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

INFORMATION TECHNOLOGY SECURITY WEAKNESSES AT A CORE DATA CENTER COULD EXPOSE SENSITIVE DATA

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

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

FEB 15 2017

Memorandum

To: Sylvia Burns
Chief Information Officer

Lawrence S. Roberts
Assistant Secretary – Indian Affairs

From: Mary L. Kendall
Deputy Inspector General

Subject: Final Evaluation Report – Information Technology Security Weaknesses at a Core Data Center Could Expose Sensitive Data
Report No. 2016-ITA-021

We conducted an evaluation to assess the effectiveness of select information technology security controls for protecting the Department of the Interior's [redacted] and the computer systems it houses from potential loss or disruption. We offer eight recommendations to help ensure that DOI data centers and the systems they house are adequately secured.

In response to our draft report, the Office of the Chief Information Officer concurred with our eight recommendations. We consider seven recommendations resolved but not implemented and one recommendation resolved and implemented. We will refer these recommendations to the Office of Policy, Management and Budget for tracking and resolution.

The legislation creating the Office of Inspector General requires that we report to Congress semiannually on all audit, evaluation, and inspection reports issued; actions taken to implement our recommendations; and recommendations that have not been implemented.

If you have any questions regarding this report, please call me at 202-208-5745.

Table of Contents

Results in Brief

The Continuous Diagnostics and Mitigation (CDM) program is a dynamic approach to fortifying the cyber security of Government networks and systems, including those of the U.S. Department of the Interior (DOI). We previously evaluated DOI's CDM program in our report, "U.S. Department of the Interior's Continuous Diagnostics and Mitigation Program Not Yet Capable of Providing Complete Information for Enterprise Risk Determinations" (Report No. ISD-IN-MOA-0004-2014-I). In this evaluation, we found that the CDM program at DOI's [redacted] ([redacted] is immature and not fully effective in protecting the 24 information technology systems owned by the Bureau of Indian Affairs (BIA) and the Bureau of Indian Education (BIE) from potential exploitation. We also assessed the adequacy of controls that help ensure continuity of business operations should [redacted] experience a disaster.

We found that BIA's management practices failed to detect critical and high-risk vulnerabilities on the [redacted] ([redacted] an [redacted] high-value IT asset that contains personally identifiable information [redacted] and left thousands of critical and high-risk vulnerabilities unmitigated for years on other BIA and BIE systems. In addition, BIA's capability to identify unauthorized computers or detect and remove obsolete and potentially malicious software (i.e., malware) were inadequate, exposing [redacted] systems to potential compromise. BIA also did not monitor any of its computers to ensure they remained securely configured over time. We also found that inadequate contingency planning for [redacted] resulted in temporary disruption to DOI and other Federal agencies' mission operations due to a power outage in March 2016.

These deficiencies occurred because BIA failed to: (1) install DOI's inventory management software on all computers; (2) identify and remove unauthorized and unsupported products from BIA and BIE systems; (3) mitigate vulnerabilities in a timely manner; (4) monitor its contractors to ensure all IT security requirements were met; (5) monitor computers to ensure they remained securely configured; and (6) meet annual contingency planning and plan testing requirements. Further, the Office of Chief Information Officer (OCIO) did not provide the oversight necessary to ensure that BIA complied with the Department's IT security program. Until BIA improves its IT security practices and OCIO strengthens its oversight role, BIA high-value IT assets will remain at high risk of compromise, the results of which could have a serious adverse effect on DOI operations and cause the loss of sensitive data. We make seven recommendations to BIA and one recommendation to OCIO to help ensure that DOI data centers and the systems they house are adequately secured.

Introduction

Objective

We assessed the effectiveness of selected information technology (IT) security controls for protecting the U.S. Department of the Interior's (DOI) [redacted] ([redacted]) and the computer systems it houses from potential loss or disruption. Specifically, we assessed [redacted] progress in—

- developing inventories of computer hardware and software;
- managing operating system configurations; and
- detecting and mitigating technical vulnerabilities.

These are key elements for the foundation of an organization's IT security program and the Phase 1 requirements for the governmentwide Continuous Diagnostics and Mitigation (CDM) initiative. We also assessed the adequacy of controls that help ensure continuity of business operations should [redacted] experience a disaster.

Background

DOI spends about $1 billion annually on its information technology asset portfolio, which include data centers and the computer systems they house that support a range of bureau programs that—

- protect and manage our Nation's natural resources and cultural heritage;
- provide scientific and other information to stakeholders interested in those resources; and
- help meet responsibilities to American Indians, Alaska Natives, and affiliated Island communities.

A DOI data center is a facility used for housing and protecting computer systems and communications equipment that store and process data used to support bureau operations. [redacted] is one of the Department's [redacted]. As such, [redacted] operates 24 computer systems that support the mission of the bureaus of Indian Affairs and Indian Education. [redacted] also houses computer systems used by other bureaus and Federal agencies. Indian Affairs is responsible for overall management of the [redacted] and the BIA Chief Information Security Officer is responsible for ensuring the implementation of the Department's IT security program for BIA and BIE systems operated at [redacted]

DOI designated [redacted] as well as one of the computer systems it houses—the [redacted] ([redacted]) as high-value IT assets. According to the U.S. Office of Management and Budget (OMB), high-value IT assets refer to those IT systems, facilities, and data that are of particular interest to nation-state adversaries, such as foreign military and intelligence services.

