



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

U.S. DEPARTMENT OF THE INTERIOR'S CONTINUOUS DIAGNOSTICS AND MITIGATION PROGRAM NOT YET CAPABLE OF PROVIDING COMPLETE INFORMATION FOR ENTERPRISE RISK DETERMINATIONS

FOR OFFICIAL USE - INFORMATION WAS REDACTED FOR PUBLIC RELEASE




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

OCT 19 2016

Memorandum

To: Sylvia Burns
Chief Information Officer

From: Mary L. Kendall 
Deputy Inspector General

Subject: Revised – Final Evaluation 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

We conducted an evaluation to assess the effectiveness of the U.S. Department of the Interior’s (DOI) implementation of a Continuous Diagnostics and Mitigation (CDM) program. We made six recommendations to assist DOI with addressing our findings. These recommendations, if implemented, should result in an improved information security environment and a raised level of risk awareness.

In response to our draft report, the Office of the Chief Information Officer concurred with five recommendations, partially concurred with one recommendation, and stated that it was working to implement or close them. The response included target dates and an action official for each recommendation. We consider these recommendations resolved but not implemented, and one unresolved. 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, inspection, and evaluation reports issued; actions taken to implement our recommendations; and recommendations that have not been implemented.

If you have any questions concerning this report, please do not hesitate to contact me at 202-208-5745.

Table of Contents

Results in Brief	2
Introduction.....	3
Objective	3
Background	3
CDM Program	3
Findings.....	5
Hardware Asset Management	5
Software Asset Management.....	7
Vulnerability Management.....	8
Configuration Settings Management.....	10
Conclusion and Recommendations.....	13
Conclusion.....	13
Recommendations Summary.....	13
Appendix 1: Scope and Methodology.....	17
Scope	17
Methodology	17
Appendix 2: Technical Details.....	18
Appendix 2: Response to Draft Report.....	19
Appendix 3: Status of Recommendations.....	27

Results in Brief

The Continuous Diagnostics and Mitigation (CDM) program, established by Congress in 2013, 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). In this evaluation, our second on Defense in Depth—the process of placing multiple layers of security controls throughout an information technology (IT) system—we found that DOI’s CDM program is immature and not fully effective in protecting high-value IT assets from exploitation.

The CDM program spans 15 continuous diagnostic control areas implemented in 3 phases. DOI initially set September 30, 2014, as the implementation date of Phase 1. DOI has since changed its steady state operational goals by 5 years, to 2019. We assessed the effectiveness of the CDM program for three high-value IT assets operated by three bureaus. Specifically, we assessed the bureaus’ 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 CDM initiative.

We found that DOI’s management practices failed to detect critical and high-risk vulnerabilities on one of its high-value IT assets and left thousands of critical and high-risk vulnerabilities unmitigated for years on three of its high-value assets. In addition, DOI’s capability to identify unauthorized computers or detect and remove obsolete and potentially malicious software (i.e., malware) were inadequate, exposing departmental IT systems to potential compromise. While we found DOI’s practices for initializing its Windows computers to a secure state were effective, DOI did not monitor any of their computers to ensure they remained securely configured over time.

These deficiencies occurred because the Office of Chief Information Officer (OCIO) did not require bureaus to: (1) follow recommended best practices for vulnerability detection or ensure timely vulnerability mitigation; (2) install DOI’s inventory management software on all computers to have a complete hardware inventory; (3) establish and enforce approved software lists to protect systems against malware; or (4) monitor computers to ensure they remained securely configured. Until DOI improves its CDM practices, high-value IT assets will remain at high risk of compromise, the results of which could have a severe or catastrophic effect on departmental operations and cause the loss of sensitive data. We make six recommendations to protect DOI’s high-value IT assets from loss or disruption by strengthening its CDM practices.

Introduction

Objective

We assessed the effectiveness of the U.S. Department of Interior's (DOI) Continuous Diagnostics and Mitigation (CDM) program for three high-value information technology (IT) assets operated by the U.S. Bureau of Reclamation (USBR), the Bureau of Safety and Environmental Enforcement (BSEE), and the U.S. Geological Survey (USGS).

Background

DOI spends about \$1 billion annually on its information technology asset portfolio, which include systems 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.

The systems we selected for evaluation were designated by DOI 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 Federal operations. The loss or disruption of a high-value IT asset may be expected to have a severe or catastrophic 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 3 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 enterprisewide vulnerability and configuration management capabilities.

