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

Weaknesses in the [redacted] System Leave Assets at Increased Risk of Attack

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

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

MAR 30 2021

Memorandum

To: William E. Vajda
Chief Information Officer

From: Mark Lee Greenblatt
Inspector General

Subject: Final Evaluation Report – *Weaknesses in the* [redacted] *System Leave Assets at Increased Risk of Attack*
Report No. 2019-ITA-003

This memorandum transmits our evaluation report on the U.S. Geological Survey's progress in implementing Phase 1, "Manage Assets," of the three-phased Governmentwide Continuous Diagnostics and Mitigation program for the [redacted] system.

We will refer Recommendations 1 – 8 to the Office of Policy, Management and Budget to track their implementation and report to us on their status. In addition, we will notify Congress about our findings and we will report semiannually, as required by law, on actions you have taken to implement the recommendations and on recommendations that have not been implemented. We will also post a public version of this report on our website.

If you have any questions, please contact me at 202-208-5745.

Contents

Results in Brief

Protecting Federal computer networks and data from cyber threats remains one of the most serious economic and national security challenges. Moreover, managing and securing IT networks and operations continues to be one of the top management and performance challenges facing Federal agencies. To help Federal agencies strengthen their cyber defenses and improve resiliency in response to escalating cyber threats, Congress established the Continuous Diagnostics and Mitigation (CDM) program in 2013. The CDM program is a dynamic approach to fortifying defenses against cyber threats and helping agencies become more resilient in the face of attacks against Government networks and systems, including those of the U.S. Department of the Interior (DOI).

We evaluated the U.S. Geological Survey's (USGS') implementation of Phase 1, "Manage Assets," for the [redacted] system. Specifically, we evaluated the USGS' progress in developing inventories of computer hardware and software; limiting the use of ports, services, and protocols; managing operating system configurations; and detecting and mitigating technical vulnerabilities. We captured and analyzed computer network traffic and computer memory to search for hidden malware and other indicators of compromise.

Our testing revealed control deficiencies for hardware and software asset management and configuration management. For example, USGS' implementation of the CDM program for the [redacted] system did not effectively protect from potential loss of data or disruption of services. Specifically, the DOI did not require bureaus and offices to maintain accurate hardware asset inventories for information systems, which prevented them from monitoring key security metrics through the DOI's CDM dashboard. The absence of a requirement for bureaus and offices to maintain accurate system inventories diminished the effectiveness of other required CDM controls, as there is no way to monitor security metrics for DOI-operated systems that are not accounted for within hardware asset inventories. Such practices could and, in fact did, leave many systems exposed to vulnerabilities that could otherwise be easily patched with known fixes. We also found that the USGS failed to require systems to operate with only those ports, protocols, and services necessary for essential operations, which increased their vulnerability to attack.

These deficiencies occurred because: (1) the DOI failed to require bureaus and offices to associate hardware assets to the information systems they comprise, thereby enabling monitoring of key security metrics through the CDM dashboard; (2) the DOI failed to establish and implement CDM controls to prevent unapproved, unsupported, or potentially malicious software from being installed and executed; (3) USGS IT staff did not initialize operating system configurations on Windows servers to a secure state or monitor them for ongoing changes to baseline configurations; and (4) the USGS did not enforce the restriction of ports, services, and protocols at the host level for the [redacted] system.

Until the DOI strengthens its CDM program implementation, IT assets such as the [redacted] system will remain at high risk of compromise, which could have a severe adverse effect on departmental operations and result in the loss of sensitive data. We make three recommendations to the DOI and five recommendations to the USGS to strengthen CDM controls to fortify

defenses against cyber threats. In response to our draft report, the DOI and the USGS concurred with all eight recommendations and identified the steps that they are taking to implement them.

Introduction

Objective

Our objective was to assess the U.S. Geological Survey's (USGS') progress in implementing Phase 1, "Manage Assets," of the three-phased governmentwide Continuous Diagnostic Mitigation (CDM) program for the [redacted] system. We evaluated the USGS' progress in developing inventories of computer hardware and software; managing operating system configurations; limiting the use of ports, services, and protocols; and detecting and mitigating technical vulnerabilities.

Appendix 1 provides further details on our scope and methodology.

Background

The CDM program 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, thereby enabling IT personnel to mitigate the most significant problems first. Congress established the CDM program in 2013 to provide adequate, risk-based, and cost-effective cyber security capabilities to more efficiently allocate 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.

When the CDM program was initially rolled out across the Federal Government, the DOI was part of the initial wave for implementation in 2013. To date, the DOI has spent approximately $28 million on the CDM program and plans to spend $43 million in fiscal years 2020 and 2021.

One of the programs that receives funding from the DOI for the CDM program is the [redacted] Project, [redacted] The DOI categorizes the [redacted] system as a high-value IT asset. High-value IT assets often contain sensitive data or support mission critical operations, and their loss or disruption could have a serious adverse effect on agency operations.

Hardware Asset Management

An organization-wide inventory of computers 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 increase the effectiveness of an IT security program by certifying that all of an organization's IT assets undergo continuous monitoring to ensure they remain securely configured and free of vulnerabilities.

