuration Management, version 1.2, dated December 2012, control CM-02 – Baseline Configuration states:

"Control: The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system".

Additionally, control CM-06 – Configuration Settings states:

"c. Identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements"

Lastly, control CM-8 – Information System Component Inventory states:

"Control: The organization develops, documents and maintains an inventory of information system components that:

a. Accurately reflects the current information system;

is consistent with the authorization boundary of the information system…"

BIA - Due to the [redacted] system source code [redacted], the system is configured to support [redacted] methods. Additionally, required research or manual remediation is required to address a portion of the vulnerabilities identified on the [redacted] led to challenges in implementing documented [redacted] in a timely manner in order to meet the Departmental 30 day requirement.

BLM - During the course of the audit, BLM management was in the process of implementing a mechanism [redacted] to provide [redacted] tracking and enforcement.

BOR – Due to the following reasons, [redacted] in accordance with DOI policy:

- Technical issues with the [redacted] server led to inaccurate [redacted] status; and
- Usage of unsupported [redacted]

BSEE - BSEE receives the notification of [redacted] from a third-party application vendor, a BSEE security analyst submits a change request to the Change Control Board (CCB) for approval to apply [redacted] that are released monthly are pre-approved changes, which do not require separate CCB approval. [redacted] are tested before they are deployed.

There are a number of reasons why a [redacted] is not deployed to every system in the environment.

- Testing identifies side effects;
- The auto-deployment tools [redacted] fail to roll out [redacted] correctly to all systems;
- The individual system fails to accept [redacted];
- The responsible parties do not apply [redacted] to their respective systems; and
- Citrix-based Teleworker systems [redacted] because the systems are not on the network. Teleworkers who use [redacted].

FWS - Due to the required research or manual remediation required to address a portion of the vulnerabilities identified on the [redacted] that cannot be resolved through the automated [redacted] not consistently implemented in order to meet the 30-day requirement of remediation.

NPS - Due to the current testing and [redacted], deployment of [redacted] coordination efforts between separate entities led to challenges in remediating documented IT security vulnerabilities in a timely manner in order to meet the 30-day requirement of remediation.

OIG - Due to the timing of [redacted] testing, management had not implemented or created POA&Ms for the required IT [redacted] within the designated timeline for critical or high-risk items.

USGS - Management had not confirmed that proper credentials were deployed to the entire [redacted] to provide authenticated scans for a number of devices, and as a result was not obtaining complete insight into the vulnerability posture of the environment, in addition to restricting the use of [redacted]. Furthermore, due to the manual process of [redacted] systems, management has difficulty in comprehensively implementing [redacted] within the designated timeline for critical and high-risk items. Additionally, due to the additional research or manual remediation required to address a portion of the vulnerabilities identified, [redacted]

consistently implemented in order to meet the 30-day requirement of remediation. A process has not been developed for a post-implementation review of the application of [redacted] settings.

Inconsistent [redacted] can lead to increased risk to the computing environment, which is vital to bureau and office mission. The organizational risks could lead to potential inappropriate system access, system errors, and potential lost or disclosure of information.

We recommend DOI ensure:

2. BIA enforce existing processes to ensure IT [redacted] are implemented in accordance with the Department of the Interior, Security Control Standard [redacted] and develop a solution for the web server source code utilizing [redacted] that would allow the upgrade [redacted]
3. BLM complete the implementation of [redacted] that will allow BLM to effectively [redacted] connected to the network.
4. BOR test and deploy the latest appropriate [redacted] and ensure approved configuration baselines are applied.
5. BSEE implement a follow up process to address those systems that fail initial [redacted] to ensure all devices [redacted] in a timely manner. Systems that require extensive testing prior to [redacted] could affect the due dates [redacted] should be identified and addressed appropriately by management.
6. FWS enhance oversight and compliance to ensure all relevant and appropriate [redacted] in order to effectively implement [redacted] as required. If required remediation timelines cannot be adhered to, consistently document the business rationale or technical issue delaying vulnerability remediation.
7. NPS augment the existing testing and [redacted] to ensure effective coordination efforts between separate entities occur, allowing [redacted] to be remediated timely in accordance with the Department of the Interior, Security Control Standard for [redacted].
8. OIG ensure [redacted] in accordance with the Department of the Interior, Security Control Standard for [redacted]; and maintain POA&Ms [redacted] requiring additional time for implementation.
9. USGS ensure the proper authentication is used in performing credentialed vulnerability scanning on all moderate and high-impact networked devices [redacted]

   Augment the existing testing and [redacted] to ensure effective coordination efforts between the [redacted] occur, allowing [redacted] to be implemented timely in accordance with the Department of the Interior, Security Control Standard for [redacted].

   Obtain approval from the DOI OCIO to continue the use of [redacted]

   Ensure that [redacted] management enhance the Configuration Management Standard Operating Procedures to include a post-implementation process review of [redacted] to ensure successful implementation of [redacted] settings.

3. Implementation of the Identity and Access Management Program

KPMG noted the following weaknesses in two of 12 bureaus and offices, BIA and USGS identity and access management programs. Similar control weaknesses were identified during the fiscal year 2015 FISMA audit.

BIA

KPMG noted the following control deficiencies with the BIA account management process.

BIA has not formally documented a process for review of [redacted] accounts. In addition, BIA has not effectively implemented controls to ensure that accounts for [redacted] in a timely manner. Specifically, KPMG determined that 2 of 25 [redacted] to the BIA network after [redacted]. KPMG notified BIA management of the condition and management performed corrective action [redacted]; which KPMG validated the [redacted].

USGS

Based on inquiry of management, KPMG determined that USGS has not implemented a [redacted] before connecting to the network. KPMG was informed that some system owners have identified the need and are considering implementing the technology in the future.

KPMG observed the Department [redacted] compliance report for USGS and noted [redacted] was enforced for 78.22% of [redacted], which is less than the 85% requirement.

KPMG also noted the [redacted] process does not ensure all [redacted], are reviewed on at least an annual basis to determine whether [redacted] is appropriate. Additionally, USGS, in coordination [redacted], has not defined and implemented a process for the annual review and validation of Ce[redacted]

DOI Security Control Standard Access Control, version 1.4, dated December 2012, AC-2 Account Management

Control: The organization manages information system accounts, including:

g. Notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes;

j. Reviewing accounts annually.

DOI Security Control Standard Identification and Authentication, version 4.1, dated December 2015, IA-3 Device Identification and Authentication

Control: The information system uniquely identifies and authenticates *System Owner defined specific and/or types of devices* before establishing a local, remote or network connection.

Office of Management and Budget (OMB) Memorandum for Heads of Executive Departments and Agencies, M-16-04 states:

"To build on the strong authentication progress made during the Cybersecurity Sprint, in FY 2016 Federal agencies should continue to target the Administration Cybersecurity CAP goal of 100% strong authentication for all privileged users and 85% strong authentication for unprivileged users."

BIA performs an informal review of [redacted] on a bi-weekly basis. However, this review has not been formalized and is not documented and maintained. Additionally, the BIA Operations Team was not appropriately notified of the [redacted] in order to [redacted] in a timely manner. Due to the technological complexity of the [redacted], BIA has not identified a feasible compensating control to ensure these [redacted] in a timely manner.

USGS security management has not taken responsibility to implement a solution to [redacted] connecting to the network.

Due to the complexity of their environment, USGS security management has encountered difficulties in implementing [redacted].

USGS and [redacted] failed to develop a process to include the review of [redacted].

Not formally conducting a periodic review of [redacted] increases the risk of a user inappropriately retaining access and privileges to critical and sensitive resources, potentially compromising the security of the network. Not [redacted] users increases the risk [redacted] being inappropriately [redacted] potentially compromising the security of the network.

Without implementing a [redacted] USGS increases the risk of [redacted] the network resulting in the potential of malicious activity to USGS data and resources.

Without consistently enforcing [redacted] the risk increases that [redacted] could be compromised resulting in identity fraud and exploitation.

Not ensuring that [redacted] to the information system increases the risk of a [redacted] inappropriately retaining [redacted], potentially compromising the security of the system.

We recommend DOI ensure:

10. BIA formally document and implement a process for the review of [redacted] and retain the results of the review; and enhance the account management process to ensure that all network [redacted], are appropriately [redacted] after 90 days or at the time of user [redacted]
11. USGS identify, document, and implement a solution to [redacted] before connecting to the network.

    Define and implement processes to ensure that the [redacted] is enabled for at least 85% of [redacted]

    USGS and [redacted] should enhance existing procedures to ensure that [redacted] are reviewed at least annually.

4. Implementation of the Information Security Continuous Monitoring Program

KPMG noted the following weaknesses at four of 12 bureaus and offices, OS, IBC, BSEE, and NPS information security continuous monitoring program:

Office of the Secretary and the Interior Business Center:

KPMG inquired of the Division Chief, Information Assurance Policy, Security Architecture, Security Training and Risk Management (IAPATRM) Office of the Chief Information Officer (OCIO), the Chief Information Systems Security Section, Information Security Program Integration Branch, IAPATRM, Office of Chief Information Officer (OCIO) and others and inspected the Office of the Secretary and Interior Business Center Continuous Monitoring Plan, dated April 25, 2016. We noted the following control deficiencies:

OS and OCIO have not formally defined how Information Security Continuous Monitoring (ISCM) activities will formally integrate with organizational risk tolerance, the threat environment, business requirements, and not formally defined how ISCM information will be shared with individuals with significant security responsibilities and used to make risk-based decisions. Department of the Interior (DOI) quarterly risk management briefings provided to Authorizing Officials discuss continuous monitoring tools that are being used, but do not consistently provide documented information on results of continuous monitoring or the evolving threat environment.

OS and OCIO have not identified and defined the qualitative and quantitative performance measures that will be used to assess the effectiveness of its ISCM program and control ongoing risk, and not defined its processes for collecting and considering lessons learned to improve ISCM processes.

The [redacted] used for hardware asset management is not consistently implemented across the [redacted] Specifically, 39 of 69 judgmentally selected [redacted] assets were not managed by the [redacted] tool.

OS and OCIO has not defined how it will use automation to produce an accurate point-in-time inventory of the authorized and unauthorized software on its network and the security configuration of its software.

BSEE:

KPMG inquired of BSEE personnel responsible for managing the Bureau information security continuous monitoring program, including the Chief Information Security Officer and the Information Assurance Manager, and reviewed the BSEE Continuous Monitoring Plan dated July 2015. KPMG noted the following control deficiencies in the BSEE Continuous Monitoring Program:

BSEE has not fully defined and documented how the Information Security Continuous Monitoring (ISCM) activities will integrate with organizational risk tolerance, the threat environment, and business requirements, and not fully defined how ISCM information will be shared with individuals with significant security responsibilities and used to make risk-based decisions.

ISCM processes to implement the continuous monitoring plan have not been fully defined and documented.

BSEE has not fully defined and documented the qualitative and quantitative performance measures that will be used to assess the effectiveness of its ISCM program and control ongoing risk, and not defined processes for collecting and considering lessons learned to improve ISCM processes.

NPS:

KPMG inquired of NPS personnel responsible managing the NPS continuous monitoring program, including, Deputy Chief Information Security Officer and the Information System Security Officer for the Accounting Operations Center General Support System (AOCGSS) and reviewed the NPS Continuous Monitoring Program Plan, dated April 20, 2016. KPMG noted the following control deficiencies in the NPS information system continuous monitoring program:

[redacted] tool used for hardware asset management is not consistently implemented across the [redacted]. KPMG performed a network service [redacted] to detect the services running on the [redacted]. The [redacted], was not active on 5 of 38 AOC GSS servers. Upon further investigation, NPS discovered that three were virtual servers on the same hardware server; therefore, two instances of [redacted] were not running.

NPS has not fully defined and documented the specific processes and procedures for integrating Information Security Continuous Monitoring (ISCM) activities with NPS risk tolerance, the threat environment, and business requirements, and not fully defined and documented how ISCM information will be shared with individuals with significant security responsibilities and used to make risk-based decisions.

ISCM processes and specific procedures to implement the continuous monitoring plan have not been fully defined and documented, such as collecting security related information required for metrics, assessments, and reporting, procedures for analyzing ISCM data, reporting findings, and determining the appropriate risk responses.

NPS has not fully defined and documented the qualitative and quantitative performance measure that will be used to assess the effectiveness of its ISCM program and control ongoing risk, and not defined processes for collecting and considering lessons learned to improve ISCM processes.

NPS has not defined how it will use automation to produce an accurate [redacted] network and the security configuration of its software.

[redacted] application with the add-on [redacted] software capability, which is part of the [redacted] initiative, is due for deployment by the Department and will provide an authorized software capability. NPS has not defined how it will use the tools to produce an accurate [redacted] on its network and the [redacted].

The Department of the Interior (DOI) Chief Information Officer (CIO) "Memo Re Ongoing A-A Through Continuous Monitoring", dated March 16, 2012 states:

"Bureaus and Offices are now required to conduct ongoing system authorizations based upon continuous monitoring that assess security controls and analyze organizational risks with a frequency sufficient to support risk-based security decisions to adequately protect organization information, New systems are still required to have all applicable security controls fully assessed prior to Authorizing Official (AO) granting an initial Authorization to Operate (ATO).

The AOs are required to:

- Conduct continuous monitoring of their respective information systems and shall utilize, to the extent practicable, common shared enterprise-wide capabilities to help achieve standardization, cost-efficiencies, and overall program effectiveness of controls across the agency;

- Monitor the security state of their 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 purview; and
- Develop, document and formally approve a continuous monitoring program for their information systems."

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 revision 4, dated April 2013 with updates as of January 22, 2015, Security Assessment and Authorization control family states:

CA-7 CONTINUOUS MONITORING

Control: The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes:

a. Establishment of [*Assignment: organization-defined metrics*] to be monitored;

b. Establishment of [*Assignment: organization-defined freq*uencies] for monitoring and [*Assignment: organization-defined freq*uencies] for assessments supporting such monitoring;

c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy;

d. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy;

e. Correlation and analysis of security-related information generated by assessments and monitoring;

f. Response actions to address results of the analysis of security-related information; and

g. Reporting the security status of organization and the information system to [*Assignment: organization-defined personnel or roles*] [*Assignment: organization-defined frequency*].

OS and OCIO have not formally defined procedures for how to routinely aggregate and summarize operational ISCM data to an appropriate level for regular reporting to individuals with significant security responsibilities to be used to make risk-based decisions.

OS and OCIO management informed KPMG that OMB and Department of Homeland Security (DHS) emphasis on new ISCM processes, tools and reporting have evolved and OS and OCIO organizations have been in an reactionary implementation mode. Making it difficult to develop meaningful performance measures.

OS and OCIO have recently implemented [redacted] tool in their environment and are in the process of fully configuring and deploying the tool for [redacted].

In addition, OS and OCIO have not developed, documented, and implemented procedures for ensuring that a complete and accurate [redacted] is maintained.

DOI is deploying the [redacted] capability for [redacted]. This capability will [redacted] to servers and workstations. Additionally, the [redacted] capability, which is part of the DHS CDM initiative, is being deployed and will provide a [redacted] while prohibiting [redacted]. A DOI-wide governance process is being developed to manage the [redacted] that would be implemented by the [redacted] capability.

BSEE has not established a complete ISCM plan due to incomplete implementation procedures.

Without knowledge of ISCM activities, risk-based decisions made by individuals with significant security responsibilities could be less effective.
Without the qualitative and quantitative performance measures, and processes for collecting and considering lessons learned, individuals with significant security responsibilities might have difficulty in assessing the effectiveness of the ISCM program in controlling ongoing risk, and assessing whether there is a need to modify ISCM processes.

NPS has recently implemented [redacted] tool in its environment to all systems. [redacted] tool was properly installed on the system but [redacted] application engaged its tamper protection and prevented [redacted] process from starting and running. Management is investigating further.

NPS has established an ISCM plan; however, it has not documented implementation procedures, because of the need to respond to evolving ISCM requirements from the Office of Management and Budget and the Department.

NPS management is waiting for the implementation of the [redacted]. Various aspects of this task order will allow the NPS to:

- [redacted] and have the ability to display them via a dashboard.
- Allow for [redacted] management approval and denial (via [redacted])
- Provide automation to assist [redacted] management capabilities.

We recommend the DOI ensure:

12. OS and OCIO define and document how ISCM activities that will integrate with organizational risk tolerance, the threat environment, business requirements, and shared with individuals with significant security responsibilities and used to make risk-based decisions.

    Identify, define and document the qualitative and quantitative performance measures that will be used to assess the effectiveness of its ISCM program and control ongoing risk, and define and document processes for collecting and considering lessons learned to improve ISCM processes and disseminate to its Bureaus and Offices.

    Define and document how it will use automation to produce an accurate [redacted] of the [redacted] on its network and the [redacted] of its software.

13. BSEE and NPS fully define and document procedures to integrate ISCM activities with risk tolerance, the threat environment, and business requirements.

    Document procedures to routinely aggregate and summarize operational ISCM data to appropriate levels for regular reporting to individuals with significant responsibilities.

    Document qualitative and quantitative performance measures to assess the effectiveness of bureau ISCM program and process for collecting lessons learned to improve ISCM processes.

14. NPS validate proper implementation of [redacted] on all servers on the [redacted].

5. Implementation of the Incident Response Program

KPMG noted the following weaknesses in the OCIO incident response program. Similar control weaknesses were identified during the fiscal year 2015 FISMA audit.

We inquired of the DOI Enterprise Incident Response Manager, Section Chief and others and inspected DOI's Computer Security Incident Response Team Handbook, dated January 4, 2014 and the Cybersecurity Operations Business Plan Budget Year 2017, dated January 30, 2015.

More specifically DOI has not:

1. Formally approved its incident response policies and procedures. KPMG was informed that DOI senior management is in the process of reviewing and approving updated incident response policies and procedures, in which DOI considered the most recent United States Computer Emergency Readiness Team (US-CERT) reporting requirements and NIST Special Publication 800-61 revision 2.
2. Identified and defined qualitative and quantitative performance measures to be used to perform trend analysis and assess the effectiveness of its incident response program.
3. Fully implemented an enterprise [redacted] tool to aid in the collection and analysis of incident information response; however, an enterprise [redacted] is planned for future implementation as part of the Department of Homeland Security Continuous Diagnostics and Monitoring initiative.
4. Defined how it plans to utilize technology to develop and maintain a [redacted] for users and systems.