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 commercial 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 critical 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. 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.

According to the CDM Concept of Operations plan, agencies should have fully implemented all CDM Phase 1 capabilities by June 30, 2014. Moreover, DOI's Office of Chief Information Officer (OCIO) initially established September 30, 2014, for departmentwide implementation of CDM Phase 1. DOI has since changed its steady state operational goals by 5 years, to 2019.

Findings

Based on our review of CDM practices at three of DOI's largest bureaus—USBR, BSEE, and USGS—we found the CDM program ineffective for protecting high-value IT assets from potential loss or disruption. Specifically, we found that for all four CDM Phase 1 controls, the bureaus either failed to implement the control, or implemented the control either incompletely or ineffectively. More than a year after DOI's projected date for fully meeting all Phase 1 requirements, more work needs to be done in order for the CDM program roll out to be a success. Overall, our findings reflect that DOI has not established a centralized capability for overseeing the implementation of IT security initiatives. Finally, this inability to oversee enterprisewide IT security measures will have wide-reaching adverse effects on DOI's capability to protect its computer networks and systems from exploitation.

Hardware Asset Management

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 DOI's 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 OMB officials, which help allocate resources and shape future IT security investments.

We found that DOI does not have an accurate inventory of its computers; therefore, it can neither identify unauthorized and potentially rogue devices, nor effectively manage, monitor, and report the security status of all devices connected to its networks. For example, as part of our technical testing at the 3 subject bureaus, we found that only 520 of 594 (88 percent) of applicable computer servers and workstations we tested were actively managed by the IBM BigFix software (see Figure 1). DOI set a priority deadline for all bureaus to meet a 95 percent goal for asset inventory reporting by the end of FY 2014. This goal coincides with the initial departmental goal of completing CDM Phase 1 by September 30, 2014. DOI has since changed its steady state operational goals by 5 years, to 2019.

High-Value Asset Hardware Inventories by Bureau

Bureau	Number of Computer Servers and Workstations Tested	Computers in IBM BigFix	Percent in IBM BigFix
USGS	95	92	97
BSEE	82	63	77
USBR	417	365	88
Total	594	520	88

Figure 1. A significant number of DOI computers we tested were not actively managed by IBM BigFix.

Source: OIG analysis of DOI data.

Although, OCIO policy requires that bureaus install IBM BigFix software agents on all applicable devices, bureau IT staff we interviewed were confused about which devices were included in the requirement. For example, some of the bureaus we reviewed did not include all domain controllers, public facing systems, development systems, or Linux-based systems, despite OCIO intention that 100 percent of all devices capable of running the agent do so. Moreover, we also learned that not all workstations in our sample were included in the IEM repository because the IBM BigFix software agent was not part of the initial or baseline software configuration for all bureau computer workstations.

The 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. 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. Finally, if only 88 percent of DOI's more than 100,000 IT hardware assets are actively managed, then the security status of more than 10,000 devices is left unknown. Such a situation creates an environment in which risk cannot be effectively measured and mitigated, increasing the likelihood for vulnerabilities to go undetected and uncorrected.

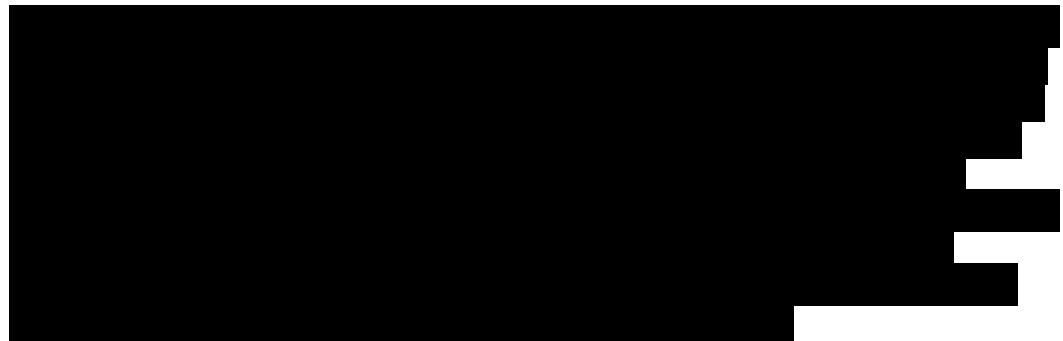
Recommendations

We recommend that DOI's Chief Information Officer:

1. Establish an ongoing process to ensure the inventory of its systems is continually updated and accurate; and
2. Enforce the requirement that all bureaus are to install IBM BigFix agents on all applicable devices to support IBM BigFix as an enterprise hardware inventory solution.