Specifically, high-value IT assets often contain sensitive data or support mission-critical operations. The loss or disruption of a high-value IT asset could have a serious adverse effect on agency operations, assets, or individuals.

CDM Program

Established by Congress in 2013, the CDM program is a dynamic approach to fortifying the cyber security of Government networks and systems. Specifically, as noted in OMB Memorandum M-14-03, "Enhancing the Security of Federal Information and Information Systems," dated November 18, 2013, CDM provides Federal agencies with capabilities and software tools that identify cyber security risks on an ongoing basis and prioritize these risks based on potential impacts, enabling IT personnel to mitigate the most significant problems first. CDM also provides risk-based and cost-effective cyber security capabilities to more efficiently allocate limited cyber security resources.

The CDM program spans 15 continuous diagnostic control areas that will be implemented in three phases. Phase 1 is the foundation for protecting Federal information systems and data by using automated software tools to help agencies establish and maintain computer hardware and software inventories and implementing enterprise wide vulnerability and configuration management capabilities. We previously evaluated DOI's CDM program in our report, "U.S. Department of the Interior's Continuous Diagnostics and Mitigation Program Not Yet Capable of Providing Complete Information for Enterprise Risk Determinations" (Report No. ISD-IN-MOA-0004-2014-I).

An organizationwide inventory of computers and software programs is a fundamental control that helps Federal agencies ensure that only authorized computers and approved software are present in each agency's IT environment. Moreover, accurate hardware and software inventories also increase the effectiveness of an IT security program by certifying that 100 percent of an organization's IT assets undergo continuous monitoring to ensure they remain securely configured and free of vulnerabilities.

Vulnerability management is the process of detecting and remediating system vulnerabilities. Vulnerabilities are software flaws or system misconfigurations that can be exploited to gain access to or control of an information system. Vulnerability scanners are specialized software programs that automate the vulnerability detection process. Specifically, vulnerability scanners search large databases of known vulnerabilities associated with commonly used computer operating systems and software applications. When a match is found in the database, the scanner alerts the operator to a possible vulnerability. The scanners rank vulnerabilities according to their potential to harm the system, allowing an organization to prioritize and mitigate its most critical vulnerabilities. Most vulnerability scanners also generate reports to help system administrators fix discovered vulnerabilities. System administrators commonly remediate vulnerabilities by applying software patches, updating a system configuration, or

adding a compensating control. DOI's IBM BigFix repository also contains vulnerability data for the systems monitored.

Configuration management is the process of assessing and, if necessary, modifying settings to ensure that such IT assets as computer servers and clients (e.g., workstations and laptops) remain in a secure state, with security configurations implemented and set, and are not vulnerable to exploitation. Often, operating systems on these computers are configured by the vendor for ease-of-deployment and ease-of-use rather than for security, leaving them exploitable in their default state. To address this issue, the Center for Internet Security (CIS) has published recommended configuration settings, called benchmarks, for securing a wide variety of computer operating systems. We used the CIS benchmark to measure compliance with best practices in our testing.

Initializing a computer's operating system to a secure state is not sufficient to ensure ongoing protection against exploitation. As such, ongoing configuration monitoring is essential for maintaining the security of the Department's high-value IT assets. For example, computer operating systems that are improperly configured are susceptible to compromise and thus may potentially be used by intruders to gain unauthorized access to the Department's computer network. Once inside, the intruder can use the compromised computer to exploit other weaknesses, which could result in the loss or impairment of Department IT resources, including its high-value IT assets. Because operating system configurations can change when software patches are applied or when computers are upgraded, it is necessary to monitor operating systems continuously to verify that they remain securely configured.

Data centers and the computer and communication systems they house are vulnerable to a variety of disruptions such as power outages, hardware failures, or equipment destruction resulting from fire or other catastrophic events. Contingency planning defines the resources needed and processes to be followed in order to effectively and efficiently recover a system following a disruption. If a disruption occurs and the contingency plan is not effective, the organization could be unable to perform critical business operations. Thus, contingency planning and contingency plan testing helps mitigate the risk to business operations by providing assurance that the data center and the computer and communication systems it houses will be recoverable and normal operations can be restored following a disruption.

The Federal Information Modernization Act of 2014 (FISMA) defines specific information security requirements Federal agencies, including DOI, must satisfy and assigns responsibilities to agency heads, senior agency officials, and agency inspectors general for satisfying FISMA requirements. FISMA requires that agencies develop policies and procedures commensurate with the risk and magnitude of harm resulting from the malicious or unintentional impairment of agency information assets. Under FISMA, the Department's Chief Information

Officer (CIO) is responsible for developing and overseeing departmentwide, risk-based, and cost-effective program for meeting Federal and departmental IT security requirements.

Independent verification and validation (IV&V) is a structured, two-step quality control and quality assurance process widely used for improving products and processes in the information technology domain. Verification, the first step, determines whether a product or process meets regulations. Validation, the second step, establishes evidence to provide a high degree of assurance that a product or process meets its intended requirement.

Findings

Based on our review of Continuous Diagnostics and Mitigation (CDM) and contingency planning practices at the [redacted] ([redacted] we found that the Bureau of Indian Affairs' (BIA) CDM program ineffective for protecting the 24 BIA and Bureau of Indian Education (BIE) systems at [redacted] from potential loss or disruption. Specifically, we found that the bureaus either failed to implement all four CDM Phase 1 controls, or implemented the control incompletely or ineffectively. We also found that BIA's poor contingency planning practices contributed to computer hardware failures at [redacted] which adversely affected mission operations for BIA, the Office of the Special Trustee and the U.S. Department of Health and Human Services when their information technology (IT) systems housed at [redacted] became unavailable. Overall, our findings reflect that the Office of the Chief Information Officer (OCIO) does not provide effective oversight of bureaus and cannot ensure that bureaus fully implement the Department's IT security program.