NIST Special Publication 800-61 Revision 2, Computer Security Incident Handling Guide, August 2012 states:

- Section 3.1.1 Preparing to Handle Incidents
  - Incident Analysis Resources: Current baselines of expected network, system, and application activity
- Section 3.2.3 Sources of Precursors and Indicators
  - Security Information and Event Management (SIEM) products are similar to IDPS products, but they generate alerts based on analysis of log data.
  - A network flow is a particular communication session occurring between hosts. Routers and other networking devices can provide network flow information, which can be used to find anomalous network activity caused by malware, data exfiltration, and other malicious acts. There are many standards for flow data formats, including NetFlow, sFlow, and IPFIX.
- Section 3.4.1 Lessons Learned
  - One of the most important parts of incident response is also the most often omitted: learning and improving.
- Section 3.4.2 Using Collected Incident Data
  - Lessons learned activities should produce a set of objective and subjective data regarding each incident
  - Another good use of the data is measuring the success of the incident response team. If incident data is collected and stored properly, it should provide several measures of the success (or at least the activities) of the incident response team.
  - Possible metrics for incident-related data include:
    - Number of Incidents Handled.
    - Time Per Incident
    - Objective Assessment of Each Incident.
    - Subjective Assessment of Each Incident.
  - Besides using these metrics to measure the team's success, organizations may also find it useful to periodically audit their incident response programs.

NIST SP 800-53 Rev. 4 April 2013, IR-1 Incident Response Policy and Procedures states:

Control: The organization:

a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:

1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and

b. Reviews and updates the current:

1. Incident response policy [Assignment: organization-defined frequency]; and

2. Incident response procedures [Assignment: organization-defined frequency].

Department of the Interior (DOI) Security Control Standard Incident Response Version: 1.2, December 2012 states: IR-1 Incident Response Policies and Procedures

Applicability: Bureaus and Offices

Control: The organization develops, disseminates, and reviews/updates at least annually:

a. A formal, documented incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.

NIST SP 800-53 Rev. 4 April 2013, IR-5 Incident Monitoring states:

Control: The organization tracks and documents information system security incidents.

Control Enhancements:

(1) Incident Monitoring / Automated Tracking / Data Collection / Analysis

The organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.

IR-8 Incident Response Plan states:

Control: The organization:

a. Develops an incident response plan that:

6. Provides metrics for measuring the incident response capability within the organization;

7. Defines the resources and management support needed to effectively maintain and mature an incident response capability;

8. Is reviewed and approved by all relevant parties;

b. Distributes copies of the incident response plan to all relevant parties and organizational elements;

c. Reviews the incident response plan at least annually;

d. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing;

e. Communicates incident response plan changes to all relevant parties and organizational elements.

NIST AC-4 Information Flow Enforcement states:

Control: The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on applicable policy.

1. DOI management has not formally approved Incident Response policy and procedures that incorporates NIST SP 800-61 revision 2 and US-CERT reporting requirements.

2. DOI management has not developed procedures to identify and define qualitative and quantitative performance measures and perform trend analysis to assess the effectiveness of its incident response program.
3. DOI, working in conjunction with the DHS CDM initiative, plans to implement an enterprise [redacted] tool, but has not yet reached the point of implementing a [redacted] and integrating it with other incident detection and response tools.
4. DOI management has not developed a process to determine how technology will be used to develop and maintain a baseline of expected data flows for users and systems.

Inconsistent, less effective reporting, analysis and response to incidents may occur across the organization unless incident response policies and procedures are formally approved and communicated to DOI Bureaus and Offices.

DOI management may not be able to adequately assess the effectiveness, consistency and improvements needed in the Departmental Incident Detection and Response program, unless qualitative and quantitative performance measures and a baseline of expected results are developed and maintained, and information from a variety of incident detection and response tools are integrated with a [redacted]

We recommend DOI:

15. Formally approve and communicate throughout the Department updated incident response policies and procedures.
16. Define qualitative and quantitative performance measures that will be used to assess the effectiveness and maturity of its incident response program.
17. Continue to define and implement technology tools, such as a [redacted] tool that advance incident detection and response capabilities.
18. Define how to utilize technology to develop and maintain a [redacted] traffic for users and systems.

6. Implementation of the Contingency Planning Program

KPMG noted the following weaknesses at 5 of 13 bureaus and offices, BLM, FWS, OSM, OST, and USGS contingency planning programs. Similar control weaknesses were identified during the fiscal year 2015 FISMA audit.

BLM

BLM did not perform a contingency plan test or exercise in fiscal year 2016. However, management considered an actual event that occurred during the year, but did not document the results and corrective actions were not updated within the [redacted] contingency plan.

FWS

KPMG noted the following control deficiencies with the Business Continuity Plan (BCP) and the FWS Continuity of Operations Plan (COOP):

- FWS has not been able to successfully facilitate a Business Process Analysis (BPA) for the Bureau's Business Continuity Plan (BCP) that includes network infrastructure reconstruction. The BCP [redacted] in parallel with the FWS COOP Plan.

- The FWS COOP has not been formally reviewed and updated since 2013 to consider components such as operating location changes and changes in organizational management.

OSM and OST

The [redacted] and [redacted] contingency plans have not been tested in FY15 or FY16 to help ensure the recoverability and continuity of functions, operations, and resources.

USGS

KPMG determined that [redacted] Contingency Plan was last updated on November 19, 2014. The contingency plan does not accurately reflect the current operating environment such as out-of-date architectural diagrams and a lack of documented procedures for the [redacted] back-up solution.

DOI Security Control Standard Planning, version 1.3, dated December 2012, CP-2 Contingency Planning, states: Control: The organization:

d. Reviews the contingency plan for the information system *at least annually*;

e. Revises the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing

DOI Security Control Standard Contingency Planning, Version 1.3, CP-4 Contingency Plan Testing and Exercises, states:

Control: The organization:

A) Tests and/or exercises the contingency plan for the information system at least annually using functional exercise for moderate impact systems; classroom exercise/table top written tests for low impact systems to determine the plan's effectiveness and the organization's readiness to execute the plan; and

B) Reviews the contingency plan test/exercise results and initiates corrective action.

S.2521 - Federal Information Security Modernization Act of 2014(Page 128 STAT. 3081) states:

> Plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

Federal Continuity Directive 1 (FCD-1), dated October 2012, states:

> "Requirements for Continuity Plans and Procedures:
>
> 1. Organizations must develop and document a continuity plan and its supporting procedures so that, when implemented, the plan and procedures provide for the continued performance of an organization's essential functions under all circumstances and provide for integration with other Government and non-government organizations, as appropriate.
>
> 2. The Organization Head, such as the Secretary, Director, or Administrator, or a designee, must approve and sign the continuity plan, to include significant updates or addendums.
>
> 3. Organizations must annually review their continuity plan and update, if changes occur, and document the date of the review and the names of personnel conducting the review…"

National Institute of Standards and Technology 800-34, "Contingency Planning Guide for Federal Information Systems (NIST 800-34), dated November 2010, states:

> "Section 3 describes the process to develop and maintain an effective information system contingency plan. The process presented is common to all information systems. The seven steps in the process are:
>
> 1. Develop the contingency planning policy
> 2. Conduct the Business Impact Analysis (BIA)
>
> > *The BIA is a key step in implementing the Contingency Plan (CP) controls in NIST SP 800-53 and in the contingency planning process overall. The BIA enables the ISCP Coordinator to characterize the system components, supported mission/business processes, and interdependencies. The BIA purpose is to correlate the system with the critical mission/business processes and services provided, and based on that information, characterize the consequences of a disruption.*
>
> 3. Identify preventive controls
> 4. Create contingency strategies
> 5. Develop an information system contingency plan
> 6. Ensure plan testing, training, and exercises
> 7. Ensure plan maintenance

BLM management has not placed attention on updating the [redacted] Contingency Plan based on corrective action needed based on an actual event. Recent reorganizations and a lack of identified and properly trained resources are contributing factors.

The Business Continuity Process (BCP), which includes a Business Process Analysis (BPA), has not been developed in parallel with the FWS Continuity of Operations Plan (COOP). The FWS COOP Plan has not been updated since 2013 because until May 2016, FWS did not have a Bureau Emergency

Coordinator to facilitate the incorporation of business risks, conduct a review of and make updates to the COOP.
KPMG was informed that due to changes in leadership, OSM has experienced challenges in having the ability to test the [redacted] Contingency Plan.

OST is in the process of moving their alternate site from [redacted]. The process to set up this alternate site has been delayed therefore; OST has lacked a designated contingency site to perform testing.

The USGS [redacted] contingency planning documentation has not been consistently reviewed and updated to reflect the current operating environment.

Without updating the BLM network operations center contingency plan based on corrective actions, lessons learned for an event are not carried forward for use in future events. As a result, in the event of a disaster, the network operations center contingency plan may not be adequate to continue essential BLM activities. Failure to adequately train staff in their Contingency Plan roles and responsibilities increases the risk of system recovery delays due to poor coordination or understanding of responsibilities.

Lack of a business inclusive and up-to-date COOP, and the development of a BCP, hinders FWS from being prepared to continue the operation of essential functions during hazards, emergencies or other situations that may disrupt normal operations.

Without testing the contingency plans deficiencies in the plan may not be identified and addressed. As a result, in the event of an emergency or disaster, the information system contingency plans may not be adequate to continue essential Bureau functions.

We recommend DOI ensure:

19. BLM and USGS update their respectively contingency plans, BLM [redacted] contingency plan and the USGS [redacted] contingency plans in accordance with NIST requirements.
20. FWS review and update the FWS COOP Plan. The COOP should be updated in accordance with [redacted] requirements not addressed by the DOI COOP plan. FWS develop a BCP. The BCP should focus on sustaining an organization's mission business processes during and after a disruption.
21. OSM and OST test their respective contingency plans, [redacted] Contingency Plan and the OST Contingency Plan in accordance with NIST requirements. The test documentation should include methodology, procedures, results, and lessons learned. Where necessary, the OSM and OST contingency plans should be updated based on the results of the contingency plan test.

Conclusion

As part of the FISMA performance audit of the subset of DOI information systems, we assessed the effectiveness of the Department's information security program and practices and the implementation of the security controls in NIST SP 800-53 Revision 4. We identified needed improvements in most areas audited including contractor systems, configuration management, identity and access management, information security continuous monitoring, incident response and contingency planning.

Management Response to Report

Recommendation 1: Ensure OS and OCIO define and document roles, responsibilities and procedures for government oversight, monitoring and reporting of contractor provided systems and services to ensure contractors are performing, monitoring and reporting required security controls in accordance with contractual requirements.

OCIO Management Response: Concur. OS/OCIO will define and document roles, responsibilities and procedures for government oversight, monitoring and reporting of contractor systems and services to ensure contractors are performing, monitoring and reporting required security controls in accordance with DOI security and contractual requirements.

Recommendation 2: BIA enforce existing processes to ensure IT [redacted] are implemented in accordance with the Department of the Interior, Security Control Standard for [redacted] and develop a solution for the web server source code utilizing [redacted] that would allow the upgrade [redacted].

BIA Management Response: Concur. The identification of missing critical [redacted] on the [redacted] systems relates to [redacted] updates. The Microsoft [redacted] are pushed out [redacted] to all production servers and systems on the Indian Affairs network. Due to our suppression of reboots on production servers, BIA's IT Support Team missed some [redacted]. After receiving the FISMA findings, BIA immediately remediated 11 of 12 of the [redacted]. The remaining server is a test server identified as [redacted] that cannot [redacted]. This server has hardware issues that must be repaired before BIA can install updates; this is now in process. The [redacted] servers communicate with [redacted] and BIA monitors them to keep [redacted] up to date. BIA is reviewing its [redacted] and will update the [redacted] to remediate any gaps. BIA is currently testing and verifying the effects of disabling [redacted] servers.

Recommendation 3:_BLM complete the implementation of the [redacted] that will allow BLM to effectively [redacted] connected to the network.

BLM Management Response: Concur and implemented. BLM completed the deployment [redacted] and tested that it effectively removed the problem the previous [redacted] caused in updating [redacted] The previous [redacted], made updating [redacted] problematic.

Recommendation 4: BOR test and deploy the latest appropriate [redacted] and ensure approved configuration baselines are applied.

BOR Management Response: Concur. Remediation actions under Plan of Actions and Milestones (POA&M) Number 32329 include: Install, configure and test database [redacted], application server [redacted] upgrade, and implement vulnerability scanning using [redacted].

Recommendation 5: BSEE implement a follow up process to address those systems that fail initial [redacted] to ensure all devices are [redacted] in a timely manner. Systems that require extensive testing prior to patching that could affect the due dates for [redacted] should be identified and addressed appropriately by management.

BSEE Management Response: Concur. To resolve this finding, BSEE will institute processes and procedures to address [redacted] that occasionally fail, as well as [redacted] systems residing on [redacted]

Recommendation 6: FWS enhance oversight and compliance to ensure all relevant and appropriate [redacted] in order to effectively implement [redacted] as required. Ifrequired remediation timelines cannot be adhered to, consistently document the business rationale or technical issue delaying vulnerability remediation.

FWS Management Response: Concur. The FWS concurs with the finding, which is also repeated under FWS-NFR-01. The FWS replaced the [redacted] systems cited in the [redacted] of FWS-NFR-01 with new servers as of September 22, 2016. FWS last updated the *Enterprise Patch Management Process* document on December 16, 2015. FWS is updating this document to include the more recent procedures. The FWS has opened POA&M # 32369 for the [redacted] oundary.

Recommendation 7: NPS augment the existing testing and [redacted] to ensure effective coordination efforts between separate entities occur, allowing [redacted] to be remediated timely in accordance with the Department of the Interior, Security Control Standard for [redacted].

NPS Management Response: Concur. The NPS Office oflnformation Resources (OIR) and the Accounting Operating Center (AOC) has taken immediate actions to improve its [redacted] processes and is in the process of implementing enterprise solutions (DHS/DOI CDM) to automate control of its information technology asset [redacted] and to address [redacted] findings. In FY 2016, OIR began [redacted] all of the NPS's [redacted] workstations utilizing a third party [redacted] management program.

Currently most NPS offices and regions are still responsible for [redacted]. We are in the process of implementing centralized [redacted] for all NPS servers.

Recommendation 8: OIG ensure [redacted] in accordance with the Department of the Interior, Security Control Standard for [redacted]; and maintain POA&Ms for [redacted] requiring additional time for implementation.

OIG Management Response: Concur. OIG created POA&M 32366 to track weakness remediation. Once OIG evaluates CDM tools, OIG will implement a more robust remediation process for Critical and High vulnerabilities. OIG updated [redacted] process with the following improvements:

- Increased scanners from one to four scanners by region;
- Scans now scheduled to run multiple times through the day versus once a week;
- Local administrators now assist in remediation;
- Tenable agents now deployed to all systems;
- Decommissioned two blades [redacted]
- Pushed [redacted] now require user restart.

OIG is evaluating CDM tools for patching.

Recommendation 9: USGS ensure the proper authentication is used in performing credentialed vulnerability scanning on all moderate and high-impact networked devices within [redacted] Augment the existing testing and [redacted] to ensure effective coordination efforts between the [redacted] occur, allowing [redacted] to be implemented timely in accordance with the Department of the Interior, Security Control Standard for [redacted]. Obtain approval from the DOI OCIO to continue the use of [redacted] Ensure that [redacted] management enhance the Configuration Management Standard Operating Procedures to include a

post-implementation process review of [redacted] to ensure successful implementation of [redacted] settings.

USGS Management Response: Concur. [redacted] staff will work with [redacted] to ensure that proper authentication is used in performing credentialed vulnerability scanning on all moderate and high-impact networked devices, USGS is undertaking improvements to ensure that effective coordination efforts support timely [redacted] staff will review [redacted] protocol usage to either disable or restrict the use of these protocols on networked devices or obtain approval from the DOI OCIO to continue use. [redacted] staff will develop and implement [redacted] processes in accordance with organization policy or standards to ensure timely and secure installation of [redacted], with emphasis on areas identified in the assessment [redacted] management will enhance the Configuration Management Standard Operating Procedures to include a post- implementation process review of [redacted] to ensure successful implementation of [redacted] settings.

Recommendation 10: BIA formally document and implement a process for the review of [redacted]; and retain the results of the review; and enhance the account management process to ensure that all network [redacted], are appropriately disabled after 90 days or at the time of user [redacted]

BIA Management Response: Concur and Implemented . This finding was addressed during the remediation of a previous audit finding from 2015 (OIG FISMA FY2015-ITA-072, Recommendation 27) which was closed on January 18, 2017. Specifically, BIA developed a Standard Operating Procedure that outlined the manual process that currently exists withi n Indian Affairs. The process includes comparing a current list of [redacted] to a current listing of [redacted] in BIA's Identity Information System and taking appropriate action to remedy issues as necessary .

The performance of this control is at least monthly and evidence of the review is to be maintained indefinitely.

Recommendation 11: USGS identify, document, and implement a solution to [redacted] before connecting to the network. Define and implement processes to ensure that the [redacted] is enabled for at least 85% of [redacted] USGS and [redacted] should enhance existing procedures to ensure that [redacted] are reviewed at least annually.

USGS Management Response: Concur. USGS enterprise support webpages provide security recommendations for all USGS to implement compensating controls. USGS will investigate the full implementation leveraging other infrastructure and security programs such as the [redacted] program. For example, [redacted] tool on the roadmap scheduled for FY 2020, may contribute to hardware authorization and access controls. USGS will define and implement processes to achieve 85% [redacted] enabled [redacted] authentication by FY 2018. Further, USGS will update its account recertification procedures to ensure that [redacted] are reviewed at least annually by FY 2018.

Recommendation 12a: OS and OCIO define and document how ISCM activities will integrate with organizational risk tolerance, the threat environment, business requirements, and shared with individuals with significant security responsibilities and used to make risk-based decisions.

OCIO Management Response: Concur. OS/OCIO will define and document how ISCM activities will integrate with organizational risk tolerance, the threat environment, business requirements and share relevant information with individuals with significant security responsibilities to make risk-based decisions. The time table is dependent on [redacted], funding and hiring people for this cybersecurity program.

Recommendation 12b: Identify, define and document the qualitative and quantitative performance measures that will be used to assess the effectiveness of its ISCM program and control ongoing risk, and define and document processes for collecting and considering lessons learned to improve ISCM processes and disseminate to its bureaus and offices.

OCIO Management Response: Concur. OCIO will identify, define and document the qualitative and quantitative performance measures to assess the effectiveness of the ISCM program and control ongoing risk, and define and document processes for collecting and considering lessons learned to improve ISCM process and in collaboration with bureaus and offices. The time table is dependent on [redacted] direction, as well as funding and hiring staff to support [redacted] program.