Software Asset Management

We found that DOI failed to establish and implement approved software lists to ensure that unapproved, unsupported, or potentially malicious software (i.e., malware) were not present on bureau computers. Although the bureaus we visited used IBM BigFix to identify software programs installed on their computers, they did not compare installed software to an approved software list to identify unapproved and potentially malicious software. This occurred because OCIO deferred to the bureaus for managing risk related to using unapproved and unsupported software. As such, we found that none of the three bureaus had implemented the software management CDM control.



The longer vulnerabilities remain uncorrected, the greater the risk the vulnerabilities will be exploited by attackers, and the results of which could have a severe adverse effect on bureau operations, assets, or individuals. Moreover, our knowledge of the extent of the unsupported software present is incomplete and compounded the problem because bureaus have not installed IBM BigFix software programs on all computers to have a complete software inventory.

Recommendation

We recommend that DOI's Chief Information Officer:

3. Implement software management controls that—
 - a. maintain an accurate inventory of installed software products;
 - b. recognize and report on unauthorized and unsupported products;
 - c. include procedures for removal of unauthorized products; and
 - d. include planning support for moving away from unsupported products.

Vulnerability Management

Detecting and mitigating vulnerabilities before they can be exploited are essential for protecting DOI's high-value IT assets from loss or disruption. As part of our evaluation, we found that all three bureaus failed to detect critical and high-risk vulnerabilities on their high-value IT assets. Thousands of critical and high-risk vulnerabilities were left unmitigated for years on three of DOI's high-value IT assets. These deficiencies occurred because bureaus did not—

- Use the most effective techniques for vulnerability detection,
- Promptly mitigate discovered vulnerabilities; or
- Quarantine systems when critical and high-risk vulnerabilities went unmitigated.

Finally, because DOI does not have a complete inventory of computers, DOI cannot ensure that vulnerability detection and mitigation process is applied to 100 percent of the computers connected to its networks. As a result, some DOI computers may not undergo vulnerability scanning and thus may contain undetected and uncorrected vulnerabilities.

While we found that all three bureaus had implemented DOI's vulnerability management process, including automated vulnerability discovery and prioritized remediation, we found that USGS failed to consistently use credentialed scanning techniques for vulnerability detection. Credentialed vulnerability scans are performed using administrator-level privileges and provide more comprehensive vulnerability checks than scans without credentials. For this reason, the National Institute of Standards and Technology (NIST) recommends that organizations conduct credentialed scans as part of their vulnerability management program in its Special Publication No. 800-53 Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations" dated April 2013 (NIST SP 800-53). By not performing credentialed scans, thousands of vulnerability checks of varying impact levels that require elevated privileges to verify specific settings and file information are rendered inoperable. Without these checks, critical and

high-impact vulnerabilities will go undetected. As such, not performing credentialed scans increases the probability that critical and high-impact vulnerabilities will remain undetected and uncorrected. This creates an environment in which risk cannot be effectively measured and mitigated, increasing the likelihood that vulnerabilities present on DOI’s high-value IT assets could be exploited by attackers. The result of exploitation could have a severe adverse effect on the availability of mission-critical DOI systems and could result in the loss of sensitive data.

We tested a total of 3,684 devices at the 3 affected bureaus using the credentials of privileged user accounts, which were provided by bureau representatives. Hardware devices tested included computer servers, workstations, and other network devices, such as firewalls and routers, as discovered.

Our tests found almost 100,000 unmitigated critical and high-risk vulnerabilities on 3 of DOI’s high-value IT assets (see Figure 2). More troubling, almost 6,000 of the vulnerabilities we detected had remained unmitigated for years, even though software patches to fix the vulnerabilities were available.

DOI’s 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
BSEE	779	9,025	226
USBR	1,986	69,533	4,920
USGS	919	11,466	660
Total	3,684	90,024	5,806
NOTE: Includes critical and high-risk vulnerabilities where available software patches went unapplied for more than 2 years.			

Figure 2. We identified 90,024 unmitigated critical and high-risk vulnerabilities on DOI’s high-value IT assets, including 5,806 with available software patches.

Source: OIG analysis of DOI data.