Incomplete Hardware Asset Inventories

The goal of the CDM hardware asset management control is to actively inventory and track all hardware devices, such as computers, routers, and firewalls, so that only authorized devices are present in the Department of the Interior's (DOI) IT environment. As part of implementing this control, DOI selected IBM BigFix software as its enterprisewide solution for managing hardware and software inventories. In order to develop inventories of authorized hardware devices and approved software products, IBM BigFix agents (software programs) must first be installed on all DOI computers. Once installed, the agents register DOI computers and the software programs on them to a central repository. The repository serves as an authoritative departmentwide hardware and software inventory. The data in the repository are used for reporting key IT security metrics to senior DOI and Office of Management and Budget (OMB) officials, which help allocate resources and shape future IT security investments.

We performed discovery scans at [redacted] using network addresses supplied by BIA and BIE. We identified 793 BIA network devices and 209 BIE network devices representing either a computer, firewall appliance or other network device. For BIA, we tested 185 of the 793 devices (23 percent) to determine whether the devices were included in the Department's hardware inventory. We found that 22 of the 185 devices (12 percent) were not included in the hardware inventory because DOI's hardware inventory management solution (IBM BigFix) had not been installed on those devices[1]. BIA IT security personnel stated that the IBM BigFix software was not installed on the 22 devices because the systems associated with them were either test systems or under development. BIA IT staff thought only computers and network devices that were part of production systems

[1] We provided the specific details of our scan results to the BIA Chief Information Security Officer after completion of our tests.

needed to have the Department's inventory management software installed on them.

None of the 209 BIE devices (computers, firewalls etc.) at [redacted] were included in the Department's hardware inventory because the Department's inventory management solution had not been installed on them. This occurred because Indian Affairs, which includes both BIA and BIE, did not fund the purchase of IBM BigFix licenses for BIE systems. According to the BIA Chief Information Security Officer, BIE purchased IBM BigFix software licenses and installation on all BIE IT assets is projected to be completed by April 2017.

OCIO requires that all bureaus and offices load IBM BigFix agents on 100 percent of supported workstations, servers, and devices. This hardware asset inventory control is critical to the overall effectiveness of DOI's CDM program. For example, without a complete and accurate hardware inventory, DOI cannot demonstrate that 100 percent of the applicable devices connected to its networks undergo continuous monitoring to ensure the devices are securely configured and free of critical and high-risk vulnerabilities. A system breach of 1 of the 24 moderate impact systems at [redacted] could result in the disruption of mission-critical bureau operations and could also result in the loss of sensitive data. Moreover, CDM reports will be inaccurate as they will be based on incomplete information, which could lead to a misrepresentation of the security status of DOI's high-value IT assets and a misallocation of resources.

Software Asset Management Control Not Implemented

We found that BIE did not implement the software asset management control because the IBM BigFix software needed to develop the software inventory was not installed on any BIE computers. This occurred as previously stated, because Indian Affairs did not provide the necessary funding to BIE to acquire the IBM BigFix software licenses.

To quantify the risk to [redacted] systems, including the high-value IT asset [redacted] we tested [redacted] computers for the presence of vulnerabilities including those associated with unsupported or potentially malicious software. Our tests confirmed the presence of unsupported software containing hundreds of critical and high-risk vulnerabilities on BIA and BIE computers. Upon completion of our tests we provided the details of these vulnerabilities to BIA for remediation.

Thousands of Unmitigated Critical and High-Risk Vulnerabilities on High-Value IT Assets

Detecting and mitigating vulnerabilities before they can be exploited are essential for protecting DOI's high-value IT assets from loss or disruption. We found that the contractor hired by BIE to operate the [redacted] ([redacted]) had not implemented the Department's vulnerability

management process for [redacted] a high-value IT asset containing sensitive information including personally identifiable information (PII) [redacted]

We also found that BIA and BIE left thousands of critical and high-risk vulnerabilities unmitigated for years. These deficiencies occurred because Indian Affairs did not—

- effectively oversee the contractor responsible for implementing required security controls on [redacted]
- promptly mitigate discovered vulnerabilities; and
- mitigate vulnerabilities associated with unsupported software by either removing the software or upgrading to a newer version.

Moreover, because neither BIA nor BIE have complete inventories of computers, the bureaus cannot ensure that vulnerability detection and mitigation process was applied to 100 percent of the computers connected to its networks. As a result, some BIA and BIE computers may not undergo vulnerability scanning and thus, may contain undetected and uncorrected vulnerabilities.

We tested 1,002 BIA and BIE devices at [redacted] using the credentials of privileged user accounts provided by bureau representatives. The hardware devices we tested included computer servers, workstations, and other network devices, such as firewalls and routers, as discovered.

Although the OCIO's security policy requires that bureaus mitigate all critical and high-risk vulnerabilities within 30 days of detection, our tests found over 20,000 unmitigated critical and high-risk vulnerabilities on BIA and BIE's IT assets (see Figure 1). Almost 4,000 of the vulnerabilities we detected remained unmitigated for years, even though software patches to fix the vulnerabilities were available. We found a total of 13,430 instances of vulnerabilities on 337 Microsoft Windows workstations and servers, some of which date back to 2009. We provided the details of these vulnerabilities to BIA for remediation.