Recommendation 12c: Define and document how it will use automation to produce an accurate [redacted] of the [redacted] on its network and the security configuration of its software.

OCIO Management Response: Partially Concur. DOI will define and document how it will automate and produce an accurate point-in-time inventory of the [redacted] on its networks upon full implementation of [redacted] DOI does not plan to automate [redacted] nor is it on the [redacted]; however, DOI is deploying automated operating system security configuration using IBM [redacted]

Recommendation 13: BSEE and NPS fully define and document procedures to integrate ISCM activities with risk tolerance, the threat environment, and business requirements. Document procedures to routinely aggregate and summarize operational ISCM data to appropriate levels for regular reporting to individuals with significant responsibilities. Document qualitative and quantitative performance measures to assess the effectiveness of bureau ISCM program and process for collecting lessons learned to improve ISCM processes.

BSEE Management Response: Concur. The 2015 BSEE Information System Continuous Monitoring Plan is being updated to include the following:

- List of individuals with significant security responsibilities.
- List of ISCM information, the frequency of collection and of reporting to a dashboard of key metrics which will be used to inform risk decision makers of security posture.
- Qualitative and quantitative performance measures that will be used to assess the effectiveness of the [redacted] ISCMP, achieve situational awareness and control ongoing risk.
- Perform root cause analysis for vulnerabilities and review past accepted risks to improve ISCM processes.

NPS Management Response: Concur. The NPS has taken significant steps to strengthen the ISCM. Last year the NPS's ISCM program was operating at a defined level, with the NPS performing several, but not all, recommended activities indicative of higher maturity levels. This year, the NPS will take several steps to improve the effectiveness of its ISCM program. The FY 2017 update for the NPS ICSM will include these elements addressed in this finding.

Recommendation 14: NPS validate proper implementation of [redacted] on all servers on the [redacted].

NPS Management Response: Concurred and implemented. The audit report states the following: *The [redacted] tool usedfor hardware asset management is not consistently implemented across the [redacted]. KPMG performed a network service scan of the AOC GSS using a Nessus scanner to detect the services running on the [redacted]. The [redacted] detected that [redacted] which is the [redacted], was not active on 5 of 38 [redacted] servers. Uponfurther investigation, NPS discovered that three were virtual servers on the same hardware server; therefore, two instances of the [redacted] were not running.* The NPS has resolved the issue [redacted] from running.

Recommendation 15: Formally approve and communicate throughout the Department updated incident response policies and procedures.

OCIO Management Response: Concur. DOI will formally approve and communicate the updated DOI Incident Response Procedures across the Department. DOI Incident Response Policy was formally released in November 2016 with the release of the updated DOI IT Security Control Standards.

Recommendation 16: Define qualitative and quantitative performance measures that will be used to assess the effectiveness and maturity of its incident response program.

OCIO Management Response: Concur. In response to the finding, DOI has integrated incident response (IR) test exercises into our program. DOI Computer Incident Response Center (CIRC) staff will be regularly tested on various aspects of Incident Handling including, who to escalate certain incidents to, which teams to get involved, when an incident must be reported to US- CERT, etc. It will take several years to mature the program to the level required due to the number of interdependencies. The time table is dependent on [redacted] direction, as well as funding and hiring staff to support [redacted] program.

Recommendation 17: Continue to define and implement technology tools, such as a [redacted] and a [redacted] tool that advance incident detection and response capabilities.

OCIO Management Response: Partially Concur. OCIO does not have sufficient funding to provide, operate, and maintain an [redacted] capability. OCIO has a small [redacted] instance that was developed specifically to support a few of the DOI Shared Service customers, and we are in the process of minimally enhancing the capacity in FY 2017. Our long term plan is to await [redacted] which was expected to begin FY18. OCIO does not have an [redacted] integrity tool or capability to alert us [redacted] alterations of important data and [redacted], nor do we have plans to do so in the near future. The time table is dependent on [redacted] direction, as well as funding and hiring staff to support [redacted] program.

Recommendation 18: Define how to utilize technology to develop and maintain a [redacted] for users and systems.

OCIO Management Response: Concur. The OCIO Incident Response Program (IRP) will define a process describing how to utilize technology to develop and maintain a [redacted] network data traffic for users and systems. Supporting the IRP, the OCIO's Enterprise Infrastructure Services Section, will continue to provide access to a variety of network tools and systems to assist in tracking and responding to alarms and alerts, providing historical network traffic baselines and patterns, and identifying network traffic anomalies, to name a few.

Recommendation 19: BLM and USGS update their respectively contingency plans, BLM [redacted] contingency plan and the USGS [redacted] contingency plans in accordance with NIST requirements.

BLM Management Response: Concur. BLM established POAM ID 29736, which calls for update and testing of the [redacted] IT contingency plan. Further we will take a look at the process identified by the auditors and measure where BLM stands in the IT contingency planning process.

USGS Management Response: Concur and implemented. USGS has updated contingency planning documentation to reflect the current operating system environment. USGS has also addressed [redacted] to ensure that lessons learned, such as the need for redundancy or backup virtual disk images from the fiscal year 2016 contingency plan test are incorporated into the system contingency plan. These actions were completed January 26, 2017. Correction to report page 106 CP 5.1.3 sentences two and three should be removed as they were resolved as false positives during a factual accuracy review with the auditor.

Recommendation 20: FWS review and update the FWS COOP Plan. The COOP should be updated in accordance with [redacted] requirements not addressed by the DOI COOP plan. FWS develop a BCP. The BCP should focus on sustaining an organization's mission business processes during and after a disruption.

FWS Management Response: Concur. The FWS will conduct a Business Impact Analysis to correlate the system with the critical mission/business processes and services provided , and based on that information, characterize the consequences of a disruption, in accordance with NIST 800-34, "Contingency Planning Guide for Federal Information Systems." FWS [redacted] will coordinate with the appropriate offices to ensure that the bureau Business Impact Analysis includes input from mission/business stakeholders to identify business processes, potential impacts, maximum tolerable downtime and recovery point objectives. The COOP (Continuity of Operations) plan falls under the purview of the Chief of Emergency Management & Physical Security. [redacted] will coordinate with the bureau Emergency Coordinator in the Emergency Management & Physical Security office to update the COOP at least annually. The FWS currently has an open POA&M # 30522 in the FWS Program for this action.

Recommendation 21: OSM and OST test their respective contingency plans, [redacted] Contingency Plan and the OST Contingency Plan in accordance with NIST requirements. The test documentation should include methodology, procedures, results, and lessons learned. Where necessary, the OSM and OST contingency plans should be updated based on the results of the contingency plan test.

OSM Management Response: Concur. OSMRE will conduct Contingency Plan Testing in accordance with NIST 800-53A Rev 4 for those controls in the Contingency Plan family for our [redacted] The test documentation will include methodology, procedures, results, and lessons learned. The Contingency Plan will be updated, if necessary, based on the results of the Contingency Plan Test.

OST Management Response: Concur. OST has changed its datacenter site and the disaster recovery (DR) Capability/Contingency plan for [redacted] which lacks the capability to respond effectively to the complete loss of the new primary datacenter. Due to datacenter consolidation, the OST datacenter has been moved to the BIA [redacted]. OST is working with BIA to establish a [redacted] to support Infrastructure as a Service/Disaster Recovery Capability in line with OCIO efforts to optimize data center utilization within the Department.

Additionally, OST has obtained funding to re-architect its existing compute and storage services to provide data replication capability to offsite facilities should BIA be unable to meet the requirements.

Appendix I – Summary of FISMA Program Areas

The following table summarizes the Cybersecurity Framework Security Function area in which control deficiencies were identified. It should not be used to infer program area compliance in general, and does not correlate to the overall program area assessments provided in Appendix V or responses provided for the FY2016 CyberScope Responses.

The Identify function consists of risk management and contractor system program areas. The Protect function consists of configuration management, identity and access management, and security and privacy training program areas. The Detect function consists of the information security continuous monitoring program area. The Respond function consists of incident response and the Recover function consists of the contingency planning program areas.

Functions	BIA	BLM	BOR	BSEE	FWS	NPS	OCIO	OIG	OS	OSMRE	OST	USGS
Identify							**X**					
Protect	**X**	**X**	**X**	**X**	**X**	**X**		**X**				**X**
Detect				**X**		**X**	**X**					
Respond							**X**					
Recover		**X**			**X**					**X**	**X**	**X**

Legend:
X – Weakness identified in FISMA Program Area

This table lists the FISMA reporting metric attributes that a bureau/office has a control deficiency.

Bureau	Program Area[13]	Recommendation #	Deficiencies identified in FY 2016 FISMA Reporting Metric Attribute	
BIA	CM	2	2.1.8	Remediates configuration-related vulnerabilities, including scan findings, in a timely manner as specified in organization policy or standards. (NIST 800-53: CM-4, CM-6, RA-5, SI-2)
		2	2.1.9	Develops and implements a patch management process in accordance with organization policy or standards, including timely and secure installation of software patches. (NIST SP 800-53: CM-3, SI-2, OMB M-16-04, DHS Binding Operational Directive 15-01)
	IAM	10	2.2.6	Enforces PIV or a NIST LOA 4 credential for logical access for at least 85% of non-privileged users. (Cybersecurity Sprint, OMB M-16-04, PMC, 2016 CIO FISMA Metrics 2.4.1)
		10	2.2.8	Ensures that accounts are terminated or deactivated once access is no longer required or after a period of inactivity, according to organizational policy
BLM	CM	3	2.1.8	Remediates configuration-related vulnerabilities, including scan findings, in a timely manner as specified in organization policy or standards. (NIST 800-53: CM-4, CM-6, RA-5, SI-2)
	CM	3	2.1.9	Develops and implements a patch management process in accordance with organization policy or standards, including timely and secure installation of software patches. (NIST SP 800-53: CM-3, SI-2, OMB M-16-04, DHS Binding Operational Directive 15-01)
	CP	19	5.1.6	Tests system-specific contingency plans, in accordance with organizationally defined timeframes, to determine the effectiveness of the plans as well as readiness to execute the plans if necessary. (NIST SP 800-53: CP-4)
BOR	CM	4	2.1.8	Remediates configuration-related vulnerabilities, including scan findings, in a timely manner as specified in organization policy or standards. (NIST 800-53: CM-4, CM-6, RA-5, SI-2)
		4	2.1.9	Develops and implements a patch management process in accordance with organization policy or standards, including timely and secure installation of software patches. (NIST SP 800-53: CM-3, SI-2, OMB M-16-04, DHS Binding Operational Directive 15-01)

[13] Risk Management (RM), Contractor Systems (CS), Configuration Management (CM), Identity and Access Management (IAM), Security Training and Privacy (ST), Information System Continuous Monitoring (ISCM), Incident Response (IR), and Contingency Planning.

BSEE	CM	5	2.1.8	Remediates configuration-related vulnerabilities, including scan findings, in a timely manner as specified in organization policy or standards. (NIST 800-53: CM-4, CM-6, RA-5, SI-2)
	CM	5	2.1.9	Develops and implements a patch management process in accordance with organization policy or standards, including timely and secure installation of software patches. (NIST SP 800-53: CM-3, SI-2, OMB M-16-04, DHS Binding Operational Directive 15-01)
	ISCM	13	3.1.1.3	The organization has not defined how ISCM information will be shared with individuals with significant security responsibilities and used to make risk based decisions.
	ISCM	13	3.1.1.4	The organization has not defined how it will integrate ISCM activities with organizational risk tolerance, the threat environment, and business/mission requirements.
	ISCM	13	3.1.1.7	The organization has not identified and defined the qualitative and quantitative performance measures that will be used to assess the effectiveness of its ISCM program, achieve situational awareness, and control ongoing risk
	ISCM	13	3.1.1.8	The organization has not defined its processes for collecting and considering lessons learned to improve ISCM processes.
FWS	CM	6	2.1.8	Remediates configuration-related vulnerabilities, including scan findings, in a timely manner as specified in organization policy or standards. (NIST 800-53: CM-4, CM-6, RA-5, SI-2)
	CM	6	2.1.9	Develops and implements a patch management process in accordance with organization policy or standards, including timely and secure installation of software patches. (NIST SP 800-53: CM-3, SI-2, OMB M-16-04, DHS Binding Operational Directive 15-01)
	CP	20	5.1.2	Incorporates the system's Business Impact Analysis and Business Process Analysis into analysis and strategy toward development of the organization's Continuity of Operations Plan, Business Continuity Plan (BCP), and Disaster Recovery Plan (DRP). (NIST SP 800-34).
NPS	CM	7	2.1.8	Remediates configuration-related vulnerabilities, including scan findings, in a timely manner as specified in organization policy or standards. (NIST 800-53: CM-4, CM-6, RA-5, SI-2)
	CM	7	2.1.9	Develops and implements a patch management process in accordance with organization policy or standards, including timely and secure installation of software patches. (NIST SP 800-53: CM-3, SI-2, OMB M-16-04, DHS Binding Operational Directive 15-01)

	ISCM	13	3.1.1.3	The organization has not defined how ISCM information will be shared with individuals with significant security responsibilities and used to make risk based decisions.
	ISCM	13	3.1.1.4	The organization has not defined how it will integrate ISCM activities with organizational risk tolerance, the threat environment, and business/mission requirements.
	ISCM	13	3.1.1.7	The organization has not identified and defined the qualitative and quantitative performance measures that will be used to assess the effectiveness of its ISCM program, achieve situational awareness, and control ongoing risk
	ISCM	13	3.1.1.8	The organization has not defined its processes for collecting and considering lessons learned to improve ISCM processes.
OIG	CM	8	2.1.8	Remediates configuration-related vulnerabilities, including scan findings, in a timely manner as specified in organization policy or standards. (NIST 800-53: CM-4, CM-6, RA-5, SI-2)
	CM	8	2.1.9	Develops and implements a patch management process in accordance with organization policy or standards, including timely and secure installation of software patches. (NIST SP 800-53: CM-3, SI-2, OMB M-16-04, DHS Binding Operational Directive 15-01)
OS	CS	1	1.2.3	Obtains sufficient assurance that the security controls of systems operated on the organization's behalf by contractors or other entities and services provided on the organization's behalf meet FISMA requirements, OMB policy, and applicable NIST guidelines. (NIST SP 800-53: CA-2, SA-9)
	ISCM	12	3.1.1.3	The organization has not defined how ISCM information will be shared with individuals with significant security responsibilities and used to make risk based decisions.
	ISCM	12	3.1.1.4	The organization has not defined how it will integrate ISCM activities with organizational risk tolerance, the threat environment, and business/mission requirements.
	ISCM	12	3.1.1.7	The organization has not identified and defined the qualitative and quantitative performance measures that will be used to assess the effectiveness of its ISCM program, achieve situational awareness, and control ongoing risk.
	ISCM	12	3.1.1.8	The organization has not defined its processes for collecting and considering lessons learned to improve ISCM processes.

	ISCM	12	3.1.1.10	The organization has not defined how it will use automation to produce an accurate point-in-time inventory of the authorized and unauthorized devices and software on its network and the security configuration of these devices and software.
	IR	15	4.1.1.5	Incident response processes have not been fully defined and are performed in an ad-hoc, reactive manner for the following areas: incident response planning, incident response training and testing; incident detection and analysis; incident containment, eradication, and recovery; incident coordination, information sharing, and reporting to internal and external stakeholders using standard data elements and impact classifications within timeframes established by US-CERT.
	IR	16	4.1.1.7	The organization has not identified and defined the qualitative and quantitative performance measures that will be used to assess the effectiveness of its incident response program, perform trend analysis, achieve situational awareness, and control ongoing risk.
	IR	17	4.1.1.9	The organization has not identified and defined the incident response technologies needed in one or more of the following areas and relies on manual/procedural methods in instances where automation would be more effective. Use of incident response technologies in the following areas is ad-hoc. • Web application protections, such as web application firewalls • Event and incident management, such as intrusion detection and prevention tools, and incident tracking and reporting tools • Aggregation and analysis, such as security information and event management (SIEM) products • Malware detection, such as anti-virus and antispam software technologies • 1nformation management, such as data loss prevention • File integrity and endpoint and server security tools
	IR	18	4.1.1.12	The organization has not defined how it plans to utilize technology to develop and maintain a baseline of network operations and expected data flows for users and systems.
	IR	16	4.4.1.1	Incident response stakeholders are consistently implementing, monitoring, and analyzing qualitative and quantitative performance measures across the organization and are collecting, analyzing, and reporting data on the effectiveness of the organization's

				incident response program.
OSM	CP	21	5.1.6	Tests system-specific contingency plans, in accordance with organizationally defined timeframes, to determine the effectiveness of the plans as well as readiness to execute the plans if necessary. (NIST SP 800-53: CP-4)
OST	CP	21	5.1.6	Tests system-specific contingency plans, in accordance with organizationally defined timeframes, to determine the effectiveness of the plans as well as readiness to execute the plans if necessary. (NIST SP 800-53: CP-4)
USGS	CM	9	2.1.8	Remediates configuration-related vulnerabilities, including scan findings, in a timely manner as specified in organization policy or standards. (NIST 800-53: CM-4, CM-6, RA-5, SI-2)
	CM	9	2.1.9	Develops and implements a patch management process in accordance with organization policy or standards, including timely and secure installation of software patches. (NIST SP 800-53: CM-3, SI-2, OMB M-16-04, DHS Binding Operational Directive 15-01)
	IAM	11	2.2.6	Enforces PIV or a NIST LOA 4 credential for logical access for at least 85% of non-privileged users. (Cybersecurity Sprint, OMB M-16-04, PMC, 2016 CIO FISMA Metrics 2.4.1)
	IAM	11	2.2.7	Tracks and controls the use of administrative privileges and ensures that these privileges are periodically reviewed and adjusted in accordance with organizationally defined timeframes. (2016 CIO FISMA Metrics 2.9, 2.10; OMB M-16-04, CIS 5.2)
	CP	19	5.1.3	Develops and maintains documented recovery strategies, plans, and procedures at the division, component, and IT infrastructure levels. (NIST SP 800-34
	CP	19	5.1.7	Develops after-action reports that address issues identified during contingency/disaster recovery exercises in order to improve contingency/disaster recovery processes. (FCD1, NIST SP 800-34)