A total of 12,931 critical and high-risk [REDACTED] vulnerabilities across 1,644 hosts could be mitigated with the application of vendor-supplied patches. We discovered at least one instance of missing patches from 1999 and 5,195 of the [REDACTED] patches were greater than 2 years old. The U.S. Department of Homeland Security (DHS) explored the correlation between malicious Exploit Kits (EK) and the vulnerabilities they most commonly target in its “Weekly Analytic Synopsis Product” from July 1, 2015. Of the critical vulnerabilities we discovered, 426 are currently being targeted by the top 25 EK’s identified in the DHS report.

Although the OCIO’s security policy requires that bureaus mitigate all critical and high-risk vulnerabilities within 30 days of detection, we found that OCIO did not have an oversight process in place to ensure bureau compliance. In addition, OCIO policy does not include a provision for quarantining computers (i.e., removing the computers from DOI’s network) when critical and high-risk vulnerabilities go unmitigated. Quarantining computers with unmitigated vulnerabilities prevents attackers from exploiting them. Not surprisingly, the longer vulnerabilities remain unmitigated, the greater the risk that the vulnerabilities will be exploited. Compromising DOI’s high-value IT assets by exploiting any of the thousands of vulnerabilities we detected could have a severe adverse effect on bureau operations and result in the loss of sensitive data.

Recommendation

We recommend that DOI’s Chief Information Officer:

4. Incorporate and enforce the following items into its newly evolving vulnerability management program—
 - a. enterprise-level monitoring and reporting of all devices and software packages;
 - b. enterprise-level enforcement of consistent assessment, detection, prioritization and remediation techniques;
 - c. required elevated account credential usage for testing;
 - d. enterprise-level monitoring and bureau accountability for patch deployment; and
 - e. enterprise-level quarantining for critically vulnerable systems that are not patched in a pre-defined timeframe.

Configuration Settings Management

Initializing computer operating systems to a secure state or baseline and ongoing configuration monitoring is essential for maintaining the security of DOI’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 DOI’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 DOI’s IT resources, including its high-value IT assets.

Recommended baselines for secure configuration of selected computer operating systems widely deployed across Federal agencies are defined by the U.S. Government Configuration Baseline (USGCB). For example, the secure USGCB baseline for Windows operating systems recommends 422 configuration settings. OMB Memorandum M-11-33, “FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy

Management,” dated September 14, 2011 requires that Federal agencies adopt USGCB for securing agency computer operating systems. For USGCB covered computer operating systems, DOI has mandated a 100 percent compliance requirement with the recommended USGCB configuration settings, with a wavier process for granting exceptions on a case by case basis. As of the date of this evaluation, OCIO has approved 11 waivers for systems within DOI, and has implemented a process for reviewing and approving waiver applications for the bureaus. To help Federal agencies validate their implementation of USGCB, the Center for Internet Security (CIS) developed an automated scoring tool, the CIS Configuration Assessment Tool.

Using the CIS Configuration Assessment Tool, we verified 200 of the 422 Windows [REDACTED] configuration settings on 392 USBR, USGS, and BSEE workstations and servers, which were part of 3 high-value IT assets. We found that on average, the workstations tested had a 96 percent compliance rate.

The CIS tool can also assess the security of computer operating systems against recommended security baseline settings that are not included in the USGCB standard. We were unable to test any of the USGS servers for compliance with recommended configuration settings without modifying server configurations, which would have potentially degraded the availability of a USGS high-value IT asset. We assessed five [REDACTED] Server [REDACTED] servers at BSEE and found that the server operating system configurations were, on average, 81 percent compliant with the associated CIS benchmark. At USBR, we tested 8 [REDACTED] servers and 11 [REDACTED] Server [REDACTED] servers and found that, on average, the Linux servers were 81 percent compliant and the [REDACTED] servers were 80 percent compliant.

There is no requirement for Federal agencies to adopt a specific or industry-recommended computer operating system configuration settings for operating systems not addressed by USGCB. However, NIST SP 800-53 requires agencies to define secure configuration settings for all of its IT systems. DOI has not defined or enforced secure baseline configuration settings for the thousands of computers running non-USGCB computer operating systems (such as Cisco IOS, Linux, or Mac OS X) used departmentwide. OCIO has deferred to the bureaus the responsibility to establish baseline configuration settings for operating systems not covered by USGCB. As such, bureaus currently perform duplicative configuration analysis and implementation, without use of a standardized departmentwide baseline.