[redacted]

[redacted] Unmitigated Critical and High-Risk Vulnerabilities

Bureau	Number of Devices Tested	Critical and High-Risk Vulnerabilities Detected	Critical and High-Risk Vulnerabilities With Available Software Patches
BIA	793	14,441	2,388
BIE	209	5,694	1,584
Total	**1,002**	**20,135**	**3,972**

NOTE: Includes critical and high-risk vulnerabilities where available software patches went unapplied for more than one year.

Figure 1. We identified 20,135 unmitigated critical and high-risk vulnerabilities on DOI's high-value IT assets, including 3,972 with available software patches.
Source: OIG analysis of DOI data.

We also found hundreds of critical and high-risk vulnerabilities on BIA and BIE computers associated with software programs that were no longer supported by the vendor, and accordingly, no longer receive software updates or security patches. Unlike vulnerabilities associated with supported software programs, vulnerabilities present on unsupported software can only be remediated by removing the software or by upgrading to a newer version. As a result, these vulnerabilities will remain unmitigated until the software is either removed or upgraded.

Compromising DOI's high-value IT assets by exploiting any of the thousands of vulnerabilities we detected could have a serious adverse effect on bureau operations and result in the loss of sensitive data.

Finally, we found that [redacted] had not implemented the Department's vulnerability management program since 2009. This occurred because the system is managed by a third-party contractor and the contract's statement of work did not contain explicit requirements for vulnerability detection and mitigation. In 2009, BIA began tracking this IT security deficiency, but it remained unresolved until June 2016, when the contractor began monthly vulnerability scanning of [redacted] We attribute this deficiency to BIA not providing the oversight necessary to ensure that its contractors implemented required IT security controls. Compromising [redacted] could result in the loss of PII [redacted]

[redacted] Computer Servers Not Securely Configured

To help organizations validate that their computers are securely configured the Center for Internet Security (CIS) developed an automated scoring tool (the CIS Configuration Assessment Tool). Using the CIS Configuration Assessment Tool, we tested 14 Windows servers and 4 Windows workstations at BIA and the 6 BIE

servers that store and process [redacted] data. For the BIA computers tested the computer servers were 90 percent compliant and the workstations were 76 percent compliant with the related CIS secure baseline settings. The [redacted] servers tested, however, were only 42 percent complaint with recommended CIS benchmark settings.

According to BIA officials, the servers were put into production before securely configuring the operating system because the contract did not specifically require the contractors to do so. National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations," requires agencies to define secure configuration settings for all of its IT systems, including those managed by third parties. [redacted] servers were not securely configured because OCIO did not provide adequate oversight to ensure BIE met Federal and Department IT security requirements. As such, [redacted] servers were susceptible to compromise, which could result in the disruption of Indian School operations and in the loss of sensitive data.

Finally, we found that neither BIA nor BIE monitored operating system configuration settings to ensure computers remained securely configured over time. This occurred on BIA managed systems because OCIO did not mandate computer operating system configuration monitoring even though configuration monitoring is a recommended best practice and IBM BigFix provides the capability. [redacted] operating system configurations were not monitored because BIA's contract did not require it. Without ongoing configuration monitoring, DOI increases the risk that computers operating high-value IT assets could be compromised—which could potentially have a serious or adverse effect on DOI operations, assets, and individuals.

During our review, we learned that OCIO is developing secure baselines for its operating systems and requiring that bureaus configure their operating systems using the baselines. OCIO is also requiring bureaus to monitor computer operating systems to ensure they remain securely configured. OCIO set a deadline of June 30, 2018, for departmentwide implementation of these two new security measures.

Recommendations

We recommend that BIA:

1. Establish an ongoing process to ensure the inventory of its systems is continually updated and accurate;
2. Install IBM BigFix agents on all applicable BIA and BIE devices;
3. Implement controls that identify and remove unauthorized and unsupported products from BIA and BIE systems;
4. Ensure that critical and high risk vulnerabilities on BIA and BIE systems are mitigated within 30 days of detection in accordance with DOI policy;
5. Review contracts for BIA and BIE systems managed by contractors to ensure the contract contains the appropriate Federal computer security requirements, including critical IT security controls such as vulnerability detection and mitigation;
6. Monitor contractors managing BIA and BIE systems to ensure all IT security requirements are met; and
7. Monitor system configuration settings to ensure BIA and BIE systems remain securely configured over time.

Ineffective Contingency Planning Practices Resulted in Temporary Loss of Data Center Availability

Proper planning and preparation for potential disruptions to the [redacted] are imperative to ensure that BIA, BIE, and external customers can perform mission operations without interruption. For example, NIST 800-34-rev1 "Contingency Planning Guide for Federal Information Systems," May 2010, requires that Federal agencies develop contingency plans for data centers and the systems they house and test the plans at least annually. Contingency plan development and annual plan testing helps ensure continuity of data center operations in the event of a disruption.