Appendix II – Listing of Acronyms

Acronym	Definition
A&A	Assessment & Authorizations
AC	Access Control
AO	Authorizing Official
AOC GSS	Accounting Operations Center General Support System
ASOC	Advanced Security Operations Center
ATO	Authority/Authorization to Operate
AU	Audit and Accountability
BCISO	Bureau Chief Information Security Officer
BCP	Business Continuity Plan
BIA	Bureau of Indian Affairs
BLM	Bureau of Land Management
BOR	Bureau of Reclamation
BPA	Business Process Analysis
BSEE	Bureau of Safety and Environmental Enforcement
BUTST	Bureau Unix Technical Support Team
CA	Security Assessment and Authorization
CCB	Change Control Board
CDM	Continuous Diagnostics and Mitigation
CIGIE	Council of the Inspector General for Integrity and Efficiency
CIO	Chief Information Officer
CIRC	Computer Incident Response Center
CISO	Chief Information Security Officer
CM	Configuration Management
CMM	Continuous Monitoring

Acronym	Definition
CONOPS	Concept of Operations
COOP	Continuity of Operations Plan
COUA	Certified Organizational Unit Administrators
CP	Contingency Planning
CS	Contractor System
CSAM	Cyber Security Assessment and Management
CVE	Common Vulnerability and Exposures
CVODSS	Central Valley Operations Decision Support System
DHS	Department of Homeland Security
DOI	United States Department of the Interior
DRP	Disaster Recovery Plan
ECNS	Enterprise Core Network Services
EHI	Enterprise Hosting Environment
ESN	DOI Enterprise Services Network
FCD	Federal Continuity Directive
FCHS	Foundation Cloud Hosting Services
FDCC	Federal Desktop Core Configuration
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
FISSA	Federal Information System Security Awareness
FTP	File Transfer Protocol
FWS	US Fish and Wildlife Service
FY	Fiscal Year
GSS	General Support System
HAR	Historical Archive and Reports
HQ	Headquarters

Acronym	Definition
HSPD	Homeland Security Presidential Directive
IA	Identification and Authentication
IA	Information Assurance
IAM	Identity and Access Management
IAPATRM	Information Assurance Policy, Security Architecture, Security Training and Risk Management
IEM	IBM Endpoint Manager
IG	Inspector General
IP	Internet Protocol
IR	Incident Response
IRTM JAHP	Information Resources and Technology Management Java Application Hosting Platform
ISCM	Information Security Continuous Monitoring
ISSO	Information System Security Officer
IT	Information Technology
ITSOT	Information Technology Security Operations Team
KPMG	KPMG LLP
LAN	Local Area Network
MS	Microsoft
MVM	McAfee Vulnerability Manager
NAC	Network Access Control
NFR	Notice of Findings and Recommendations
NGTOC	National Geospatial Technical Operations Center
NIST	National Institute of Standards and Technology
NMRP	National Map Reengineering Project
NOC	Network Operations Center
NPS	National Park Service

Acronym	Definition
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
ONRR	Office of Natural Resources Revenue
OS	Office of the Secretary
OS	Operating System
OSMRE	Office of Surface Mining Reclamation and Enforcement
OST	Office of the Special Trustee for American Indians
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PL	Planning
PM	Program Management
POA&M	Plan of Action and Milestones
POODLE	Padding Oracle On Downgraded Legacy Encryption
PUB	Publication
PY	Prior Year
RA	Risk Assessment
RBST	Role Based Security Training
REV	Revision
RFQ	Request for Quotation
RM	Risk Management
RMSS	Reclamation Mission Support System
SA	System and Services Acquisition
SAT	Security Assurance Team
SC	System and Communication Protection
SCAP	Security Content Automation Protocol

Acronym	Definition
SCCM	System Center Configuration Manager
SDW	Spatial Data Warehouse
SI	System and Information Integrity
SIEM	Security Information and Event Management
SOL	Office of the Solicitor
SOW	Statement of Work
SP	Special Publication
SQL	Structured Query Language
SSP	System Security Plan
SSL	Secure Sockets Layer
ST	Security and Awareness Training
STIG	Security Technical Implementation Guide
TERPS	Tribal Enrollment and Payment System
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
TIMS	Technical Information Management System
US	United States
US-CERT	United States Computer Emergency Readiness Team
USC	United States Code
USGCB	United States Government Configuration Baseline
USGS	United States Geological Survey
VFC	Virtustream Federal Cloud
VPN	Virtual Private Network
WSUS	Windows Server Update Services

Appendix III – Prior Year Recommendation Status

Appendix III provides the status of FY2015. Below is a summary table of the FY15 FISMA report recommendation and the status as of 9/30/2016.

Table 1. FY2015 FISMA Report Recommendations and Status as of 9/30/2016

FY2015 FISMA Report Recommendation and Status 44 of 59 Recommendations are Open				
ID	**Recommendation**	**OCIO Response as of 9/30/15**	**Status of 9/30/16 (OPEN or CLOSED)**	**Comment**
1	BLM: "Enhance [redacted] management schedules for [redacted] and allocate resources to deploy [redacted] on the timeframe designated by the DOI standards."	Concur. Existing POA&Ms (26564 and 26990) have been updated with the FYI 5 finding notes. The overall vulnerability posture has greatly improved. However, BLM will ensure that [redacted] have been installed and are reporting correctly on all National Applications systems and will review [redacted] procedures to align with DOI standards.	Completed/Closed on 9/19/2016. [BLM-5015].	No comment.
2	BLM: "Finalize the deployment of [redacted] and [redacted] within all BLM networks to provide [redacted] and vulnerability management capabilities."	Concur. The existing POA&Ms (26564 and 26990) have been updated with the FYI 5 finding notes. The overall vulnerability posture has greatly improved. However, BLM will ensure that [redacted] have been installed and are reporting correctly on all National Applications systems and will review [redacted] procedures to align with DOI standards.	Completed/Closed on 9/19/2016. [BLM-5016].	No comment.
3	BLM: "Ensure IT software [redacted] are implemented in accordance with the DOI Risk Assessment and System and Integrity	Concur. The existing POA&Ms (26564 and 26990) have been updated with the FY15 finding notes. The overall vulnerability posture has greatly improved. However, BLM will ensure that [redacted] have	Completed/Closed on 9/19/2016. [BLM-5017].	Although DOI considers this recommendation closed; it is a repeat finding of FY16 FISMA recommendation 3.

	Information security control standards.	been installed and reporting correctly on all National Applications systems and will review [redacted] procedures to align with DOI standards.		
4	BOR: "Enhance the vulnerability management procedures to include a periodic review of the [redacted] settings."	Concur. The BOR Vulnerability Management Procedure has been updated to include a periodic review of the [redacted] configuration settings.	Completed/Closed on 5/19/2016. [BOR-5019].	No comment.
5	BOR: "Ensure IT software [redacted] are deployed timely to the [redacted] management guidance and Department of the Interior, Security Control Standard for RA-5."	Concur. [redacted] are being deployed more timely, partly in response to the [redacted], and according to DOI guidance. BOR has reduced the number of critical vulnerabilities by 80% over the last two months. The average number of vulnerabilities per machine went from 26 to 11. Additionally, all identified [redacted] servers have had the latest [redacted] applied.	OPEN, Target Completion Date: 5/1/2017. [BOR-5020].	See FY16 FISMA recommendation #4.
6	BSEE: "Ensure IT software [redacted] are implemented in accordance with the DOI Risk Assessment and System and Integrity Information security control standards."	Management response: Concur. BSEE will continue to expand their efforts to ensure [redacted] and security advisories are addressed upon dissemination by US-CERT or discovery through vulnerability assessment tools. Numerous improvements to [redacted] process and tools have already been implemented and continue to be fine-tuned to assure compliance with DOI Risk Assessment and System and Integrity Information security control standards. Process enhancements include leveraging pre-approved changes and accelerated testing for operating system [redacted], as well as certain third party applications, to expedite remediation of critical security advisories. [redacted] system	OPEN. Target Completion Date: 12/30/2016. [BSE-5011].	See FY16 FISMA recommendation #5.

		enhancements have improved [redacted] performance through restructuring of deployment packages and modification of [redacted] boundaries. These improvements have already contributed to [redacted] lowering their average number of vulnerabilities on a per system basis. BSEE will also evaluate other [redacted] tools, such as [redacted] as alternatives to further improve patch management within the BSEE environment.		
7	BSEE: "Update and maintain active POA&Ms for items requiring additional time for remediation."	Concur. BSEE will reassess our POA&M update and maintenance process and the roles responsible for monitoring them and define a strategy for items requiring additional time for fixes.	Completed/Closed on 9/8/2016 (FY2016). [BSE-5012].	No comment.
8	BSEE: "Develop a solution for [redacted] support that would allow security fixes to be deployed to majority of the BSEE environment. Possible solutions may include one or more of the following: a. Re-development of [redacted] to support newer versions of [redacted] b. Utilization of sandbox technologies [redacted] etc.). c. c. Alternative [redacted] strategies to cover majority of BSEE environment."	Concur. BSEE will engage with BSEE, BOEM and ONRR representatives to review solution alternatives, which enable deployment of security fixes to the majority of the BSEE environment. BSEE is already demonstrating progress towards this recommendation. An upgrade and re-platforming of the [redacted] was initiated in FY15 and is expected to be complete in FY16. We anticipate these system improvements will reduce the number of longstanding vulnerabilities and better position the Bureau for adhering to a regular [redacted] schedule. A balanced strategy will be devised for remaining legacy systems and application support that meets Mission area needs and protects BSEE's security posture.	Completed/Closed on 9/8/2016 (FY2016). [OCIO Ref #: BSE-5013].	No comment.

9	FWS: "Ensure IT software [redacted] are deployed timely according to [redacted] guidance and Department of the Interior, Security Control Standard for RA-5."	Concur. The FWS created POA&M 29649 in the Enterprise Core Network Services (ECNS) boundary. FWS management will ensure IT [redacted] are deployed timely according to [redacted] guidance and Department of the Interior, Security Control Standard for Risk Assessment RA-5 Vulnerability Scanning.	OPEN, Target Completion Date: 12/31/2017. [FWS-5016].	See FY16 FISMA recommendation #6.
10	FWS: "Augment the [redacted] process with their existing vulnerability scanning tools by analyzing multiple data points to improve detection of missing [redacted], in addition to improving oversight of System Owner remediation efforts."	Concur. The FWS created POA&M 29649 in the Enterprise Core Network Services (ECNS) boundary. FWS management will augment the [redacted] process with their existing vulnerability scanning tools by analyzing multiple data points to improve detection of missing [redacted], in addition to improving oversight of System Owner remediation efforts.	OPEN, Target Completion Date: 12/31/2017. [FWS-5017].	No comment.
11	NPS: "Ensure IT software [redacted] are deployed timely according to [redacted] guidance and Department of the Interior, Security Control Standard for RA-5."	Concur. National Park Service [redacted] has taken immediate action and manually applied [redacted] all servers. A renewed effort is underway to resolve the outstanding issue with receiving [redacted], in accordance with DOI Security Control Standard RA-5.	OPEN, Target Completion Date: 8/31/2019. [NPS-5018].	See FY16 FISMA recommendation #7.
12	NPS: "Update and maintain active Plan of Action and Milestones (POA&Ms) for items requiring additional time for fixes."	Concur. Plan of Action and Milestones (POA&Ms) are under review and will be updated accordingly.	Completed/Closed on 5/19/2016. [NPS-5019].	No comment.
13	NPS: "Test and deploy newer versions of [redacted] to support recently upgraded implementation of [redacted]	Concur. The [redacted] based applications require very specific versions of [redacted] to function correctly. Updates have already been applied [redacted] to address more serious	OPEN, Target Completion Date: 8/31/2019. [NPS-5020].	No comment.

	[redacted] for compatibility."	vulnerabilities. The remaining issues are under investigation by National Park Service's [redacted] support. Newer versions will be applied when compatibility is confirmed by IBM. Other older application versions are also in need of upgrade to address additional vulnerabilities.		
14	OCIO and the Business Integration Office: "Develop and coordinate a [redacted] strategy and process that outlines responsibility of all three groups ([redacted]., OCIO, and BIO Team), coordinates the deployment of software security fixes (Operating System, Database, and Application), and maintains a vulnerability scanning process that provides oversight to the respective groups."	Concur.	Completed/Closed on 4/20/2016. [OIG-0264].	No comment.
15	OCIO and the Business Integration Office: "Ensure IT software [redacted] are deployed timely according to [redacted] guidance and Department of the Interior, Security Control Standard for RA-5."	Concur.	Completed/Closed on 4/20/2016. [OIG-0265].	No comment.
16	OCIO and the Business Integration Office: "Disable or restrict the use of the [redacted] on networked devices.	Concur.	Completed/Closed on 4/20/2016. [OIG-0266].	No comment.

17	OSMRE: "Ensure IT [redacted] are deployed timely according to the [redacted] guidance and Department of the Interior, Security Control Standard for RA-5."	Concur. OSMRE has since created a POA&M and is tracking [redacted] on a weekly basis.	Completed/Closed on 8/4/2016. [OSM-5004].	No comment.
18	OSMRE: "Disable or restrict the use of the [redacted] on networked devices."	Concur. Of the four identified instances of [redacted] discovered the OSMRE has disabled three and restricted the use of the fourth pending a vendor firmware update.	Completed/Closed on 8/4/2016. [OSM-5005].	No comment.
19	OST: "Ensure IT [redacted] are deployed timely according to [redacted] guidance and Department of the Interior, Security Control Standard for RA-5."	Concur. OST will open a POA&M to track corrective actions.	Completed/Closed on 9/8/2016. [OST-5006].	No comment.
20	OST: "Disable or restrict the use of the [redacted] on networked devices."	Concur. OST will open a POA&M to track corrective actions.	Completed/Closed on 7/24/2016. [OST-5007].	No comment.
21	USGS: "Continue corrective actions as described in POA&M 28734, which includes continued vulnerability scanning by the contractor and Management performing remediation activities on items discovered."	Concur. Management concurs with this recommendation as documented in September 2015 USGS response to USGS-NFR-01, W/P Reference USGS- FISMA-VA-04. USGS is tracking corrective actions through POA&M 29474 assigned to Asset 439 Cloud Pilot.	OPEN, Target Completion Date: 11/30/2016. [WGS-5006].	No comment.
22	USGS: "Continue to develop and migrate the [redacted] information system into the new cloud-based environment developed under the	Concur. Management concurs with this recommendation as documented in September 2015 USGS response to USGS-NFR-01. USGS is tracking corrective actions through POA&M 29474 assigned to [redacted] Cloud Pilot.	OPEN, Target Completion Date: 1/2/2017. [WGS-5007].	No comment.

	Foundational Cloud Hosting Services contract."			
23	USGS: "Ensure the vulnerability management program and flaw remediation processes consider cloud-based information systems that are part of the USGS system inventory."	Concur. Management concurs with this recommendation as documented in September 2015 USGS response to USGS-NFR-01. USGS is tracking corrective actions through POA&M 29474 assigned to Asset 439 Cloud Pilot.	OPEN, Target Completion Date: 10/19/2016. [WGS-5008].	No comment.
24	SOL: "Ensure IT [redacted] are deployed timely according to [redacted] guidance and Department of the Interior, Security Control Standard for RA-5."	Concur. SOL is reevaluating current [redacted] technology for ongoing suitability as well as exploring the possible use of [redacted] for ongoing deployments. SOL will create a POA&M for tracking.	OPEN. [SOL-5006].	No comment.
25	SOL: "Create and maintain active Plan of Action and Milestones (POA&Ms) for items requiring additional time for fixes."	Concur. SOL has collaborated with the OCIO Information Assurance Policy, Security Architecture, Security Training and Risk Management (IAPATRM) group for POA&M support. Going forward, this process will be managed in collaboration with the IAPATRM group. SOL will a create POA&M for tracking.	OPEN. [SOL-5007].	No comment.
26	SOL: "SOL management should identify the Linux Cent0S5 and CentOS7 components operating in the SOL network environment, develop, document, and implement an agreed-upon set of baseline configurations."	Concur. SOL utilizes security appliances based on the [redacted]. SOL is in the process of documenting the baseline configuration for these devices. SOL will create a POA&M for tracking.	OPEN. [SOL-5008].	No comment.
27	BIA: "Develop and implement a process for the periodic review of AD database administrator access	Concur. The implementation of [redacted] will facilitate the completion of this recommendation.	OPEN. [BIA-5018].	See FY16 FISMA recommendation #10.

	and maintain evidence of the review."			
28	BLM: "Implement a process by which administrative personnel coordinate a periodic review in accordance with the DOI access control security control standard of all user accounts and associated access levels to include the recertification of the appropriateness by users' direct supervisors."	Concur. This recommendation will be tracked through a new POA&M in CSAM. The BLM National Operations Center IT Security group will work with the Project Managers and User Representatives to develop a process for account reviews, create a standard operating procedure document, and ensure each application is performing them on a defined schedule.	OPEN, Target Completion Date: 12/29/2017. [BLM-5018].	No comment.
29	BLM: "Continue with the Department-led planned implementation of the [redacted] tool in fiscal year 2016 to provide the means of automated prevention of unauthorized device connections and/or detection of such connections to prompt manual intervention."	Concur. BLM is working with DOI in this effort. A deployment date has not been identified.	OPEN, Target Completion Date: 12/29/2017. [BLM-5019].	No comment.
30	BOR: "Continue with the Department-led planned implementation of the [redacted] tool in fiscal year 2016 to provide the means of automated prevention of unauthorized device connections and/or detection of such connections to prompt manual intervention."	Concur. BOR is continuing with the Department led planned implementation of the [redacted] tool. No additional corrective actions are planned. DOI POA&M 22737 exists to address this.	OPEN, Target Completion Date: 12/31/2017. [BOR-5021].	No comment.