Finally, the bureaus did not monitor operating system configuration settings to ensure computers remained securely configured over time. This occurred 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. Without having ongoing configuration monitoring, DOI increases the risk that their computers operating high-value IT assets may be

compromised. The results of which could potentially have a serious or adverse effect on DOI operations, assets, and individuals.

Recommendation

We recommend that DOI's Chief Information Officer:

5. Establish a departmentwide configuration baseline for each widely used operating system not covered by USGCB that includes a waiver application and approval process; and
6. Monitor computer operating system configuration settings to ensure computers remain securely configured.

Conclusion and Recommendations

Conclusion

The decentralized nature of DOI's operations and its longstanding culture of autonomy have hindered DOI's success in implementing an effective enterprisewide CDM program. These issues occurred because DOI's Chief Information Officer has limited visibility of and control over a majority of DOI's IT investments, operates in an organizational structure that marginalizes the authority of the position, and often cannot consistently enforce security measures, such as CDM, across DOI's computer networks.

Our findings demonstrate that DOI's CDM program is immature. DOI has been slow to implement hardware and software asset management capabilities even though it initially planned to implement all Phase 1 CDM controls by September 30, 2014. DOI has since changed its steady state operational goals by 5 years, to 2019. Without complete and accurate hardware inventories, DOI can neither identify unauthorized devices nor verify that all its computers undergo continuous monitoring to ensure they remain securely configured and vulnerability free. In addition, bureau computers are running unsupported software containing thousands of vulnerabilities because DOI has not established and enforced approved software lists. These vulnerabilities cannot be readily mitigated because vendor provided software patches are no longer available. DOI needs to adopt NIST's recommended practices for vulnerability detection, ensure timely vulnerability mitigation, and quarantine computers when vulnerabilities remain uncorrected. Finally, DOI needs to establish operating system configuration baselines for its population of non-USGCB computers and monitor the configurations to ensure computers remain securely configured.

OMB Memorandum M-14-03 requires all government agencies to implement the remaining CDM phases by the end of fiscal year 2017. In our judgement, DOI will need to strengthen its IT governance practices and formalize roles and responsibilities to ensure that bureaus have effective processes for protecting DOI's high-value IT assets from exploitation.

Recommendations Summary

We recommend that DOI's Chief Information Officer:

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

OCIO Response: OCIO concurred with our recommendation. DOI will rely on a combination of CDM Phase 1 capabilities and processes to ensure the inventory of its systems is continually updated and accurate. Target completion date is June 30, 2018, dependent upon DHS and its contractor.

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

2. Enforce the requirement that all bureaus are to install IBM BigFix agents on all applicable devices to support IBM BigFix as an enterprise hardware inventory solution.

OCIO Response: OCIO concurred with our recommendation. DOI will rely on a combination of CDM Phase 1 capabilities and processes to ensure 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 PMB to track its implementation.

3. Implement software management controls that—
 - a. maintain an accurate inventory of installed software products;
 - b. recognize and report on unauthorized and unsupported products;
 - c. include procedures for removal of unauthorized products; and
 - d. include planning support for moving away from unsupported products.

OCIO Response: OCIO concurred with our recommendation. DOI will rely on a combination of CDM Phase 1 capabilities and processes that will address software asset management controls. Target completion date is June 30, 2019, dependent upon DHS and its contractor. Bureaus and offices will also need the additional time to deconflict software inventories.

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. Incorporate and enforce the following items into its newly evolving vulnerability management program—
 - a. enterprise-level monitoring and reporting of all devices and software packages;
 - b. enterprise-level enforcement of consistent assessment, detection, prioritization and remediation techniques;
 - c. required elevated account credential usage for testing;
 - d. enterprise-level monitoring and bureau accountability for patch deployment; and

- e. enterprise-level quarantining for critically vulnerable systems that are not patched in a pre-defined timeframe.

OCIO Response: OCIO concurred with our recommendation, except for element 4e. DOI will rely on a combination of CDM Phase 1 capabilities and processes to ensure recommendation elements 4a through 4d are implemented. OCIO believes that recommendation 4e, quaranting of systems, may have a detrimental impact on agency systems and is not required as a NIST security control. Target completion date is June 30, 2018, dependent upon DHS and its contractor.

OIG Reply: NIST instructs system owners to select compensating security controls when specific security controls are inadequately implemented to protect the organization. This recommendation is a Defense-in-Depth control layer to compensate for DOI's failure to implement SI-2 Flaw Remediation, with a timely and all inclusive patch management solution. With an accurate inventory of vulnerabilities and the capability to quarantine systems based on an evaluation of any type of threat, DOI can secure its environment while CDM Phase 1 continues to move forward.