During a power outage on March 14, 2016, we found that inadequate contingency planning and plan testing resulted in computer hardware failures at [redacted] and loss of system availability of BIA, the U.S. Department of Health and Human Services (HHS), and the Office of the Special Trustee (OST) systems. A power outage at a utility substation affected about 4,500 customers including [redacted] Loss of power to the data center triggered the successful "failover" to [redacted] generators and

power was immediately restored to computers in the data center; however, power was not immediately restored to the [redacted] computer room air conditioning units. As a result, the temperature in [redacted] reached 120 degrees Fahrenheit within an hour, causing computer hardware failures and loss of system availability. Power was not restored to computer room air conditioning units when [redacted] generators came on line because the electrical switch that connects the air conditioning units to the generators was set to "OFF." The incorrect setting was not identified until approximately an hour later, at which point power was returned to the computer room air conditioning units.

The computer hardware failures and temporary loss of system availability could have been avoided had [redacted] met Federal requirements for contingency planning and plan testing. For example we found that [redacted] had not tested its contingency plan for more than 2 years. Moreover, contingency plan tests for three other moderate impact systems housed by [redacted] also were not tested annually, as required. A disruption to [redacted] or the 24 moderate-impact systems it houses can result in loss of system availability and have serious to serious adverse effect on BIA, BIE, HHS, and OST operations.

A March 24, 2016 After Action Report of the power outage includes corrective actions to improve [redacted] contingency planning and plan testing practices. A contingency plan test for [redacted] was performed in October 2016. Because the After Action Report identifies corrective actions to mitigate deficiencies, we will not issue any recommendations for contingency planning and plan testing activities.

Weak Oversight of Bureau and Contractor IT Security Practices

In our judgement, OCIO could have discovered the deficiencies we identified in BIA's IT security program had it implemented processes to verify and validate bureaus' compliance with Federal and departmental IT security requirements. As a result, the CIO is not receiving timely and accurate information with which to evaluate and report to the Office of Management and Budget the status of its IT security program.

We believe that establishing an independent validation and verification function within OCIO, could strengthen the Department's security program by improving internal processes, which could help ensure that Federal and Department IT security requirements are met. Without this oversight function, DOI cannot ensure that: (1) IT security controls adequately safeguard Department data centers and the systems and data they house; (2) data centers and the systems they house can be effectively recovered and normal operations can be restored following a disruption; and (3) contractors entrusted with implementing security controls for DOI systems and data meet Federal and Department IT security requirements.

Recommendation

We recommend that OCIO:

8. Establish an independent verification and validation function to ensure that all Federal and Department IT security requirements are met and its data centers and the information systems they house are adequately secured.

Conclusion and Recommendations

Conclusion

The Continuous Diagnostics and Mitigation (CDM) program at DOI's [redacted] ([redacted]) is immature and not fully effective in protecting the 24 information technology systems owned by the Bureau of Indian Affairs (BIA) and the Bureau of Indian Education (BIE) from potential exploitation. BIE did not effectively oversee the contractor responsible for implementing the Department's IT security program to ensure that vulnerabilities on the [redacted] ([redacted]), a high-value IT asset, were discovered and timely mitigated.

Bureau management practices left thousands of critical and high-risk vulnerabilities unmitigated for years on other BIA and BIE systems. BIA and BIE computers are running vulnerable unsupported software because the Department has not established and enforced approved software lists. These vulnerabilities cannot be readily mitigated because vendor-provided software patches are no longer available. We also found that [redacted] contingency planning practices contributed to a hardware failures that temporarily affected the availability of BIA, BIE, the Office of the Special Trustee, and Department of Health and Human Services systems.

These deficiencies occurred because BIA failed to: (1) install DOI's inventory management software on all computers; (2) identify and remove unauthorized and unsupported products from BIA and BIE systems; (3) mitigate vulnerabilities in a timely manner; (4) monitor its contractors to ensure all IT security requirements were met; (5) monitor computers to ensure they remained securely configured; and (6) meet annual contingency planning and plan testing requirements. Further, in our judgement, these deficiencies occurred because the Office of the Chief Information Officer (OCIO) did not provide the necessary oversight to ensure that bureaus and their contractors met Federal and Department IT security requirements. OCIO's IT security program would benefit from an independent verification and validation function for its IT security program. Such a program would improve OCIO's internal process and reduce the risk of compromise to DOI's high-value IT assets.

Recommendation Summary

We recommend that BIA:

1. Establish an ongoing process to ensure the inventory of its systems is continually updated and accurate.

   BIA Response: BIA concurred with our recommendation. BIA will document a process to ensure that the inventory of its systems is continually updated and accurate. Target completion date is June 30, 2018.

OIG Reply: Based on the information provided, we consider this recommendation resolved, but not yet implemented. We will refer this recommendation to the Office of Policy, Management and Budget (PMB) to track its implementation.

2. Install IBM BigFix agents on all applicable BIA and BIE devices.

   BIA Response: BIA concurred with our recommendation. BIA will install BigFix agents on all applicable devices. Target completion date is June 30, 2018.

   OIG Reply: Based on the information provided, we consider this recommendation resolved, but not yet implemented. We will refer this recommendation to PMB to track its implementation.

3. Implement controls that identify and remove unauthorized and unsupported products from BIA and BIE systems.

   BIA Response: BIA concurred with our recommendation. BIA is implementing CDM phase 1 controls that will incorporate capabilities for software asset management controls. Target completion date is June 30, 2019.

   OIG Reply: Based on the information provided, we consider this recommendation resolved, but not yet implemented. We will refer this recommendation to PMB to track its implementation.

4. Ensure that critical and high-risk vulnerabilities on BIA and BIE systems are mitigated within 30 days of detection in accordance with DOI policy.