31	FWS: "Identify and implement a network access control solution for the identification, authentication and management of devices attempting to connect to the FWS network."	Concur. The FWS has existing POA&M 26397 in the [redacted] oundary. The FWS is in the process of installing network tools called [redacted] that is part of the DOI continuous monitoring initiative. [redacted] polling to view and catalog every device that is connected to the network. DOI has indicated that [redacted] may be integrated with [redacted] to easily authorize and deny any device that is placed on the network. [redacted] will allow visibility on systems in approximately 10 minutes of being connected to the network. Currently, [redacted] is in the discovery phase and is scheduled to deploy during FY 2016.	OPEN, Target Completion Date: 12/31/2017. [FWS-5018].	No comment.
32	OCIO: "Develop and implement a formal account management process to ensure that accounts are appropriately created, managed, disabled, and removed."	Concur.	OPEN, Target Completion Date: 11/30/2016. [OIG-0267].	No comment.
33	SOL: "Implement an automated solution for disabling network accounts after 90 days, document and implement a process for the annual review of SOL network accounts."	Concur. The policy and procedure for annual review will be updated as part the SOL System Security Plan (SSP) and policy update activities currently underway. SOL has identified a technology solution for automating account maintenance. SOL will procure and implement a solution during FY16 Q2. SOL will create a POA&M for tracking.	OPEN. [SOL-5009].	No comment.
34	BLM: "Identify and define key events that represent moderate to significant risks to the operation and	Concur. The recommendation will be tracked through a new POA&M in CSAM. BLM has logs from [redacted] available that are parsed out by system but the [redacted]	OPEN, Target Completion Date: 12/29/2017. [BLM-5020].	No comment.

	availability of National Applications data."	is not installed and configured on all National Applications systems. BLM will pursue getting [redacted] installed on National Application systems, identify key events, and assign personnel to formally document and review events. The process, roles, and responsibilities will be documented in a standard operating procedure.		
35	BLM: "Assign the ISSO, or other security personnel, the responsibility of formally documenting and reviewing events and researching the nature of suspicious activity for root cause, risk mitigation, and trends on a weekly basis as defined by department policy."	Concur. The recommendation will be tracked through a new POA&M in CSAM. BLM has logs from [redacted] available that are parsed out by system but the [redacted] is not installed and configured on all National Applications systems. BLM will pursue getting [redacted] installed on National Application systems, identify key events, and assign personnel to formally document and review events. The process, roles, and responsibilities will be documented in a standard operating procedure.	OPEN, Target Completion Date: 12/29/2017. [BLM-5021].	No comment.
36	BOR: "Identify and define key events that represent moderate to significant risks to the operation and availability of [redacted] data."	Concur. A POA&M will be created to address the audit log review process and examining logs for indications of inappropriate or unusual activity.	OPEN, Target Completion Date: 6/1/2017. [BOR-5022].	No comment.
37	BOR: "Assign the ISSO, or other security personnel, the responsibility of formally documenting and reviewing events and researching the nature of suspicious activity for root cause, risk mitigation, and trends on a weekly basis	Concur. A POA&M will be created to address the audit log review process and examining logs for indications of inappropriate or unusual activity.	OPEN, Target Completion Date: 6/1/2017. [BOR-5023].	No comment.

	as defined by department policy.			
38	SOL: "Identify and document auditable events and activities that should be monitored on [redacted]"	Concur. SOL will create a POA&M for tracking.	OPEN. [SOL-5010].	No comment.
39	SOL: "Develop and implement a process to ensure SOL [redacted] server audit logs are reviewed and analyzed for inappropriate and/or unusual activity, in accordance with the DOI Audit and Accountability Security Control Standard."	Concur. SOL is evaluating [redacted] solutions that will correlate audit logs and facilitate efficient analysis of potential nefarious activities. SOL will also explore collaborative opportunities with [redacted] operations. SOL will create a POA&M for tracking.	OPEN. [SOL-5011].	No comment.
40	OCIO: "Continue updating incident response policies and procedures, to include the incident response security control standard and incident response handbook in accordance with NIST Special Publication 800-61 revision 2 and US-CERT federal incident notification guidelines."	Concur.	OPEN. [OIG-0268].	See FY16 FISMA recommendation #15 and #16.
41	OCIO: "Disseminate updated and approved incident response policies and procedures to all bureau and offices."	Concur.	OPEN. [OIG-0269].	No comment.
42	OCIO: "Establish a timeline for bureaus and offices to fully implement updated	Concur.	OPEN. [OIG-0270].	No comment.

	incident response policies and procedures."			
43	BIA: "BIA management should continue to work with [redacted] security personnel to ensure that the SSP is complete and accurate; including verifying the accuracy of the implementation statements for controls AC-02, IA-02, IA-03 and CP-04."	Concur.	OPEN. [BIA-5019].	No comment.
44	FWS: "Ensure all production information systems follow the NIST SP 800-37 Risk Management Framework to include authorization."	Concur. The FWS created POA&M 29656 in the [redacted] boundary. The use of [redacted] platform was discontinued within the FWS before the OIG initiated its FY 2015 FISMA audit. FWS Information Resources and Technology Management (IRTM) has allocated resources for [redacted] to undergo the A&A (Assessment & Authorization) process. At the conclusion of the process, the [redacted] solution will operate with an Authority To Operate (ATO).	OPEN, Target Completion Date: 12/31/2017. [FWS-5019].	No comment.
45	FWS: "Enforce the requirement to ensure that the [redacted] SSP is complete and accurate including documenting implementation statements."	Concur. The FWS created POA&M 29608 in the [redacted] boundary. FWS IT Security is modifying control inheritance for [redacted] The security team will document appropriate implementation statements after the modification.	OPEN, Target Completion Date: 12/31/2017. [FWS-5020].	No comment.
46	OCIO: "Coordinate with SOL management to ensure that the [redacted] SSP is complete and accurate including documenting implementation	Concur.	OPEN. [OIG-0271].	No comment.

	statements for controls IA- 02, AU-02 and CP-09."			
47	BIA: "Enhance the current [redacted] process to ensure that users with significant security responsibilities are identified, are aware of their training requirements, and are reminded that individuals are responsible for maintaining evidence of their training in accordance with the DOI [redacted] Standard."	Concur.	Completed/Closed on 8/3/2016. [BIA-5020].	No comment.
48	USGS: "Enforce the current process for ensuring that the active directory network accounts for users who do not complete the annual security training are disabled until the requirement is met."	Concur. Management concurs with this recommendation as documented in October 2015 USGS response to USGS-NFR-03. USGS is tracking corrective actions through POA&M 29624 assigned to USGS Program.	OPEN, Target Completion Date: 11/19/2016. [WGS-5009].	No comment.
49	USGS: "Enhance the current process for ensuring that all personnel with significant information security to include system administrator responsibilities are identified and appropriately assigned [redacted] system.	Concur. Management concurs with this recommendation as documented in October 2015 USGS response to USGS-NFR-03. USGS is tracking corrective actions through POA&M 29624 assigned to USGS Program.	OPEN, Target Completion Date: 11/19/2016. [WGS-5010].	No comment.
50	FWS: "Enforce the current process and provide information system support, for the management, oversight	Concur. The FWS created POA&M 29608 under the FWS Program to address necessary corrective actions.	OPEN, Target Completion Date: 12/31/2017. [FWS-5021].	No comment.

	and remediation of POA&Ms."			
51	BIA: "Coordinate with business management to enhance the mission essential functions for the COOP."	Concur. OIMT has been without a Disaster Recovery (DR) lead for a year, and as such, the DR responsibilities including COOP, were collateral for other personnel. OIMT now has a full-time employee filling this position and plans are in place to perform necessary testing.	OPEN. [BIA-5021].	No comment.
52	BIA: "Ensure that the COOP is tested on an annual basis and the test plan and results are appropriately documented and maintained."	Concur. OIMT has been without a Disaster Recovery (DR) lead for a year, and as such, the DR responsibilities including COOP, were collateral for other personnel. OIMT now has a full-time employee filling this position and plans are in place to perform necessary testing.	OPEN. [BIA-5022].	No comment.
53	BLM: "Test the NOC Contingency Plan in accordance with NIST requirements. The test documentation should indicate the methodology, procedures, results, and lessons learned. Where necessary, the NOC Contingency Plan should be updated based on the results of the test."	Concur. This recommendation will be tracked through a new POA&M in CSAM. The BLM National Operations Center (NOC) Contingency Plan (CP) is currently in revision. Once this has been completed, the CP will be tested in accordance with NIST. The CP will be updated based on the results of the plan.	OPEN. [BLM-5022].	See FY16 FISMA recommendation #19.
54	BLM: "Train recovery team members on their system recovery roles and responsibilities."	Concur. This recommendation will be tracked through a new POA&M in CSAM. The BLM National Operations Center (NOC) IT Security group will work with the Project Managers and User Representatives to develop a process for account reviews, create a standard operating procedure document, and ensure each application is performing them on a defined schedule.	OPEN, Target Completion Date: 12/29/2017. [BLM-5023].	No comment.

55	BOR: "Design and implement a process in which the status of backups jobs are reviewed daily to help ensure unsuccessful backups are manually resolved when not automatically rerun to success the following day."	Concur. A portion of this recommendation is already in place [redacted] backups are currently reviewed daily. A POA&M will be created to address the weakness of unsuccessful backups being resolved when not automatically rerun to success the following day. The POA&M will be associated with [redacted], which maintains the responsibility for [redacted] backups.	OPEN, Target Completion Date: 12/31/2016. [BOR-5024].	No comment.
56	FWS: "Follow the existing process to ensure that information system components are appropriately identified and backups are consistently performed, in accordance with Departmental policy, for all [redacted] servers."	Concur. The FWS created POA&M 29652 in the [redacted] boundary. The Information System Security Officer (ISSO) will take steps in concert with the Operations Manager to ensure that the [redacted] is accurate and current, per established procedures. The ISSO will also maintain artifacts of backup schedule or replication schedule for all [redacted] components.	OPEN, Target Completion Date: 12/31/2017. [FWS-5022].	No comment.
57	SOL: "Develop and document a COOP in accordance with the requirements documented in FCD-1."	Concur. SOL will collaborate with OCIO Information Assurance Policy, [redacted] group to develop and document the SOL COOP plan. SOL will create a POA&M for tracking.	OPEN. [SOL-5012].	No comment.
58	SOL: "Enforce the requirement to test the SOL Network contingency plans at least annually."	Concur. SOL will collaborate with OCIO [redacted] group to develop annual CP plan testing. SOL will create a POA&M for tracking.	OPEN. [SOL-5013].	No comment.
59	SOL: "Update and enforce information system backup procedures to ensure backups are performed in accordance with control CP-09 of the DOI	Concur. SOL will update backup procedures to be consistent with DOI CP-09 of the DOI Contingency Planning Security Control Standard. This will be done in coordination and collaboration with OCIO's [redacted],	OPEN. [SOL-5014].	No comment.

	Contingency Planning Security Control Standard."	[redacted] group. SOL will create a POA&M for tracking.		

Appendix IV – NIST SP 800-53 Security Controls Cross-Referenced to FY2016 OIG FISMA Metrics

The table below represents NIST SP 800-53 security controls that KPMG considered during the performance audit.

Continuous Monitoring Management	
CA-1	Security Assessment and Authorization Policies and Procedures
CA-2	Security Assessments
CA-5	Plan of Action and Milestones
CA-7	Continuous Monitoring
Configuration Management	
CM-1	Configuration Management Policy and Procedures
CM-2	Baseline Configurations
CM-3	Configuration Change Control
CM-4	Security Impact Analysis
CM-6	Configuration Settings
CM-7	Least Functionality
CM-8	Information System Component Inventory
RA-5	Vulnerability Scanning
SI-2	Flaw Remediation
Identity and Access Management	
AC-1	Access Control Policy and Procedures
AC-2	Account Management
AC-10	Concurrent Session Control
AC-11	Session Lock
AC-17	Remote Access
AC-18	Wireless Access
IA-2	Identification and Authentication
IA-3	Device Identification and Authentication
Incident and Response Reporting	
IR-1	Incident Response Policy and Procedures
IR-4	Incident Handling
IR-5	Incident Monitoring
IR-6	Incident Reporting
IR-7	Incident Response Assistance
IR-8	Incident Response Plan
AU-6	Audit Review, Analysis, and Reporting
AU-9	Protection of Audit Information
Risk Management	
RA-1	Risk Assessment Policy and Procedures
RA-2	Security Categorization
CA-2	Security Assessments
CA-6	Security Authorization
CA-7	Continuous Monitoring
PL-2	System Security Plan
PM-5	Information System Inventory
SI-3	Malicious Code Protection
SI-4	Information System Monitoring
SI-8	Spam Protection

AU-2	Auditable Events
AU-3	Content of Audit Records
Security Training	
AT-1	Security Awareness and Training Policy and Procedures
AT-3	Security Training
AT-4	Security Training Records
Plan of Action and Milestone	
CA-5	Plan of Action and Milestones
PM-3	Information Security Resources
PM-4	Plan of Action and Milestones Process
Remote Access Management	
AC-1	Access Control Policy and Procedures
AC-17	Remote Access
PL-4	Rules of Behavior
PS-6	Access Agreements
IA-2	Identification and Authentication
IR-6	Incident Reporting
Contingency Planning	
CP-1	Contingency Planning Policy and Procedures
CP-2	Contingency Plan
CP-4	Contingency Plan Testing and Exercises
CP-7	Alternate Processing Site
CP-9	Information System Backup
SA-12	Supply Chain Protection
Contractor Systems	
CA-2	Security Assessments
PL-2	System Security Plan
PM-5	Information System Inventory
SA-1	System and Services Acquisition Policy and Procedures
SA-4	Acquisitions

Appendix V – 2016 FISMA Reporting Metrics

The following tables contain the responses to the control metrics established by DHS for the annual OIG FISMA Reporting Metrics.

Risk Management (Identify)	
1.1	Has the organization established a risk management program that includes comprehensive agency policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? The Department of the Interior (DOI) has established a risk management program; however, improvements are needed as policies and procedures have not been formally approved. More specifically, the DOI Security Control Standards, which are in the process of being updated to be aligned with the National Institute of Standards and Technology (NIST) Special Publication 800-53 revision 4. Based on internal DOI milestones; DOI expected to formalize the DOI Security Control Standards by March 31, 2016. All Bureau and Office information systems are to complete control level migration, including assessment, for all controls as part of the annual control assessments, including those identified as critical controls and those controls new to NIST SP 800-53 revision 4 by December 31, 2016.
1.1.1	Identifies and maintains an up-to-date system inventory, including organization- and contractor-operated systems, hosting environments, and systems residing in the public, hybrid, or private cloud. (2016 CIO FISMA Metrics, 1.1; NIST Cybersecurity Framework (CF) 1D.AM.1, NIST 800-53: PM-5) Metric met.
1.1.2	Develops a risk management function that is demonstrated through the development, implementation, and maintenance of a comprehensive governance structure and organization-wide risk management strategy as described in NIST SP 800-37, Rev. 1. (NIST SP 800-39) Metric met.
1.1.3	Incorporates mission and business process-related risks into risk-based decisions at the organizational perspective, as described in NIST SP 800-37, Rev. 1. (NIST SP 800-39) Metric met.
1.1.4	Conducts information system level risk assessments that integrate risk decisions from the organizational and mission/business process perspectives and take into account threats, vulnerabilities, likelihood, impact, and risks from external parties and common control providers. (NIST SP 800-37, Rev. 1, NIST SP 800-39, NIST SP 800-53: RA-3)

	Metric met.
1.1.5	Provides timely communication of specific risks at the information system, mission/business, and organization-level to appropriate levels of the organization. Metric met.
1.1.6	Performs comprehensive assessments to categorize information systems in accordance with Federal Standards and applicable guidance. Metric met.
1.1.7	Selects an appropriately tailored set of baseline security controls based on mission/business requirements and policies and develops procedures to employ controls within the information system and its environment of operation. Metric met.
1.1.8	Implements the tailored set of baseline security controls as described in 1.1.7. Metric met.
1.1.9	Identifies and manages risks with system interconnections, including through authorizing system interconnections, documenting interface characteristics and security requirements, and maintaining interconnection security agreements. (NIST SP 800-53: CA-3) Metric met.
1.1.10	Continuously assesses the security controls, including hybrid and shared 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. Based on review of the DOI Fiscal Year 2016 Mid-Year Assurance Statement on Internal Controls Over Information Technology, dated September 9, 2016; two of 21 financial systems, OSM – Coal Fee Collection Management System and OST – Trust Funds Accounting System, did not fully assess NIST 800-53 revision 4 controls.
1.1.11	Maintains ongoing information system authorizations 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 (OMB M-14-03, NIST Supplemental Guidance on Ongoing Authorization).

	Metric met.
1.1.12	Security authorization package contains system security plan, security assessment report, and POA&M that are prepared and maintained in accordance with government policies. (SP 800-18, SP 800-37) Metric met.
1.1.13	POA&Ms are maintained and reviewed to ensure they are effective for correcting security weaknesses. Metric met.
1.1.14	Centrally tracks, maintains, and independently reviews/validates POA&M activities at least quarterly. Metric met.
1.1.15	Prescribes the active involvement of information system owners and common control providers, chief information officers, senior information security officers, authorizing officials, and other roles as applicable in the ongoing management of information-system-related security risks. Metric met.
1.1.16	Implemented an insider threat detection and prevention program, including the development of comprehensive policies, procedures, guidance, and governance structures, in accordance with Executive Order 13587 and the National 1nsider Threat Policy. (PMC; NIST SP 800-53: PM-12) Metric met.
1.1.17	Provide any additional information on the effectiveness (positive or negative) of the organization's Risk Management program that was not noted in the questions above. Based on all testing performed, is the Risk Management program effective? No further information provided
Contractor Systems (Identify)	
1.2	Has the organization established a program to oversee systems operated on its behalf by contractors or other entities, including other government agencies, managed hosting environments, and systems and services residing in a cloud external to the organization that is inclusive of policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines?

	DOI has established a program to oversee information systems operated on behalf of DOI; however, implementation requires improvement at the Office of the Secretary, Interior Business Center.
1.2.1	Establishes and implements a process to ensure that contracts/statements of work/solicitations for systems and services, include appropriate information security and privacy requirements and material disclosures, FAR clauses, and clauses on protection, detection, and reporting of information. (FAR Case 2007-004, Common Security Configurations, FAR Sections 24.104, 39.101, 39.105, 39.106, 52.239-1; PMC, 2016 CIO Metrics 1.8, NIST 800-53, SA-4 FedRAMP standard contract clauses; Cloud Computing Contract Best Practices) Metric met.
1.2.2	Specifies within appropriate agreements how information security performance is measured, reported, and monitored on contractor- or other entity-operated systems. Metric met.
1.2.3	Obtains sufficient assurance that the security controls of systems operated on the organization's behalf by contractors or other entities and services provided on the organization's behalf meet FISMA requirements, OMB policy, and applicable NIST guidelines. (NIST SP 800-53: CA-2, SA-9) DOI has approximately 22 operational contractor operated information systems of 123 information systems and relies on contractors to operate these information systems and process information on their behalf. The Office of the Secretary's procedures for monitoring contractor-operated information systems are not formally documented, consistently performed, and roles and responsibilities not fully defined.
1.2.4	Provide any additional information on the effectiveness (positive or negative) of the organization's Contractor Systems Program that was not noted in the questions above. Based on all testing performed, is the Contractor Systems Program effective? No further information provided.
Configuration Management (Protect)	
2.1	Has the organization established a configuration management program that is inclusive of comprehensive agency policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Metric met.