We consider recommendations 4a through 4d resolved but not yet implemented and will refer these recommendations to PMB for tracking. We consider recommendation 4e unresolved and will refer to PMB for resolution.

- 5. Establish a departmentwide configuration baseline for computers not covered by USGCB that includes a waiver application and approval process.

OCIO Response: OCIO concurred with our recommendation. DOI will rely on a combination of CDM Phase 1 capabilities and processes to ensure the inventory of its systems is continually updated and accurate. DOI will develop baselines for common operating systems in accordance with NIST SP 800-70r3, National Checklist Program for IT Products – Guidelines for Checklist Users and Developers. Target completion date is June 30, 2018, dependent upon DHS and its contractor.

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.

- 6. Monitor computer operating system configuration settings to ensure computers remain securely configured.

OCIO Response: OCIO concurred with our recommendation. DOI will rely on a combination of CDM Phase 1 capabilities and processes to

ensure the inventory of its systems is continually updated and accurate. DOI will develop baselines for common operating systems in accordance with NIST SP 800-70r3, National Checklist Program for IT Products – Guidelines for Checklist Users and Developers. Target completion date is June 30, 2018, dependent upon DHS and its contractor.

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.

Appendix I: Scope and Methodology

Scope

For this evaluation, our work was limited to the specific procedures and analysis described in the “Rules of Engagement Addendum” completed with each bureau, and was based only on the information made available through May 21, 2015.

Methodology

To accomplish our evaluation objectives, we—

- conducted interviews with subject matter experts at the Office of the Chief Information Officer, the U.S. Bureau of Reclamation, the Bureau of Safety and Environmental Enforcement, and the U.S. Geological Survey;
- developed scripts and network tests for on-site testing to obtain system-specific data;
- compared our results with the data in IBM BigFix; and
- analyzed the findings.

We based initial assessment targets on a range of Internet-Protocol (IP) addresses provided by the bureaus. 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. In order to evaluate a finding without chance of damage or impact to operations, we performed manual testing when possible. Many findings, however, were not testable without having local access to the systems. We reported technical findings that presented a significant concern to warrant additional evaluation and mitigation by the bureaus 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 the bureaus to provide workstation and server configurations and deviations. Then, we used automated tools to determine whether the devices were adequately configured.

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: Office of the Chief Information Officer's Response

The Office of the Chief Information Officer's response to our draft report follows on page 20.




United States Department of the Interior

OFFICE OF THE SECRETARY

Washington, DC 20240

SEP 30 2016

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

From: Sylvia Burns 
Chief Information Officer

Subject: Office of Inspector General, Draft Evaluation 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

The Department of the Interior (DOI), Office of the Chief Information Officer, (OCIO) appreciates the opportunity to review, Office of Inspector General (OIG) Draft Evaluation Report, 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 response to this draft report and as required, Attachment 1 conveys OCIO management comment. Attachment 2 provides a Statement of Actions planned by DOI to implement OIG's recommendations, the responsible officials, and the target dates for implementation. Attachment 3 provides the U.S. Bureau of Reclamation's comments on their Information Security Technical Vulnerability Assessment (ISTVA).

If you have any questions, please contact me at (202) 208-6194. Staff may contact Richard Westmark, Chief, Compliance and Audit Management (CAM) Branch at (202) 513-0749.

cc: Lawrence Ruffin, Chief Information Security Officer
Kris Caylor, Chief, Strategic and Capital Planning & Portfolio Management Branch
Joseph Seger, Acting Director, Information and Technology Management Division
Alexandra Lampros, Financial Specialist, Office of Financial Management
Richard Westmark, Chief, Compliance and Audit Management Branch

Attachments:

1. OCIO Management Comment on OIG Draft Report No. ISD-IN-MOA-0004-2014-I

2. Office of the Chief Information Officer Statement of Actions to Address Office of Inspector General Draft Evaluation Report U.S. Department of the Interior's (DOI) Continuous Diagnostics and Mitigation (CDM) Program Not Yet Capable of Providing Complete Information for Enterprise Risk Determinations Report No. ISD-IN-MOA-0004-2014-I
3. USBR Comments on ISTVA ISD-IN-MOA-0004-2014-E

OCIO Management Comment on OIG Report No. ISD-IN-MOA-0004-2014-I

U. S. Department of the Interior's (DOI) Office of Inspector General (OIG) Draft Report No. ISD-IN-MOA-0004-2014-I references to September 2014 as the DOI's Continuous Diagnostics and Mitigation (CDM) Phase 1 implementation. However, DOI is continuing its CDM Phase 1 work with Department of Homeland Security (DHS). CDM Phase 1 actually has two subphases.