   BIA Response: BIA concurred with our recommendation. BIA is implementing CDM phase 1 controls that will incorporate capabilities and processes for vulnerability management. Target completion date is June 30, 2018.

   OIG Reply: Based on the information provided, we consider this recommendation resolved, but not yet implemented. We will refer this recommendation to PMB to track its implementation.

5. Review contracts for BIA and BIE systems managed by contractors to ensure the contract contains the appropriate Federal computer security requirements, including critical IT security controls such as vulnerability detection and mitigation.

   BIA Response: BIA concurred with our recommendation. Indian Affairs reviewed the [redacted] Statement of Work and determined that the overarching security requirements are included. In addition, BIA produced a guidance document to reset expectations with the [redacted] contractor regarding security

and privacy controls and more clearly define deliverables and reporting requirements that support those controls. This document will be shared with other BIA and BIE Contracting Officers for use in support of future Indian Affairs contracts. Indian Affairs considers this recommendation resolved and implemented.

OIG Reply: We noted BIA's prompt action to resolve this recommendation as a result of findings from our evaluation. Based on BIA's response and review of the guidance document, we consider this recommendation resolved and implemented.

6. Monitor contractors managing BIA and BIE systems to ensure all IT security requirements are met.

   BIA Response: BIA concurred with our recommendation. As of July 2016, Indian Affairs receives monthly vulnerability scanning reports from the [redacted] contractor. Indian Affairs considers this recommendation resolved and implemented.

   OIG Reply: We agree with BIA's directing the [redacted] contractor to implement the Department's vulnerability management process. BIA's response, however, did not mention actions taken to ensure that monthly credentialed vulnerability scans for the entire population of [redacted] computers are consistently performed. As such, we consider the recommendation resolved, but not yet implemented. We will refer this recommendation to PMB to track its implementation.

7. Monitor system configuration settings to ensure BIA and BIE systems remain securely configured over time.

   BIA Response: BIA concurred with our recommendation. BIA is implementing CDM phase 1 controls that will incorporate capabilities and processes to monitor configuration settings to ensure computers remain securely configured. Target completion date is June 30, 2018.

   OIG Reply: Based on the information provided, we consider this recommendation resolved, but not yet implemented. We will refer this recommendation to PMB to track its implementation.

We recommend that OCIO:

8. Establish an independent verification and validation function to ensure that all Federal and Department IT security requirements are met and its data centers and the information systems they house are adequately secured.

   OCIO Response: OCIO concurred with our recommendation. The Compliance and Audit Management (CAM) Branch is the OCIO's

independent verification and validation for closing IT audit recommendations and conducts FISMA compliance reviews using independent auditors and other assessments across bureaus and offices within DOI. OCIO considers this action complete.

OIG Reply: Based on the information provided, we consider this recommendation resolved, but not yet implemented. OCIO has not provided evidence that bureau data centers and the information assets they house are independently evaluated to ensure that Federal and Department IT security requirements are met. As such, we consider the recommendation resolved but not yet implemented. We will refer this recommendation to PMB to track its implementation.

Appendix 1: Scope and Methodology

Scope

The objective of this evaluation was to assess the effectiveness of security controls for Phase 1 of the governmentwide Continuous Diagnostics and Mitigation initiative. We performed technical testing of the [redacted] ([redacted] computer networks and systems and evaluated selected physical security controls.

For this evaluation, our work was limited to the specific procedures and analysis described in the "Rules of Engagement" completed with the Bureau of Indian Affairs (BIA), and was based only on the information made available through June 29, 2016.

Our testing did not include third-party customer systems because their data and applications are owned by the third parties and not the Department.

Methodology

To accomplish our evaluation objectives, we—

- conducted interviews with subject matter experts at the Office of the Chief Information Officer, BIA, and the Bureau of Indian Education;
- performed a walkthrough of [redacted]
- reviewed system security documentation for a sample of systems;
- developed scripts and network tests for on-site testing to obtain system-specific data; and
- compared the results of our technical tests with the data in IBM BigFix.

We obtained a listing of Department-owned assets hosted at [redacted] and judgmentally selected three systems for detailed testing. We selected our sample based on the FIPS 199 security categorizations of "Moderate" and systems rated highest for having sensitive data, quantity of sensitive information controlled or handled, uniqueness of the dataset or capability, impact of loss or compromise, system dependencies, communication support, and type of risk in the event the system is compromised.

We conducted onsite technical testing at BIA's [redacted] from April 25, 2016 through April 29, 2016, and from June 28, 2016 through June 29, 2016. We based initial assessment targets on a range of Internet-Protocol (IP) addresses provided by BIA for Department-owned assets at [redacted] Using the IP ranges provided, we performed discovery tests for common services. Responding IP addresses were then scanned for vulnerabilities with administrative rights. We configured automated tools with "safe" settings so they would not directly impact services.

We then reviewed the automated testing results for relevancy and accuracy. We reported technical findings that presented a significant concern to warrant

additional evaluation and mitigation by BIA and BIE in separate technical vulnerability assessment reports.

As part of our technical testing, we used NESSUS®, an automated vulnerability detection tool to test computers and network devices for vulnerabilities, such as computers running outdated or unpatched software or network services with known security weaknesses. NESSUS® ranks vulnerabilities as critical, high, moderate, or low based on their potential to harm the system.

We asked BIA and BIE to provide workstation and server configurations and deviations. Then, we used automated tools to determine whether the devices were adequately configured.