2.1.1	Develops and maintains an up-to-date inventory of the hardware assets (i.e., endpoints, mobile assets, network devices, input/output assets, and SMART/NEST devices) connected to the organization's network with the detailed information necessary for tracking and reporting. (NIST CF 1D.AM-1; 2016 CIO FISMA Metrics 1.5, 3.17; NIST 800-53: CM-8) Metric met.
2.1.2	Develops and maintains an up-to-date inventory of software platforms and applications used within the organization and with the detailed information necessary for tracking and reporting. (NIST 800-53: CM-8, NIST CF 1D.AM-2) Metric met.
2.1.3	Implements baseline configurations for IT systems that are developed and maintained in accordance with documented procedures. (NIST SP 800-53: CM-2; NIST CF PR.1P-1) Metric met.
2.1.4	Implements and maintains standard security settings (also referred to as security configuration checklists or hardening guides) for IT systems in accordance with documented procedures. (NIST SP 800-53: CM-6; CIO 2016 FISMA Metrics, 2.3) Metric met.
2.1.5	Assesses configuration change control processes, including processes to manage configuration deviations across the enterprise that are implemented and maintained. (NIST SP 800-53: CM-3, NIST CF PR.1P-3) Metric met.
2.1.6	Identifies and documents deviations from configuration settings. Acceptable deviations are approved with business justification and risk acceptance. Where appropriate, automated means that enforce and redeploy configuration settings to systems at regularly scheduled intervals are deployed, while evidence of deviations is also maintained. (NIST SP 800-53: CM-6, Center for 1nternet Security Controls (C1S) 3.7) Metric met.
2.1.7	Implemented SCAP certified software assessing (scanning) capabilities against all systems on the network to assess both code-based and configuration-based vulnerabilities in accordance with risk management decisions. (NIST SP 800-53: RA-5, S1- 2; CIO 2016 FISMA Metrics 2.2, C1S 4.1) Metric met.

2.1.8	Remediates configuration-related vulnerabilities, including scan findings, in a timely manner as specified in organization policy or standards. (NIST 800-53: CM-4, CM-6, RA-5, S1-2) DOI has established a configuration management program; however, vulnerability and patch management implementation improvements are needed. Eight of 13 Bureaus and Offices, BIA, BLM, BOR, BSEE, FWS, NPS, OIG, and USGS did not consistently remediate security patches and vulnerabilities in accordance with the DOI Risk Assessment and System Information Integrity Security Control Standards.
2.1.9	Develops and implements a patch management process in accordance with organization policy or standards, including timely and secure installation of software patches. (NIST SP 800-53: CM-3, S1-2, OMB M-16-04, DHS Binding Operational Directive 15-01) DOI has established a configuration management program; however, vulnerability and patch management implementation improvements are needed. Eight of 13 Bureaus and Offices, BIA, BLM, BOR, BSEE, FWS, NPS, OIG, and USGS did not consistently remediate security patches and vulnerabilities in accordance with the DOI Risk Assessment and System Information Integrity Security Control Standards.
2.1.10	Provide any additional information on the effectiveness (positive or negative) of the organization's Configuration Management Program that was not noted in the questions above. Based on all testing performed, is the Configuration Management Program effective? No further information provided.
Identity and Access Management (Protect)	
2.2	Has the organization established an identity and access management program, including policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? The Department has established an identity and access management program; however, implementation improvements are needed at two bureaus, Bureau of Indian Affairs (BIA) and U.S. Geological Survey (USGS).
2.2.1	Ensures that individuals requiring access to organizational information and information systems sign appropriate access agreements, participate in required training prior to being granted access, and recertify access agreements on a predetermined interval. (NIST 800-53: PL-4, PS-6) Metric met.
2.2.2	Ensures that all users are only granted access based on least privilege and separation-of-duties principles.

	Metric met.
2.2.3	Distinguishes hardware assets that have user accounts (e.g., desktops, laptops, servers) from those without user accounts (e.g. networking devices, such as load balancers and intrusion detection/prevention systems, and other input/output devices such as faxes and 1P phones). Metric met.
2.2.4	Implements PIV for physical access in accordance with government policies. (HSPD 12, F1PS 201, OMB M-05-24, OMB M-07-06, OMB M-08-01, OMB M-11-11) Metric met.
2.2.5	Implements PIV or a NIST Level of Assurance (LOA) 4 credential for logical access by all privileged users (system, network, database administrators, and others responsible for system/application control, monitoring, or administration functions). (Cybersecurity Sprint, OMB M-16-04, PMC, 2016 CIO FISMA Metrics 2.5.1) Metric met.
2.2.6	Enforces PIV or a NIST LOA 4 credential for logical access for at least 85% of non-privileged users. (Cybersecurity Sprint, OMB M-16-04, PMC, 2016 CIO FISMA Metrics 2.4.1) Based on the DOI IBM Bigfix Personal Identity Verification (PIV) compliance report, USGS is enforcing PIV for logical access for 78% of non-privileged users.
2.2.7	Tracks and controls the use of administrative privileges and ensures that these privileges are periodically reviewed and adjusted in accordance with organizationally defined timeframes. (2016 CIO FISMA Metrics 2.9, 2.10; OMB M-16-04, CIS 5.2) The USGS National Map Re-engineering Project (NMRP) did not define and implement a process to ensure all user accounts to include developers are reviewed annually in accordance with DOI Access Control Security Control Standard. [redacted]
2.2.8	Ensures that accounts are terminated or deactivated once access is no longer required or after a period of inactivity, according to organizational policy. BIA did not consistently deactivate network user access for 2 of 25 terminated employees. Both terminated user accounts maintained remote access to the BIA computing environment. BIA management took immediate action and disabled 1 of 2 user access.

2.2.9	Identifies, limits, and controls the use of shared accounts. (NIST SP 800-53: AC-2) Metric met.
2.2.10	All users are uniquely identified and authenticated for remote access using Strong Authentication (multi-factor), including PIV. (NIST SP 800-46, Section 4.2, Section 5.1, NIST SP 800-63) Metric met.
2.2.11	Protects against and detects unauthorized remote access connections or subversion of authorized remote access connections, including through remote scanning of host devices. (C1S 12.7, 12.8, FY 2016 CIO FISMA metrics 2.17.3, 2.17.4, 3.11, 3.11.1) Metric met.
2.2.12	Remote access sessions are timed-out after 30 minutes of inactivity, requiring user re-authentication, consistent with OMB M-07-16 Metric met.
2.2.13	Enforces a limit of consecutive invalid remote access logon attempts and automatically locks the account or delays the next logon prompt. (NIST 800-53: AC-7 Metric met.
2.2.14	Implements a risk-based approach to ensure that all agency public websites and services are accessible through a secure connection through the use and enforcement of https and strict transport security. (OMB M-15-13) Metric met.
2.2.15	Provide any additional information on the effectiveness (positive or negative) of the organization's 1dentity and Access Management Program that was not noted in the questions above. Based on all testing performed is the 1dentity and Access Management Program effective? No further information provided.
Security and Privacy Training (Protect)	

2.3	Has the organization established a security and privacy awareness and training program, including comprehensive agency policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? DOI has established an effective security and privacy awareness training program.
2.3.1	Develops training material for security and privacy awareness training containing appropriate content for the organization, including anti-phishing, malware defense, social engineering, and insider threat topics. (NIST SP 800-50, 800-53: AR-5, OMB M-15-01, 2016 CIO Metrics, PMC, National 1nsider Threat Policy (NITP)) Metric met.
2.3.2	Evaluates the skills of individuals with significant security and privacy responsibilities and provides additional security and privacy training content or implements human capital strategies to close identified gaps. (NIST SP 800-50) Metric met.
2.3.3	Identifies and tracks status of security and privacy awareness training for all information system users (including employees, contractors, and other organization users) requiring security awareness training with appropriate internal processes to detect and correct deficiencies. (NIST 800-53: AT-2) Metric met.
2.3.4	Identifies and tracks status of specialized security and privacy training for all personnel (including employees, contractors, and other organization users) with significant information security and privacy responsibilities requiring specialized training. Metric met.
2.3.5	Measures the effectiveness of its security and privacy awareness and training programs, including through social engineering and phishing exercises. (PMC, 2016 CIO FISMA Metrics 2.19, NIST SP 800-50, NIST SP 800-55) Metric met.
2.3.6	Provide any additional information on the effectiveness (positive or negative) of the organization's Security and Privacy Training Program that was not noted in the questions above. Based on all testing performed is the Security and Privacy Training Program effective? No further information provided.

Information System Continuous Monitoring	
Level One	
3.1.1	ISCM program is not formalized and ISCM activities are performed in a reactive manner resulting in an ad hoc program that does not meet Level 2 requirements for a defined program consistent with NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO ISCM CONOPS.
3.1.1.1	ISCM stakeholders and their responsibilities have not been fully defined and communicated across the organization. Metric met.
3.1.1.2	The organization has not performed an assessment of the skills, knowledge, and resources needed to effectively implement an ISCM program. Key personnel do not possess knowledge, skills, and abilities to successfully implement an effective ISCM program. Metric met.
3.1.1.3	The organization has not defined how ISCM information will be shared with individuals with significant security responsibilities and used to make risk based decisions. DOI and the National Park Service (NPS) continuous monitoring strategy and plans do not define how ISCM information will be shared with individuals with significant security responsibilities.
3.1.1.4	The organization has not defined how it will integrate ISCM activities with organizational risk tolerance, the threat environment, and business/mission requirements. DOI and the NPS's continuous monitoring strategy and plan do not define how ISCM activities will integrate into their respective risk management programs.
3.1.1.5	ISCM processes have not been fully defined and are performed in an ad-hoc, reactive manner for the following areas: ongoing assessments and monitoring of security controls; performing hardware asset management, software asset management, configuration setting management, and common vulnerability management; collecting security related information required for metrics, assessments, and reporting; analyzing ISCM data, reporting findings, and determining the appropriate risk responses; and reviewing and updating the ISCM program.

	Metric met.
3.1.1.6	ISCM results vary depending on who performs the activity, when it is performed, and the methods and tools used. Metric met.
3.1.1.7	The organization has not identified and defined the qualitative and quantitative performance measures that will be used to assess the effectiveness of its ISCM program, achieve situational awareness, and control ongoing risk. Based on inquiry of personnel with managing the DOI and NPS Information Security Continuous Monitoring program and inspection of DOI and NPS continuous monitoring strategy and plans; DOI and NPS do not identify and define the qualitative and quantitative performance measures to measure the effectiveness of their respective ISCM programs. Additionally, a process has not been fully developed to consider lessons learned to improve the ISCM programs.
3.1.1.8	The organization has not defined its processes for collecting and considering lessons learned to improve ISCM processes. Based on inquiry of personnel with managing the DOI and NPS Information Security Continuous Monitoring program and inspection of DOI and NPS continuous monitoring strategy and plans; DOI and NPS do not identify and define the qualitative and quantitative performance measures to measure the effectiveness of their respective ISCM programs. Additionally, a process has not been fully developed to consider lessons learned to improve the ISCM programs.
3.1.1.9	The organization has not identified and defined the ISCM technologies needed in one or more of the following automation areas and relies on manual/procedural methods in instances where automation would be more effective. Use of ISCM technologies in the following areas is ad-hoc. Patch management License management Information management Software assurance Vulnerability management Event management Malware detection Asset management

	Configuration management Network management Incident management Metric met.
3.1.1.10	The organization has not defined how it will use automation to produce an accurate point-in-time inventory of the authorized and unauthorized devices and software on its network and the security configuration of these devices and software. DOI has not documented how it intends to produce an accurate inventory of authorized and unauthorized devices and software on the Department network to include the Bureaus and Offices. Additionally, based on results of network reconnaissance tools, the Department's IBM Bigfix tool used for hardware asset management is not consistently implemented across the Department. Nine Bureaus and Offices, BLM, BOR, BSEE, FWS, NPS, OIG, OS, IBC, and USGS have not fully implemented Bigfix.
Level 2 Information System Continuous Monitoring	
3.2.1	The organization has formalized its ISCM program through the development of comprehensive ISCM policies, procedures, and strategies consistent with NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO ISCM CONOPS. However, ISCM policies, procedures, and strategies are not consistently implemented organization-wide. ISCM stakeholders and their responsibilities have been defined and communicated across the organization. However, stakeholders may not have adequate resources (people, processes, and technology) to effectively implement ISCM activities. Metric not evaluated as exceptions were noted in Level 1: Ad hoc.
3.2.1.1	The organization has performed an assessment of the skills, knowledge, and resources needed to effectively implement an ISCM program. 1n addition, the organization has developed a plan for closing any gaps identified. However, key personnel may still lack the knowledge, skills, and abilities to successfully implement an effective ISCM program. Metric not evaluated as exceptions were noted in Level 1: Ad hoc.
3.2.1.2	The organization has defined how ISCM information will be shared with individuals with significant security responsibilities and used to make risk-based decisions. However, ISCM information is not always shared with individuals with significant security responsibilities in a timely manner with which to make risk-based decisions. Metric not evaluated as exceptions were noted in Level 1: Ad hoc.

3.2.1.3	The organization has defined how it will integrate ISCM activities with organizational risk tolerance, the threat environment, and business/mission requirements. However, ISCM activities are not consistently integrated with the organization's risk management program. Metric not evaluated as exceptions were noted in Level 1: Ad hoc.
3.2.1.4	ISCM processes have been fully defined for the following areas: ongoing assessments and monitoring of security controls; performing hardware asset management, software asset management, configuration setting management, and common vulnerability management; collecting security related information required for metrics, assessments, and reporting; analyzing ISCM data, reporting findings, and determining the appropriate risk responses; and reviewing and updating the ISCM program. However, these processes are inconsistently implemented across the organization. Metric not evaluated as exceptions were noted in Level 1: Ad hoc.
3.2.1.5	ISCM results vary depending on who performs the activity, when it is performed, and the methods and tools used. Metric not evaluated as exceptions were noted in Level 1: Ad hoc.
3.2.1.6	The organization has identified and defined the performance measures and requirements that will be used to assess the effectiveness of its ISCM program, achieve situational awareness, and control ongoing risk. However, these measures are not consistently collected, analyzed, and used across the organization. Metric not evaluated as exceptions were noted in Level 1: Ad hoc.
3.2.1.7	The organization has a defined process for capturing lessons learned on the effectiveness of its ISCM program and making necessary improvements. However, lessons learned are not consistently shared across the organization and used to make timely improvements to the ISCM program. Metric not evaluated as exceptions were noted in Level 1: Ad hoc.
3.2.1.8	The organization has identified and fully defined the ISCM technologies it plans to utilize in the following automation areas. In addition, the organization has developed a plan for implementing ISCM technologies in these areas: patch management, license management, information management, software assurance, vulnerability management, event management, malware detection, asset management, configuration management, network management, and incident management. However, the organization has not fully implemented technology is these automation areas and continues to rely on manual/procedural methods in instances where automation would be more effective. 1n addition, while automated tools are implemented to support some ISCM activities, the tools may not be interoperable.

	Metric not evaluated as exceptions were noted in Level 1: Ad hoc.
3.2.1.9	The organization has defined how it will use automation to produce an accurate point-in-time inventory of the authorized and unauthorized devices and software on its network and the security configuration of these devices and software. However, the organization does not consistently implement the technologies that will enable it to manage an accurate point-in-time inventory of the authorized and unauthorized devices and software on its network and the security configuration of these devices and software. Metric not evaluated as exceptions were noted in Level 1: Ad hoc
Level 3 Information System Continuous Monitoring	
3.3.1	In addition to the formalization and definition of its ISCM program (Level 2), the organization consistently implements its ISCM program across the agency. However, qualitative and quantitative measures and data on the effectiveness of the ISCM program across the organization are not captured and utilized to make risk-based decisions, consistent with NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO ISCM CONOPS.ISCM stakeholders and their responsibilities have been identified and communicated across the organization, and stakeholders have adequate resources (people, processes, and technology) to effectively implement ISCM activities. Metric not evaluated as exceptions were noted in Level 1: Ad hoc.
3.3.1.1	The organization has fully implemented its plans to close any gapes in skills, knowledge, and resources required to successfully implement an ISCM program. Personnel possess the required knowledge, skills, and abilities to effectively implement the organization's ISCM program. Metric not evaluated as exceptions were noted in Level 1: Ad hoc.
3.3.1.2	ISCM information is shared with individuals with significant security responsibilities in a consistent and timely manner with which to make risk-based decisions and support ongoing system authorizations. Metric not evaluated as exceptions were noted in Level 1: Ad hoc.
3.3.1.3	ISCM activities are fully integrated with organizational risk tolerance, the threat environment, and business/mission requirements. Metric not evaluated as exceptions were noted in Level 1: Ad hoc.
3.3.1.4	ISCM processes are consistently performed across the organization in the following areas: ongoing assessments and monitoring of security controls; performing hardware asset management, software asset management, configuration setting management, and common vulnerability management; collecting security related information required for metrics, assessments, and reporting;

	analyzing ISCM data, reporting findings, and determining the appropriate risk responses; and reviewing and updating the ISCM program. Metric not evaluated as exceptions were noted in Level 1: Ad hoc.
3.3.1.5	The rigor, intensity, scope, and results of ISCM activities are comparable and predictable across the organization. Metric not evaluated as exceptions were noted in Level 1: Ad hoc.
3.3.1.6	The organization is consistently capturing qualitative and quantitative performance measures on the performance of its ISCM program in accordance with established requirements for data collection, storage, analysis, retrieval, and reporting. ISCM measures provide information on the effectiveness of ISCM processes and activities. Metric not evaluated as exceptions were noted in Level 1: Ad hoc.
3.3.1.7	The organization is consistently capturing and sharing lessons learned on the effectiveness of ISCM processes and activities. Lessons learned serve as a key input to making regular updates to ISCM processes. Metric not evaluated as exceptions were noted in Level 1: Ad hoc.
3.3.1.8	The organization has consistently implemented its defined technologies in all of the following ISCM automation areas. ISCM tools are interoperable to the extent practicable. Patch management License management 1nformation management Software assurance Vulnerability management Event management Malware detection Asset management Configuration management Network management

	Incident management Metric not evaluated as exceptions were noted in Level 1: Ad hoc.
3.3.1.9	The organization can produce an accurate point-in-time inventory of the authorized and unauthorized devices and software on its network and the security configuration of these devices and software. Metric not evaluated as exceptions were noted in Level 1: Ad hoc.
Level 4 Information System Continuous Monitoring	
3.4.1	In addition to being consistently implemented (Level 3), ISCM activities are repeatable and metrics are used to measure and manage the implementation of the ISCM program, achieve situational awareness, control ongoing risk, and perform ongoing system authorizations. Metric not evaluated as exceptions were noted in Level 1: Ad hoc.
3.4.1.1	The organization's staff is consistently implementing, monitoring, and analyzing qualitative and quantitative performance measures across the organization and is collecting, analyzing, and reporting data on the effectiveness of the organization's ISCM program. Metric not evaluated as exceptions were noted in Level 1: Ad hoc.
3.4.1.2	Skilled personnel have been hired and/or existing staff trained to develop the appropriate metrics to measure the success of the ISCM program. Metric not evaluated as exceptions were noted in Level 1: Ad hoc.
3.4.1.3	Staff are assigned responsibilities for developing and monitoring ISCM metrics, as well as updating and revising metrics as needed based on organization risk tolerance, the threat environment, business/mission requirements, and the results of the ISCM program. Metric not evaluated as exceptions were noted in Level 1: Ad hoc.
3.4.1.4	The organization has processes for consistently implementing, monitoring, and analyzing qualitative and quantitative performance measures across the organization and is collecting, analyzing, and reporting data on the effectiveness of its processes for performing ISCM. Metric not evaluated as exceptions were noted in Level 1: Ad hoc.