- Delivery Order 1 delivered IBM Endpoint Manager (IEM), formerly BigFix.
- Task Order 2 that will implement other tools to meet the capability goals, (i.e., RES, Forescout, and RSA-Archer Dashboard).

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 DHS-DOI partnership. While the implementation is funded, the sustaining operations and maintenance (O&M) resources are not programmed for 2018 and outyears. Steady-state is an O&M state which follows successful implementation that can demonstrate operational effectiveness and efficiency.

OIG report found that 520 of 594 (88 percent) of applicable computer servers and workstations tested at 3 bureaus between March 2015 and May 2015 were actively managed by IEM. OCIO continues to work with bureaus to extend this capability.

OCIO has been collecting self-reported bureau and office vulnerability data and reporting this information to senior agency political leadership on a recurring basis since summer 2015. Between May 11, 2016 and August 18, 2016 alone, bureaus and offices have reported an aggregate vulnerability reduction of 78%.

OCIO will follow up with the Bureau of Safety and Environmental Enforcement (BSEE), the U.S. Bureau of Reclamation (USBR), and the U.S. Geological Survey (USGS) for their respective OIG Information Security Technical Vulnerability Assessment Report, published during September 2015, No. ISD-IN-MOA-0004-2014-D, ISD-IN-MOA-0004-2014-E, and ISD-IN-MOA-0004-2014-F, respectively. Each of these reports are summarized in the Draft OIG Report No. ISD-IN-MOA-0004-2014-I although none of these separate reports contain specific recommendations.

Office of the Chief Information Officer
Statement of Actions to Address Office of Inspector General Draft Evaluation Report
U.S. Department of the Interior's (DOI) Continuous Diagnostics and Mitigation (CDM)
Program Not Yet Capable of Providing Complete Information for Enterprise Risk
Determinations
Report No. ISD-IN-MOA-0004-2014-I

We recommend that DOI's Chief Information Officer:

Hardware Asset Management

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

Response: The DOI's Office of the Chief Information Officer (OCIO) concurs with this recommendation. 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 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: Lawrence Ruffin, Chief Information Security Officer

Lead Contact & Title: Kris Caylor, Chief, Strategic and Capital Planning & Portfolio Management Branch

Target Completion Date: (June 30, 2018)

Recommendation 2: *Enforce the requirement that all bureaus are to install IBM BigFix agents on all applicable devices to support IBM BigFix as an enterprise hardware inventory solution.*

Response: The DOI OCIO concurs with this recommendation. As noted in the draft report, the OIG found 520 of 594 (88 percent) of applicable computer servers and workstations tested at 3 bureaus between March 2015 and May 2015 were actively managed by IBM BigFix, formerly IBM Endpoint Manager (IEM). Efforts continue to install BigFix on all applicable devices. However, DOI OCIO will rely upon a combination of CDM tools as IEM alone cannot be used to inventory all of the Department's Information Technology (IT) hardware.

Responsible Official & Title: Lawrence Ruffin, Chief Information Security Officer

Lead Contact & Title: Kris Caylor, Chief, Strategic and Capital Planning & Portfolio Management Branch

Target Completion Date: (June 30, 2018)

Software Asset Management

Recommendation 3: *Implement software management controls that—*

- a. maintain an accurate inventory of installed software products;*
- b. recognize and report on unauthorized and unsupported products;*
- c. include procedures for removal of unauthorized products; and*
- d. include planning support for moving away from unsupported products.*

Response: The DOI OCIO concurs with this recommendation. CDM Phase 1 is still being implemented and upon reaching steady-state operations will incorporate capabilities and processes for software asset management controls. Specifically, the DOI OCIO 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, DOI OCIO will work with bureaus and offices to ensure implementation of effective (c.) procedures for removal of unauthorized products and (d.) planning support for moving away from unsupported products. The DOI OCIO, bureaus, and offices will rely upon a combination of CDM tools since 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 implementation of tools. Further, bureaus and offices will need this longer timeframe, that is 2019, to deconflict software inventories while maintaining continuity of services.