We also performed walkthroughs of [redacted] conducted interviews with [redacted] security and data center operations personnel, evaluated selected physical security controls of the data center, and reviewed system security plans, contingency plans, and [redacted] backup site documentation.

We conducted this evaluation in accordance with the Quality Standards for Inspection and Evaluation as put forth by the Council of Inspectors General on Integrity and Efficiency. We believe that the work we performed provides a reasonable basis for our conclusions and recommendations.

Appendix 2: Response to Draft Report

The Office of the Chief Information Officer's response follows on page 21.

United States Department of the Interior

OFFICE OF THE SECRETARY
Washington, D.C. 20240

JAN 0 6 2017

To: Kimberly Elmore
Assistant Inspector General for Audits, Inspections, and Evaluations

From: Sylvia Burns
Chief Information Officer

Lawrence S. Roberts
Principal Deputy Assistant Secretary - Indian Affairs

Subject: Office of Inspector General, Information Technology Security Weaknesses at the U.S. Department of the Interior's Core Data Center Could Expose Sensitive Data, Draft Evaluation Report No. 2016-ITA-021, November 2016

The Department of the Interior (Department), Bureau of Indian Affairs (BIA) and the Office of the Chief Information Officer (OCIO), appreciate the opportunity to respond to the Office of Inspector General (OIG) Draft Evaluation Report (Report), Information Security Weaknesses at the U.S. Department of the Interior's Core Data Center Could Expose Sensitive Data, 2016-ITA-021. Attachment 1 provides the Department's planned corrective actions to implement the OIG's recommendations and serves as our formal response.

The BIA and OCIO on behalf of the Department, fully cooperated with the OIG since being advised of this evaluation. The Department accepts the OIG's recommendations and has engaged the BIA to develop the planned corrective action responses for recommendations 1 through 7 and engaged the appropriate OCIO program areas to develop planned corrective action response for recommendation 8.

The Department appreciates the OIG's evaluation of this data center and its objective perspective on this aspect of the Department's IT security posture in the interest of promoting excellence, integrity, and accountability in our IT program, operations, and management.

If you have any questions, please contact me at (202) 2086194 or sylvia_burns@ios.doi.gov. Staff may contact Richard Westmark, Chief, Compliance and Audit Management (CAM) at (202) 513-0749, or richard_westmark@ios.doi.gov.

cc: Allen Lawrence, Office of Financial Management (PFM), Chief, Internal Control and Audit Follow-up (ICAF) Branch
Alexandra Lampros, PFM, ICAF,
Richard Westmark, Chief, Compliance and Audit Management Branch

Attachment:

1. Joint Bureau of Indian Affairs (BIA) and Office of the Chief Information Officer (OCIO) Statement of Actions Planned to Address Office of Inspector General (OIG) Draft Evaluation Report - Information Technology Security Weaknesses at the U.S. Department of the Interior's Core Data Center Could Expose Sensitive Data, Draft Report No. 2016-ITA-021

Attachment 1

Joint Bureau of Indian Affairs (BIA) and Office of the Chief Information Officer (OCIO) Statement of Actions Planned to Address Office of Inspector General Draft Evaluation Report - *Information Technology Security Weaknesses at the U.S. Department of the Interior's Core Data Center Could Expose Sensitive Data*
Draft Report No. 2016-ITA-021

We recommend that BIA:

Recommendation 1: Establish an ongoing process to ensure the inventory of its systems is continually updated and accurate.

Response: Indian Affairs concurs with this recommendation and will document a process to ensure that the inventory of its systems is continually updated and accurate. It should be noted that DOI's Continuous Diagnostics and Mitigation (CDM) Phase 1 is still being implemented and upon reaching steady-state operations will incorporate CDM capabilities and processes to ensure the inventory of its systems is continually updated and accurate. DOI and DHS will complete CDM Phase 1 tools implementation later in 2017 and achieve steady-state operations between 2018 and 2019. Implementation timeframes are driven by the DHS-DOI partnership. While the implementation is funded, the sustaining operations and maintenance (O&M) resources are not programmed for 2018 and out years. Steady-state is an O&M state which follows successful implementation that can demonstrate operational effectiveness and efficiency. Indian Affairs will rely upon a combination of CDM tools as one single tool cannot satisfy the entirety of this recommendation. Timeframes for initial implementation of tools are dependent upon DHS and its contractor.

Responsible Official & Title: Thomas Hoyler, Associate Chief Information Security Officer

Target Completion Date: June 30, 2018

Recommendation 2: Install IBM BigFix agents on all applicable BIA and BIE devices.

Response: Indian Affairs concurs with this recommendation. As of December 7, 2016 IBM BigFix was installed on 7,340 assets (96%) on the BIE network and on 5,661 assets (99%) on the BIA network. Efforts continue to install BigFix on all applicable devices and upon reaching steady-state operations will be able to demonstrate ongoing compliance with this requirement. However, Indian Affairs will rely upon a combination of CDM tools as BigFix alone cannot be used to inventory all Information Technology (IT) hardware.

Responsible Official & Title: Thomas Hoyler, Associate Chief Information Security Officer

Target Completion Date: June 30, 2018

Recommendation 3: Implement controls that identify and remove unauthorized and unsupported products from BIA and BIE systems.