3.4.1.5	Data supporting ISCM metrics are obtained accurately, consistently, and in a reproducible format. Metric not evaluated as exceptions were noted in Level 1: Ad hoc.
3.4.1.6	The organization is able to integrate metrics on the effectiveness of its ISCM program to deliver persistent situational awareness across the organization, explain the environment from both a threat/vulnerability and risk/impact perspective, and cover mission areas of operations and security domains. Metric not evaluated as exceptions were noted in Level 1: Ad hoc.
3.4.1.7	The organization uses its ISCM metrics for determining risk response actions including risk acceptance, avoidance/rejection, or transfer. Metric not evaluated as exceptions were noted in Level 1: Ad hoc.
3.4.1.8	ISCM metrics are reported to the organizational officials charged with correlating and analyzing the metrics in ways that are relevant for risk management activities. Metric not evaluated as exceptions were noted in Level 1: Ad hoc.
3.4.1.9	ISCM is used to maintain ongoing authorizations of information systems and the environments in which those systems operate, including common controls and keep required system information and data (i.e., System Security Plan Risk Assessment Report, Security Assessment Report, and POA&M) up to date on an ongoing basis. Metric not evaluated as exceptions were noted in Level 1: Ad hoc.
3.4.1.10	The organization uses technologies for consistently implementing, monitoring, and analyzing qualitative and quantitative performance across the organization and is collecting, analyzing, and reporting data on the effectiveness of its technologies for performing ISCM. Metric not evaluated as exceptions were noted in Level 1: Ad hoc.
3.4.1.11	The organization's ISCM performance measures include data on the implementation of its ISCM program for all sections of the network from the implementation of technologies that provide standard calculations, comparisons, and presentations. Metric not evaluated as exceptions were noted in Level 1: Ad hoc.

3.4.1.12	The organization utilizes a S1EM tool to collect, maintain, monitor, and analyze IT security information, achieve situational awareness, and manage risk Metric not evaluated as exceptions were noted in Level 1: Ad hoc.
Level 5 Information System Continuous Monitoring	
3.5.1	In addition to being managed and measurable (Level 4), the organization's ISCM program is institutionalized, repeatable, self-regenerating, and updated in a near real-time basis based on changes in business/mission requirements and a changing threat and technology landscape.
3.5.1.1	The organization's assigned personnel collectively possess a high skill level to perform and update ISCM activities on a near real-time basis to make any changes needed to address ISCM results based on organization risk tolerance, the threat environment, and business/mission requirements. Metric not evaluated as exceptions were noted in Level 1: Ad hoc.
3.5.1.2	The organization has institutionalized a process of continuous improvement incorporating advanced cybersecurity and practices. Metric not evaluated as exceptions were noted in Level 1: Ad hoc.
3.5.1.3	On a near real-time basis, the organization actively adapts its ISCM program to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a timely manner. Metric not evaluated as exceptions were noted in Level 1: Ad hoc.
3.5.1.4	The ISCM program is fully integrated with strategic planning, enterprise architecture and capital planning and investment control processes, and other mission/business areas, as appropriate. Metric not evaluated as exceptions were noted in Level 1: Ad hoc.
3.5.1.5	The ISCM program achieves cost-effective IT security objectives and goals and influences decision making that is based on cost, risk, and mission impact. Metric not evaluated as exceptions were noted in Level 1: Ad hoc.
3.5.1.6	The organization has institutionalized the implementation of advanced cybersecurity technologies in near real-time.

	Metric not evaluated as exceptions were noted in Level 1: Ad hoc.
3.5.1.7	The organization has institutionalized the use of advanced technologies for analysis of trends and performance against benchmarks to continuously improve its ISCM program. Metric not evaluated as exceptions were noted in Level 1: Ad hoc.
Level 1 Incident Response	
4.1.1	Incident response program is not formalized and incident response activities are performed in a reactive manner resulting in an ad-hoc program that does not meet Level 2 requirements for a defined program consistent with FISMA (including guidance from NIST SP 800-83, NIST SP 800-61 Rev. 2, NIST SP 800-53, OMB M-16-03, OMB M-16-04, and US-CERT Federal Incident Notification Guidelines).
4.1.1.1	Incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies have not been fully defined and communicated across the organization, including the designation of a principal security operations center or equivalent organization that is accountable to agency leadership, DHS, and OMB for all incident response activities. Metric met.
4.1.1.2	The organization has not performed an assessment of the skills, knowledge, and resources needed to effectively implement an incident response program. Key personnel do not possess the knowledge, skills, and abilities to successfully implement an effective incident response program. Metric met.
4.1.1.3	The organization has not defined a common threat vector taxonomy and defined how incident response information will be shared with individuals with significant security responsibilities and other stakeholders, and used to make timely, risk-based decisions. Metric met.
4.1.1.4	The organization has not defined how it will integrate incident response activities with organizational risk management, continuous monitoring, continuity of operations, and other mission/business areas, as appropriate. Metric met.
4.1.1.5	Incident response processes have not been fully defined and are performed in an ad-hoc, reactive manner for the following areas:

	incident response planning, incident response training and testing; incident detection and analysis; incident containment, eradication, and recovery; incident coordination, information sharing, and reporting to internal and external stakeholders using standard data elements and impact classifications within timeframes established by US-CERT. DOI has not formally approved its incident response program, plans, and procedures. KPMG was informed that DOI senior management is in the process of reviewing and approving updated incident response policies and procedures, in which DOI considered the recent United States Computer Emergency Readiness Team (US-CERT) reporting requirements. An official Incident Response Handbook was updated and submitted to DOI management for review. The target for Department-wide promulgation for both is December 30, 2016.
4.1.1.6	The organization has not fully defined how it will collaborate with DHS and other parties, as appropriate, to provide on-site, technical assistance/surge resources/special capabilities for quickly responding to incidents. Metric met.
4.1.1.7	The organization has not identified and defined the qualitative and quantitative performance measures that will be used to assess the effectiveness of its incident response program, perform trend analysis, achieve situational awareness, and control ongoing risk. DOI has not identified and defined qualitative and quantitative performance measures to be used to perform trend analysis and assess the effectiveness of its incident response program.
4.1.1.8	The organization has not defined its processes for collecting and considering lessons learned and incident data to improve security controls and incident response processes. Metric met.
4.1.1.9	The organization has not identified and defined the incident response technologies needed in one or more of the following areas and relies on manual/procedural methods in instances where automation would be more effective. Use of incident response technologies in the following areas is ad-hoc. Web application protections, such as web application firewalls Event and incident management, such as intrusion detection and prevention tools, and incident tracking and reporting tools Aggregation and analysis, such as security information and event management (S1EM) products Malware detection, such as anti-virus and antispam software technologies 1nformation management, such as data loss prevention

	File integrity and endpoint and server security tools DOI has not fully implemented an enterprise Security Information and Event Management (SIEM) tool to aid in the collection and analysis of incident information response; however, an enterprise SIEM is planned for future implementation as part of the Department of Homeland Security Continuous Diagnostics and Monitoring initiative (CDM).
4.1.1.10	The organization has not defined how it will meet the defined Trusted 1nternet Connection (T1C) security controls and ensure that all agency traffic, including mobile and cloud, are routed through defined access points, as appropriate. Metric met.
4.1.1.11	The organization has not defined how it plans to utilize DHS' Einstein program for intrusion detection/prevention capabilities for traffic entering and leaving the organization's networks. Metric met.
4.1.1.12	The organization has not defined how it plans to utilize technology to develop and maintain a baseline of network operations and expected data flows for users and systems. DOI has not defined how it plans to utilize technology to develop and maintain a baseline of expected data flows for users and systems.
Level 2 Incident Response	
4.2.1	The organizational has formalized its incident response program through the development of comprehensive incident response policies, plans, and procedures consistent with FISMA (including guidance from NIST SP 800-83, NIST SP 800-61 Rev. 2, NIST SP 800-53, OMB M-16-03, OMB M-16-04, and US-CERT Federal Incident Notification Guidelines). However, incident response policies, plans, and procedures are not consistently implemented organization-wide. See metric 4.1.1
4.2.1.1	Incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies have been fully defined and communicated across the organization, including the designation of a principal security operations center or equivalent organization that is accountable to agency leadership, DHS, and OMB for all incident response activities. However, stakeholders may not have adequate resources (people, processes, and technology) to effectively implement incident response activities. Further, the organization has not verified roles and responsibilities as part of incident response testing. Metric met.

4.2.1.2	The organization has performed an assessment of the skills, knowledge, and resources needed to effectively implement an incident response program. 1n addition, the organization has developed a plan for closing any gaps identified. However, key personnel may still lack the knowledge, skills, and abilities to successfully implement an effective incident response program. Metric met.
4.2.1.3	The organization has defined a common threat vector taxonomy and defined how incident response information will be shared with individuals with significant security responsibilities and other stakeholders, and used to make timely, risk-based decisions. However, the organization does not consistently utilize its threat vector taxonomy and incident response information is not always shared with individuals with significant security responsibilities and other stakeholders in a timely manner. Metric met.
4.2.1.4	The organization has defined how it will integrate incident response activities with organizational risk management, continuous monitoring, continuity of operations, and other mission/business areas, as appropriate. However, incident response activities are not consistently integrated with these areas. Metric met.
4.2.1.5	Incident response processes have been fully defined for the following areas: incident response planning, incident response training and testing; incident detection and analysis; incident containment, eradication, and recovery; incident coordination, information sharing, and reporting using standard data elements and impact classifications within timeframes established by US-CERT. However, these processes are inconsistently implemented across the organization. Metric not evaluated as exceptions were noted in Level 1: Ad hoc.
4.2.1.6	The organization has fully defined, but not consistently implemented, its processes to collaborate with DHS and other parties as appropriate, to provide on-site, technical assistance/surge resources/special capabilities for quickly responding to incidents. Metric not evaluated as exceptions were noted in Level 1: Ad hoc.
4.2.1.7	The organization has identified and defined the qualitative and quantitative performance measures that will be used to assess the effectiveness of its incident response program, perform trend analysis, achieve situational awareness, and control ongoing risk. However, these measures are not consistently collected, analyzed, and used across the organization. Metric not evaluated as exceptions were noted in Level 1: Ad hoc.

4.2.1.8	The organization has defined its processes for collecting and considering lessons learned and incident data to improve security controls and incident response processes. However, lessons learned are not consistently captured and shared across the organization and used to make timely improvements to security controls and the incident response program. Metric not evaluated as exceptions were noted in Level 1: Ad hoc.
4.2.1.9	The organization has identified and fully defined the incident response technologies it plans to utilize in the following areas: Web application protections, such as web application firewalls Event and incident management, such as intrusion detection and prevention tools, and incident tracking and reporting tools Aggregation and analysis, such as security information and event management (S1EM) products. However, the organization has not ensured that security and event data are aggregated and correlated from all relevant sources and sensors. Malware detection such as Anti-virus and antispam software technologies 1nformation management such as data loss prevention File integrity and endpoint and server security tools However, the organization has not fully implemented technologies in these areas and continues to rely on manual/procedural methods in instances where automation would be more effective. 1n addition, while tools are implemented to support some incident response activities, the tools are not interoperable to the extent practicable, do not cover all components of the organization's network, and/or have not been configured to collect and retain relevant and meaningful data consistent with the organization's incident response policy, plans, and procedures. Metric not evaluated as exceptions were noted in Level 1: Ad hoc.
4.2.1.10	The organization has defined how it will meet the defined T1C security controls and ensure that all agency traffic, including mobile and cloud, are routed through defined access points, as appropriate. However, the organization has not ensured that the T1C 2.0 provider and agency managed capabilities are consistently implemented. Metric not evaluated as exceptions were noted in Level 1: Ad hoc.
4.2.1.11	The organization has defined how it plans to utilize DHS' Einstein program for intrusion detection/prevention capabilities for traffic entering and leaving its networks. Metric not evaluated as exceptions were noted in Level 1: Ad hoc.

4.2.1.12	The organization has defined how it plans to utilize technology to develop and maintain a baseline of network operations and expected data flows for users and systems. However, the organization has not established, and does not consistently maintain, a comprehensive baseline of network operations and expected data flows for users and systems. Metric not evaluated as exceptions were noted in Level 1: Ad hoc.

Level 3 Incident Response	
4.3.1	In addition to the formalization and definition of its incident response program (Level 2), the organization consistently implements its incident response program across the agency, in accordance with FISMA (including guidance from NIST SP 800-83, NIST SP 800-61 Rev. 2, NIST SP 800-53, OMB M-16-03, OMB M-16-04, and US-CERT Federal Incident Notification Guidelines). However, data supporting metrics on the effectiveness of the incident response program across the organization are not verified, analyzed, and correlated
4.3.1.1	Incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies have been fully defined, communicated, and consistently implemented across the organization (Level 2). Further, the organization has verified roles and responsibilities of incident response stakeholders as part of incident response testing. Metric met.
4.3.1.2	The organization has fully implemented its plans to close any gaps in the skills, knowledge, and resources needed to effectively implement its incident response program. Incident response teams are periodically trained to ensure that knowledge, skills, and abilities are maintained. Metric met.
4.3.1.3	The organization consistently utilizes its defined threat vector taxonomy and shares information with individuals with significant security responsibilities and other stakeholders in a timely fashion to support risk-based decision making. Metric met.
4.3.1.4	Incident response activities are integrated with organizational risk management, continuous monitoring, continuity of operations, and other mission/business areas, as appropriate. Metric met.

4.3.1.5	Incident response processes are consistently implemented across the organization for the following areas: incident response planning, incident response training and testing; incident detection and analysis; incident containment, eradication, and recovery; incident coordination, information sharing, and reporting using standard data elements and impact classifications within timeframes established by US-CERT. Metric not evaluated as exceptions were noted in Level 1: Ad hoc.
4.3.1.6	The organization has ensured that processes to collaborate with DHS and other parties as appropriate, to provide on-site, technical assistance/surge resources/special capabilities for quickly responding to incidents are implemented consistently across the organization. Metric not evaluated as exceptions were noted in Level 1: Ad hoc.
4.3.1.7	The organization is consistently capturing qualitative and quantitative performance metrics on the performance of its incident response program. However, the organization has not ensured that the data supporting the metrics was obtained accurately and in a reproducible format or that the data is analyzed and correlated in ways that are effective for risk management. Metric not evaluated as exceptions were noted in Level 1: Ad hoc.
4.3.1.8	The organization is consistently collecting and capturing lessons learned and incident data on the effectiveness of its incident response program and activities. However, lessons learned may not be shared across the organization in a timely manner and used to make timely improvements to the incident response program and security measures. Metric not evaluated as exceptions were noted in Level 1: Ad hoc.
4.3.1.9	The rigor, intensity, scope, and results of incident response activities (i.e. preparation, detection, analysis, containment, eradication, and recovery, reporting and post incident) are comparable and predictable across the organization. Metric not evaluated as exceptions were noted in Level 1: Ad hoc.
4.3.1.10	The organization has consistently implemented its defined incident response technologies in the following areas: Web application protections, such as web application firewalls Event and incident management, such as intrusion detection and prevention tools, and incident tracking and reporting tools

	Aggregation and analysis, such as security information and event management (S1EM) products. The organization ensures that security and event data are aggregated and correlated from all relevant sources and sensors Malware detection, such as anti-virus and antispam software technologies Information management, such as data loss prevention File integrity and endpoint and server security tools In addition, the tools are interoperable to the extent practicable, cover all components of the organization's network, and have been configured to collect and retain relevant and meaningful data consistent with the organization's incident response policy, procedures, and plans. Metric not evaluated as exceptions were noted in Level 1: Ad hoc.
4.3.1.11	The organization has consistently implemented defined TIC security controls and implemented actions to ensure that all agency traffic, including mobile and cloud, are routed through defined access points, as appropriate. Metric not evaluated as exceptions were noted in Level 1: Ad hoc.
4.3.1.12	The organization is utilizing DHS' Einstein program for intrusion detection/prevention capabilities for traffic entering and leaving their networks. Metric not evaluated as exceptions were noted in Level 1: Ad hoc.
4.3.1.13	The organization has fully implemented technologies to develop and maintain a baseline of network operations and expected data flows for users and systems. Metric not evaluated as exceptions were noted in Level 1: Ad hoc.
Level 4 Incident Response	
4.4.1	In addition to being consistently implemented (Level 3), incident response activities are repeatable and metrics are used to measure and manage the implementation of the incident response program, achieve situational awareness, and control ongoing risk. 1n addition, the incident response program adapts to new requirements and government-wide priorities.
4.4.1.1	Incident response stakeholders are consistently implementing, monitoring, and analyzing qualitative and quantitative performance measures across the organization and are collecting, analyzing, and reporting data on the effectiveness of the organization's incident response program.