Responsible Official & Title: Lawrence Ruffin, Chief Information Security Officer

Note: OCIO Director Information and Technology Management Division will be the responsible official for corrective actions for unsupported products.

Lead Contact & Title: Kris Caylor, Chief, Strategic and Capital Planning & Portfolio Management Branch

Target Completion Date: (June 30, 2019)

Vulnerability Management

Recommendation 4: *Incorporate and enforce the following items into its newly evolving vulnerability management program—*

- a. enterprise-level monitoring and reporting of all devices and software packages;*

- b. enterprise-level enforcement of consistent assessment;*
- c. required elevated account credential usage for testing;*
- d. enterprise-level monitoring and bureau accountability for patch deployment; and*
- e. enterprise-level quarantining for critically vulnerable systems that are not patched in a pre-defined timeframe.*

Response: The DOI OCIO concurs with this recommendation except for 4.e. CDM Phase 1 is still being implemented and upon reaching steady-state operations, the OCIO will incorporate CDM capabilities and processes for vulnerability management. Specifically, DOI OCIO will use CDM Phase 1 capabilities to provide (a.) enterprise-level monitoring and reporting of all devices and software packages; (b.) enterprise-level enforcement of consistent assessment; (c.) RA-5(5) Privileged Access Vulnerability Scanning in accordance with NIST Special Publication (SP) 800-53r4 supplemental guidance; (d.) monitoring and bureau accountability for patch deployment in accordance with the NIST SP 800-40 Revision 3, *Guide to enterprise Patch Management Technologies*, published July 2013. The OCIO, bureaus, and offices will rely upon a combination of CDM tools as one single tool cannot satisfy the entirety of this recommendation. DOI OCIO will replace the current scanning solution with a new enterprise tool to satisfying CDM Phase 1 vulnerability capability. The processes and procedures will be developed after the implementation of tools.

Responsible Official & Title: Lawrence Ruffin, Chief Information Security Officer

Lead Contact & Title: Kris Caylor, Chief, Strategic and Capital Planning & Portfolio Management Branch

Target Completion Date: (June 30, 2018)

Configuration Settings Management

Recommendation 5: *Establish a department wide configuration baseline for each widely used operating system not covered by USGCB that includes a waiver application and approval process.*

Response: The DOI OCIO concurs with this recommendation. CDM Phase 1 is still being implemented and upon reaching steady-state operations will incorporate capabilities and processes to monitor configuration baseline for widely used operating systems. The United States Government Configuration Baseline (USGCB) conforms to NIST SP 800-70 Revision 3, *National Checklist Program for IT Products: Guidelines for Checklist Users and Developers*, published December 2015. DOI OCIO will continue to use USGCB where applicable and the SP 800-70 otherwise for widely used operating systems not covered by USGCB. Both USGCB and NIST SP 800-70 allow for documented and approved deviations. The DOI OCIO, bureaus and offices will rely upon a combination of CDM tools and techniques 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 implementation of tools.

Responsible Official & Title: Lawrence Ruffin, Chief Information Security Officer

Lead Contact & Title: Kris Caylor, Chief, Strategic and Capital Planning & Portfolio Management Branch

Target Completion Date: (June 30, 2018)

Recommendation 6: *Monitor computer operating system configuration settings to ensure computers remain securely configured.*

Response: The DOI OCIO concurs with this recommendation. CDM Phase 1 is still being implemented. Upon reaching steady-state operations, DOI OCIO will incorporate capabilities and processes to monitor computer operating system configuration settings to ensure computers remain securely configured. DOI OCIO, bureaus, and offices 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 implementation of tools.

Responsible Official & Title: Lawrence Ruffin, Chief Information Security Officer

Lead Contact & Title: Kris Caylor, Chief, Strategic and Capital Planning & Portfolio Management Branch

Target Completion Date: (June 30, 2018)

Appendix 3: Status of Recommendations

In its response to our draft report, the Office of the Chief Information Officer concurred with five recommendations, partially concurred with one recommendation and stated that it was working to implement or close them. The response included target dates and an action official for each recommendation (see Appendix 3). We consider these recommendations resolved but not implemented.

Recommendations	Status	Action Required
1, 2, 3, 4a, 4b, 4c, 4d, 5, 6	Resolved but not implemented	We will refer these recommendations to the Office of Policy, Management and Budget to track their implementation.
4e	Unresolved	We will refer this recommendation to the Office of Policy, Management and Budget for resolution.