Response: Indian Affairs concurs that the implementation of controls that identify and remove unauthorized and unsupported products from BIA and BIE systems is needed in order to reach an optimized security state. CDM Phase 1 is still being implemented and upon reaching steady-state operations will incorporate capabilities and processes for software asset management controls. Specifically, Indian Affairs will use CDM Phase 1 capabilities to (a.) maintain an accurate inventory of installed software and (b.) recognize and report unauthorized software and unsupported products~ Further, Indian Affairs will work with the DOI OCIO to ensure implementation of effective (c.) procedures for removal of unauthorized products and (d.) planning support for moving away from unsupported products. Indian Affairs will rely upon a combination of CDM tools since one single tool cannot satisfy the entirety of this recommendation. Time frames for initial implementation of tools are dependent upon DHS and its contractor. The processes and procedures will be developed after the implementation of tools. Further, Indian Affairs will need this longer timeframe, which is 2019, to de-conflict software inventories while maintaining continuity of services.

Responsible Official & Title: Thomas Hoyler, Associate Chief Information Security Officer

Target Completion Date: June 30, 2019

Recommendation 4: Ensure that critical and high risk vulnerabilities on BIA and BIE systems are mitigated within 30 days of detection in accordance with DOI policy.

Response: Indian Affairs concurs with this recommendation. As of December 15, 2016, OCIO reported that BIA had 1.23 vulnerabilities per device which placed BIA as the third best bureau/office within the entire Department in terms of vulnerability management. OCIO reported that BIE had 2.07 vulnerabilities per device. CDM Phase 1 is still being implemented and upon reaching steady-state operations, Indian Affairs will incorporate CDM capabilities and processes for vulnerability management. Specifically, Indian Affairs will use CDM Phase 1 capabilities to perform patch deployment in accordance with the NIST SP 800-40 Revision 3, *Guide to Enterprise Patch Management Technologies,* published July 2013. Indian Affairs will rely upon a combination of CDM tools as one single tool cannot satisfy the entirety of this recommendation. Indian Affairs understands that the DOI OCIO will replace the current scanning solution with a new enterprise tool. The processes and procedures will be developed after the implementation of tools.

Responsible Official & Title: Thomas Hoyler, Associate Chief Information Security Officer

Target Completion Date: June 30, 2018

Recommendation 5: Review contracts for BIA and BIE systems managed by contractors to ensure the contract contains the appropriate Federal computer security requirements, including critical IT security controls such as vulnerability detection and mitigation.

Response: Indian Affairs reviewed the current Statement of Work for [redacted] and determined that the overarching security requirements are included; however, a guidance document was produced (*Contractor Information Technology (IT) Security and Privacy Requirements)* to reset expectations with the contractor regarding security and privacy controls as well as to more clearly define the deliverables and reporting requirements that support those controls. This document will be shared with other BIA and BIE Contracting Officers for use in support of future Indian Affairs services contracts. Indian Affairs considers this recommendation resolved and implemented.

Recommendation 6: Monitor contractors managing BIA and BIE systems to ensure all IT security requirements are met.

Response: Specific to the OIG's findings related to vulnerability scanning and patch management for [redacted] IT assets, Indian Affairs began receiving monthly reports from Infinite Campus starting in July 2016. The most recent monthly scan report was received on December 7, 2016 and shows no critical or high vulnerabilities. Indian Affairs considers this recommendation resolved and implemented.

Recommendation 7: Monitor system configuration settings to ensure BIA and BIE systems remain securely configured over time.

Response: CDM Phase 1 is still being implemented. Upon reaching steady-state operations, Indian Affairs will incorporate capabilities and processes to monitor computer operating system configuration settings to ensure computers remain securely configured. Indian Affairs will rely upon a combination of CDM tools as one single tool cannot satisfy the entirety of this recommendation. Timeframes for initial implementation of tools are dependent upon DHS and its contractor. The processes and procedures will be developed after the complete implementation of tools.

Responsible Official & Title: Thomas Hoyler, Associate Chief Information Security Officer

Target Completion Date: June 30, 2018

We recommend that OCIO:

Recommendation 8: Establish an independent verification and validation function to ensure that all Federal and Department IT security requirements are met and its data centers and the information systems they house are adequately secured.

Response: The Department's Office of the Chief Information Officer, (OCIO) concurs with this recommendation. The Compliance and Audit Management (CAM) Branch is the OCIO's independent verification and validation (IV&V) for the closure of IT audit recommendations as part of the A-50 Audit Follow-up. As part of ensuring that all Federal and Department IT security requirements are met and its data centers and the information systems they house are adequately secured, CAM conducts FISMA compliance reviews using independent auditors, and other assessments across all bureaus and offices within Interior. Similar to recommendations made in OIG and GAO IT-related final audit reports, results from these reviews and assessments are used to justify and implement improvements in the Department's IT security program. Further, OCIO has filled critical CAM leadership positions in 2016 to improve effectiveness and efficiency of its mission and functions.

Responsible Official & Title: Richard Westmark, DOI OCIO PPMD/Compliance/Audit Management Branch Chief

Target Completion Date: Complete

Appendix 3: Status of Recommendations

In its response to our draft report, the Office of the Chief Information Officer and the Bureau of Indian Affairs concurred with all eight recommendations (see Appendix 2). Based on the response, we consider seven recommendations resolved but not yet implemented and one recommendation resolved and implemented.

Recommendations	Status	Action Required
1, 2, 3, 4, 6, 7, and 8	Resolved but not yet implemented.	We will refer these recommendations to the Office of Policy, Management and Budget to track implementation.
5	Resolved and implemented.	No further response to OIG is required.

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