	DOI has not defined performance measures; therefore, incident response stakeholders are not consistently implementing, monitoring, and analyzing qualitative and quantitative performance measures across the organization and are collecting, analyzing, and reporting data on the effectiveness of the organization's incident response program.
4.4.1.2	Skilled personnel have been hired and/or existing staff trained to develop the appropriate metrics to measure the success of the incident response program. Metric met.
4.4.1.3	Incident response stakeholders are assigned responsibilities for developing and monitoring incident response metrics, as well as updating and revising metrics as needed based on organization risk tolerance, the threat environment, business/mission requirements, and the results of the incident response program. Metric met.
4.4.1.4	The organization has processes for consistently implementing, monitoring, and analyzing qualitative and quantitative performance measures across the organization and is collecting, analyzing, and reporting data on the effectiveness of its processes for performing incident response. Metric not evaluated as exceptions were noted in Level 1: Ad hoc
4.4.1.5	Data supporting incident response measures and metrics are obtained accurately, consistently, and in a reproducible format. Metric not evaluated as exceptions were noted in Level 1: Ad hoc
4.4.1.6	Incident response data, measures, and metrics are analyzed, collected, and presented using standard calculations, comparisons, and presentations Metric not evaluated as exceptions were noted in Level 1: Ad hoc.
4.4.1.7	Incident response metrics are reported to organizational officials charged with correlating and analyzing the metrics in ways that are relevant for risk management activities. Metric not evaluated as exceptions were noted in Level 1: Ad hoc.
4.4.1.8	The organization uses technologies for consistently implementing, monitoring, and analyzing qualitative and quantitative performance

	across the organization and is collecting, analyzing, and reporting data on the effectiveness of its technologies for performing incident response activities. Metric not evaluated as exceptions were noted in Level 1: Ad hoc.
4.4.1.9	The organization's incident response performance measures include data on the implementation of its incident response program for all sections of the network. *Metric not evaluated as exceptions were noted in Level 1: Ad hoc.*
Level 5 Incident Response	
4.5.1	In addition to being managed and measurable (Level 4), the organization's incident response program is institutionalized, repeatable, self-regenerating, and updated in a near real-time basis based on changes in business/mission requirements, and a changing threat and technology landscape.
4.5.1.1	The organization's assigned personnel collectively possess a high skill level to perform and update incident response activities on a near real-time basis to make any changes needed to address incident response results based on organization risk tolerance, the threat environment, and business/mission requirements. Metric not evaluated as exceptions were noted in Level 4: Managed and Measurable.
4.5.1.2	The organization has institutionalized a process of continuous improvement incorporating advanced cybersecurity practices. Metric not evaluated as exceptions were noted in Level 1: Ad hoc
4.5.1.3	On a near real-time basis, the organization actively adapts its incident response program to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a near real-time manner. Metric not evaluated as exceptions were noted in Level 1: Ad hoc.
4.5.1.4	The incident response program is fully integrated with organizational risk management, continuous monitoring, continuity of operations, and other mission/business areas, as appropriate. Metric not evaluated as exceptions were noted in Level 1: Ad hoc.
4.5.1.5	The incident response program achieves cost-effective IT security objectives and goals and influences decision making that is based on cost, risk, and mission impact.

	Metric not evaluated as exceptions were noted in Level 1: Ad hoc.
4.5.1.6	The organization has institutionalized the implementation of advanced incident response technologies in near real-time. Metric not evaluated as exceptions were noted in Level 1: Ad hoc.
4.5.1.7	The organization has institutionalized the use of advanced technologies for analysis of trends and performance against benchmarks to continuously improve its incident response program. Metric not evaluated as exceptions were noted in Level 1: Ad hoc.
4.5.1.8	The organization uses simulation based technologies to continuously determine the impact of potential security incidents to its IT assets and adjusts incident response processes and security measures accordingly. Metric not evaluated as exceptions were noted in Level 1: Ad hoc.
Section 5 Contingency Planning	
5.1	Has the organization established an enterprise-wide business continuity/disaster recovery program, including policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? DOI has established an agency-wide business continuity program; however, implementation improvements are needed at five Bureaus and Offices, Bureau of Land Management (BLM), United States Fish and Wildlife Service (FWS), Office of Surface Mining Reclamation and Enforcement (OSMRE), Office of the Special Trustee for American Indians (OST), and the United States Geological Survey (USGS).
5.1.1	Develops and facilitates recovery testing, training, and exercise (TT&E) programs. (FCD1, NIST SP 800-34, NIST SP 800-53) Metric met.
5.1.2	1ncorporates the system's Business 1mpact Analysis and Business Process Analysis into analysis and strategy toward development of the organization's Continuity of Operations Plan, Business Continuity Plan (BCP), and Disaster Recovery Plan (DRP). (NIST SP 800-34) The FWS Business Continuity Plan (BCP) has not been reviewed or updated to consider components such as operating location changes, changes in organizational management, and network infrastructure changes.

5.1.3	Develops and maintains documented recovery strategies, plans, and procedures at the division, component, and IT infrastructure levels. (NIST SP 800-34) The USGS information system, National Map Reengineering Project (NMRP) and Spatial Data Warehouse (SDW) contingency planning documentation does not reflect the current operating environment. Additionally, the NMRP and SDW Standard Operating Procedures have not been reviewed or updated since November 2014. The plan inaccurately documents the alternate processing site and backup procedures are incomplete.
5.1.4	BCP and DRP are in place and ready to be executed upon if necessary. (FCD1, NIST SP 800-34, 2016 CIO FISMA Metrics 5.3, PMC) Metric met.
5.1.5	Tests BCP and DRP for effectiveness and updates plans as necessary. (2016 CIO FISMA Metrics, 5.4 Metric met.
5.1.6	Tests system-specific contingency plans, in accordance with organizationally defined timeframes, to determine the effectiveness of the plans as well as readiness to execute the plans if necessary. (NIST SP 800-53: CP-4) Three Bureaus and Offices, BLM, OSM, and OST did not consistently test information system contingency plans annually in accordance with Departmental policy. More specifically, the BLM General Support System (GSS), OSM Enterprise GSS, and OST Headquarters West did not test its contingency plans in accordance with Department Contingency Plan policy and procedures.
5.1.7	Develops after-action reports that address issues identified during contingency/disaster recovery exercises in order to improve contingency/disaster recovery processes. (FCD1, NIST SP 800-34) The USGS NMRP management team did not incorporate lessons learned, such as the need for redundancy or backup virtual disk images, from the fiscal year 2016 contingency plan test into the system contingency plan.
5.1.8	Determines alternate processing and storage sites based upon risk assessments which ensure the potential disruption of the organization's ability to initiate and sustain operations is minimized, and are not subject to the same physical and/or cybersecurity risks as the primary sites. (FCD1, NIST SP 800-34, NIST SP 800-53: CP-6, CP-7) Metric met.

5.1.9	Conducts backups of information at the user- and system-levels and protects the confidentiality, integrity, and availability of backup information at storage sites. (FCD1, NIST SP 800-34, NIST SP 800-53: CP-9, NIST CF, PR.1P-4, NARA guidance on information systems security records) Metric met
5.1.10	Contingency planning that considers supply chain Threats. Metric met.
5.1.11	Provide any additional information on the effectiveness (positive or negative) of the organization's Contingency Planning Program that was not noted in the questions above. Based on all testing performed is the Contingency Planning Program effective? No additional information to provide.

Appendix VI – Information Security Continuous Monitoring Maturity Model. Source : Council of the Inspector General for Integrity and Efficiency (CIGIE)

The purpose of the maturity model is to (1) summarize the status of agencies' information security programs and their maturity on a 5-level scale, (2) provide transparency to agency CIOs, top management officials, and other interested readers of OIG FISMA reports about what has been accomplished and what still needs to be implemented to improve the information security program to the next maturity level, and (3) help ensure consistency across the OIGs in their annual FISMA reviews.

ISCM Program Maturity Level	Definition	People	Processes	Technology
Level 1 Ad-hoc	**1.1** ISCM program is not formalized and ISCM activities are performed in a reactive manner resulting in an ad-hoc program that does not meet Level 2 requirements for a defined program consistent with NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO ISCM CONOPS. .	**1.1.1** ISCM stakeholders and their responsibilities have not been fully defined and communicated across the organization. **1.1.2** The organization has not performed an assessment of the skills, knowledge, and resources needed to effectively implement an ISCM program. Key personnel do not possess knowledge, skills, and abilities to successfully implement an effective ISCM program. **1.1.3** The organization has not defined how ISCM information will be shared with individuals with significant security responsibilities and used to make risk-based decisions.	**1.1.5** ISCM processes have not been fully defined and are performed in an ad-hoc, reactive manner for the following areas: ongoing assessments and monitoring of security controls; performing hardware asset management, software asset management, configuration setting management, and common vulnerability management; collecting security related information required for metrics, assessments, and reporting; analyzing ISCM data, reporting findings, and determining the appropriate risk responses; and reviewing and updating the ISCM program. **1.1.6** ISCM results vary depending on who performs the activity, when it is performed, and the methods and tools used. **1.1.7** The organization has not identified and defined the qualitative and quantitative performance measures that will be used to	**1.1.9** The organization has not identified and defined the ISCM technologies needed in one or more of the following automation areas and relies on manual/procedural methods in instances where automation would be more effective. Use of ISCM technologies in the following areas is ad-hoc. -Patch management -License management -Information management -Software assurance -Vulnerability management -Event management -Malware detection -Asset management -Configuration management -Network management -Incident management **1.1.10** The organization has not defined how it will use automation to produce an accurate point-in-time inventory of the authorized and unauthorized devices

		1.1.4 The organization has not defined how it will integrate ISCM activities with organizational risk tolerance, the threat environment, and business/mission requirements.	assess the effectiveness of its ISCM program, achieve situational awareness, and control ongoing risk. **1.1.8** The organization has not defined its processes for collecting and considering lessons learned to improve ISCM processes.	and software on its network and the security configuration of these devices and software.

ISCM Program Maturity Level	Definition	People	Processes	Technology
Level 2 Defined	**2.1** The organization has formalized its ISCM program through the development of comprehensive ISCM policies, procedures, and strategies consistent with NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO ISCM CONOPS. However, ISCM policies, procedures, and strategies are not consistently implemented organization-wide.	**2.1.1** ISCM stakeholders and their responsibilities have been defined and communicated across the organization. However, stakeholders may not have adequate resources (people, processes, and technology) to effectively implement ISCM activities. **2.1.2** The organization has performed an assessment of the skills, knowledge, and resources needed to effectively implement an ISCM program. In addition, the organization has developed a plan for closing any gaps identified. However, key personnel may still lack the knowledge, skills, and abilities to successfully implement an effective ISCM program. **2.1.3** The organization has defined how ISCM information will be shared with individuals with significant security responsibilities and used to make risk-based decisions. However, ISCM information is not always shared with individuals with significant security responsibilities in a timely	**2.1.5** ISCM processes have been fully defined for the following areas: ongoing assessments and monitoring of security controls; performing hardware asset management, software asset management, configuration setting management, and common vulnerability management; collecting security related information required for metrics, assessments, and reporting; analyzing ISCM data, reporting findings, and determining the appropriate risk responses; and reviewing and updating the ISCM program. However, these processes are inconsistently implemented across the organization. **2.1.6** ISCM results vary depending on who performs the activity, when it is performed, and the methods and tools used. **2.1.7** The organization has identified and defined the performance measures and requirements that will be used to assess the effectiveness of its ISCM program, achieve situational awareness, and control ongoing risk. However, these measures are not consistently collected, analyzed, and used across the organization.	**2.1.9** The organization has identified and fully defined the ISCM technologies it plans to utilize in the following automation areas. In addition, the organization has developed a plan for implementing ISCM technologies in these areas: patch management, license management, information management, software assurance, vulnerability management, event management, malware detection, asset management, configuration management, network management, and incident management. However, the organization has not fully implemented technology is these automation areas and continues to rely on manual/procedural methods in instances where automation would be more effective. In addition, while automated tools are implemented to support some ISCM activities, the tools may not be interoperable. **2.1.10** The organization has defined how it will use automation to produce an accurate point-in-time inventory of the authorized and unauthorized devices and software on its network and the security configuration of these devices and software. However, the organization does not consistently implement the technologies that will enable it to manage an accurate point-in-time inventory of the authorized and unauthorized devices and software on its network and the security configuration of these devices and software.

		manner with which to make risk-based decisions. **2.1.4** The organization has defined how it will integrate ISCM activities with organizational risk tolerance, the threat environment, and business/mission requirements**.** However, ISCM activities are not consistently integrated with the organization's risk management program.	**2.1.8** The organization has a defined process for capturing lessons learned on the effectiveness of its ISCM program and making necessary improvements. However, lessons learned are not consistently shared across the organization and used to make timely improvements to the ISCM program.	

ISCM Program Maturity Level	Definition	People	Processes	Technology
Level 3 Consistently Implemented	**3.1** In addition to the formalization and definition of its ISCM program (Level 2), the organization consistently implements its ISCM program across the agency. However, qualitative and quantitative measures and data on the effectiveness of the ISCM program across the organization are not captured and utilized to make risk-based decisions, consistent with NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO ISCM CONOPS.	**3.1.1** ISCM stakeholders and their responsibilities have been identified and communicated across the organization, and stakeholders have adequate resources (people, processes, and technology) to effectively implement ISCM activities. **3.1.2** The organization has fully implemented its plans to close any gapes in skills, knowledge, and resources required to successfully implement an ISCM program. Personnel possess the required knowledge, skills, and abilities to effectively implement the organization's ISCM program. **3.1.3** ISCM information is shared with individuals with significant security responsibilities in a consistent and timely manner with which to make risk-based decisions and support ongoing system authorizations. **3.1.4** ISCM activities are fully integrated with organizational	**3.1.5** ISCM processes are consistently performed across the organization in the following areas: ongoing assessments and monitoring of security controls; performing hardware asset management, software asset management, configuration setting management, and common vulnerability management; collecting security related information required for metrics, assessments, and reporting; analyzing ISCM data, reporting findings, and determining the appropriate risk responses; and reviewing and updating the ISCM program. **3.1.6** The rigor, intensity, scope, and results of ISCM activities are comparable and predictable across the organization. **3.1.7** The organization is consistently capturing qualitative and quantitative performance measures on the performance of its ISCM program in accordance with established requirements for data collection, storage, analysis, retrieval, and reporting. ISCM measures provide information on the effectiveness of ISCM processes and activities. **3.1.8** The organization is consistently capturing and sharing lessons learned on the effectiveness of ISCM processes and	**3.1.9** The organization has consistently implemented its defined technologies in all of the following ISCM automation areas. ISCM tools are interoperable to the extent practicable. -Patch management -License management -Information management -Software assurance -Vulnerability management -Event management -Malware detection -Asset management -Configuration management -Network management -Incident management **3.1.10** The organization can produce an accurate point-in-time inventory of the authorized and unauthorized devices and software on its network and the security configuration of these devices and software.

		risk tolerance, the threat environment, and business/mission requirements.	activities. Lessons learned serve as a key input to making regular updates to ISCM processes.	

ISCM Program Maturity Level	Definition	People	Processes	Technology
Level 4 Managed & Measurable	**4.1** In addition to being consistently implemented (Level 3), ISCM activities are repeatable and metrics are used to measure and manage the implementation of the ISCM program, achieve situational awareness, control ongoing risk, and perform ongoing system authorizations.	**4.1.1** The organization's staff is consistently implementing, monitoring, and analyzing qualitative and quantitative performance measures across the organization and is collecting, analyzing, and reporting data on the effectiveness of the organization's ISCM program. **4.1.2** Skilled personnel have been hired and/or existing staff trained to develop the appropriate metrics to measure the success of the ISCM program. **4.1.3** Staff are assigned responsibilities for developing and monitoring ISCM metrics, as well as updating and revising metrics as needed based on organization risk tolerance, the threat environment, business/mission requirements, and the results of the ISCM program.	**4.1.4** The organization has processes for consistently implementing, monitoring, and analyzing qualitative and quantitative performance measures across the organization and is collecting, analyzing, and reporting data on the effectiveness of its processes for performing ISCM. **4.1.5** Data supporting ISCM metrics are obtained accurately, consistently, and in a reproducible format. **4.1.6** The organization is able to integrate metrics on the effectiveness of its ISCM program to deliver persistent situational awareness across the organization, explain the environment from both a threat/vulnerability and risk/impact perspective, and cover mission areas of operations and security domains. **4.1.7** The organization uses its ISCM metrics for determining risk response actions including risk acceptance, avoidance/rejection, or transfer. **4.1.8** ISCM metrics are reported to the organizational officials charged with correlating and analyzing the metrics in ways that are relevant for risk management activities.	**4.1.10** The organization uses technologies for consistently implementing, monitoring, and analyzing qualitative and quantitative performance across the organization and is collecting, analyzing, and reporting data on the effectiveness of its technologies for performing ISCM. **4.1.11** The organization's ISCM performance measures include data on the implementation of its ISCM program for all sections of the network from the implementation of technologies that provide standard calculations, comparisons, and presentations. **4.1.12** The organization utilizes a SIEM tool to collect, maintain, monitor, and analyze IT security information, achieve situational awareness, and manage risk.

			4.1.9 ISCM is used to maintain ongoing authorizations of information systems and the environments in which those systems operate, including common controls and keep required system information and data (i.e., System Security Plan Risk Assessment Report, Security Assessment Report, and POA&M) up to date on an ongoing basis.	
ISCM Program Maturity Level	**Definition**	**People**	**Processes**	**Technology**

Level 5 Optimized	**5.1** In addition to being managed and measurable (Level 4), the organization's ISCM program is institutionalized, repeatable, self-regenerating, and updated in a near real-time basis based on changes in business/mission requirements and a changing threat and technology landscape.	**5.1.1** The organization's assigned personnel collectively possess a high skill level to perform and update ISCM activities on a near real-time basis to make any changes needed to address ISCM results based on organization risk tolerance, the threat environment, and business/mission requirements.	**5.1.2** The organization has institutionalized a process of continuous improvement incorporating advanced cybersecurity and practices. **5.1.3** On a near real-time basis, the organization actively adapts its ISCM program to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a timely manner. **5.1.4** The ISCM program is fully integrated with strategic planning, enterprise architecture and capital planning and investment control processes, and other mission/business areas, as appropriate. **5.1.5** The ISCM program achieves cost-effective IT security objectives and goals and influences decision making that is based on cost, risk, and mission impact.	**5.1.6** The organization has institutionalized the implementation of advanced cybersecurity technologies in near real-time. **5.1.7** The organization has institutionalized the use of advanced technologies for analysis of trends and performance against benchmarks to continuously improve its ISCM program.

Report Fraud, Waste, and Mismanagement

Fraud, waste, and mismanagement in Government concern everyone: Office of Inspector General staff, departmental employees, and the general public. We actively solicit allegations of any inefficient and wasteful practices, fraud, and mismanagement related to departmental or Insular Area programs and operations. You can report allegations to us in several ways.

By Internet: www.doioig.gov

By Phone: 24-Hour Toll Free: 800-424-5081
Washington Metro Area: 202-208-5300

By Fax: 703-487-5402

By Mail: U.S. Department of the Interior
Office of Inspector General
Mail Stop 4428 MIB
1849 C Street, NW.
Washington, DC 20240