As part of implementing this Hardware Asset Management CDM control, the DOI selected [redacted] as its enterprise-wide solution for managing hardware inventories. To develop inventories of authorized computers, [redacted] agents (software programs) are first installed on all computers that are part of a DOI or bureau computer system. Once installed, the agents register DOI computers to a central repository. The repository serves as an authoritative departmentwide hardware inventory. The data in the repository is used for monitoring, tracking, and reporting key IT security metrics to senior officials from the DOI, the U.S. Department of Homeland Security, and Office of Management and Budget. All of these officials help allocate resources and prioritize mitigation efforts that strengthen an organization's IT security posture.

Software Asset Management

A software asset can be as small as a line of source code or as large as a software suite made up of multiple products, thousands of individual executables, and many lines of code. Software Asset Management (SWAM) provides an organization with visibility into the software installed and operating on its network so the organization can appropriately manage authorized software and remove unauthorized software. Proper management of software assets begins with lists of authorized (whitelist) and unauthorized (blacklist) software products and executables. Some lists may be defined globally, such as known executable files that contain malicious code, while others are defined by device role, such as authorized software products.

Configuration Management

Configuration management is the process of assessing and modifying settings as necessary to ensure that IT assets such 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[1] published recommended configuration settings, called benchmarks, for securing a wide variety of computer operating systems.

Initializing a computer's operating system to a secure state does not provide ongoing protection against exploitation. Accordingly, ongoing configuration monitoring is essential to maintain the security of the DOI's high-value IT assets. Because operating system configurations can change

[1] The Center for Internet Security is a nonprofit organization responsible for the CIS Controls and Benchmarks.

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.

Information systems should also be configured to provide only essential capabilities to accomplish their tasks. This includes prohibiting or restricting the use of ports, protocols, and services to only those necessary to accomplish tasks.[2] While systems could use a total of 65,536 ports, only a very limited number of ports are actually required for a system to operate based on the network services needed for system functionality.

Unnecessary ports that are left open on a system increase the number of possible pathways that an attacker could use to exploit a system to perform malicious activities such as stealing or destroying sensitive data. Any ports that must be opened for a system's functionality should be documented as a baseline for authorizing allowed open ports and to support continuous monitoring. This baseline should be periodically reviewed so that only open ports are authorized to align with required changing system functionality over time. Periodic review would also prevent unnecessary ports from remaining open, limiting the attack surface of the system.

Vulnerability Management

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

Threat Hunting

Combating advanced cyber threats requires acknowledging that traditional cyber defenses—firewalls, intrusion detection systems, and antivirus software—often fail to deter or detect sophisticated malware. As a best practice, organizations should assume the systems that operate infrastructure are already potentially compromised and search the computer networks that operate infrastructure for hidden malware. The objective of this approach is to track and disrupt cyber adversaries as early as possible in the attack sequence and to measurably improve the speed and accuracy of organizational responses. This proactive approach is referred to as "threat hunting," which includes using techniques such as capturing and analyzing computer network traffic for malicious communications and dissecting computer memory to find malware.

Network forensics, an integral part of threat hunting, is the investigation of network traffic patterns and data captured in transit between computing devices to search for compromised systems. Network traffic is typically acquired through the use of a network tap or port mirror to

[2] Ports are communication paths into a system component for network services.

monitor all traffic flowing between networks of different trust levels. Analysts specifically look for indicators of compromise. For example, one indicator could be signs of command and control beaconing where a malicious software program could be communicating back to a threat actor's machine. Another potential indicator is suspicious network connections such as systems that should not be communicating with one another. Network forensics can be used as a method to identify which systems may have been compromised through the presence of anomalous network activity.

Memory forensics, another integral part of threat hunting, is the analysis of volatile data in a computer's memory dump. It involves acquiring RAM (random access memory) off network devices and then analyzing its contents to identify artifacts that may indicate compromise. It can provide unique insights into runtime system activity, including open network connections and recently executed commands or processes. In many cases, critical data pertaining to attacks or threats exist in memory such as network connections, account credentials, chat messages, injected code fragments and internet history. Memory forensics is an important component of threat hunting, as many network-based security solutions, such as firewalls and anti-virus tools, are unable to detect malware written directly into a computer's physical memory or RAM.

Prior Evaluations of the DOI's CDM Program

We previously evaluated the DOI's CDM Program in two prior reports. In our 2016 evaluation, we found that the CDM program at the DOI's [redacted] was immature and not fully effective in protecting the [redacted] IT systems owned by the [redacted] from potential exploitation.[3] In our 2017 evaluation, we found that the DOI's CDM program was ineffective for protecting high-value IT assets from potential loss of data or disruption of services at three of the DOI's largest bureaus—the Bureau of Reclamation, the Bureau of Safety and Environmental Enforcement, and the U.S. Geological Survey (USGS).[4]

[3] *Information Technology Security Weaknesses at a Core Data Center Could Expose Sensitive Data* (Report No. 2016-ITA-021), dated February 2017.

[4] *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), dated September 2016.

Findings

We found that the CDM program for [redacted] was ineffective for protecting high-value assets from potential loss of data and disruption of services. Specifically, we found that the DOI and the USGS failed to implement the CDM Phase 1 controls completely and effectively. These issues occurred because the Office of the Chief Information Officer (OCIO) and USGS personnel did not provide effective oversight of the CDM program, particularly for high-value assets, leaving systems vulnerable to cyber attacks and malicious use.

As hardware asset management is one of four controls for Phase 1, we attempted to validate the completeness and accuracy of the hardware inventory for the [redacted] system by tracing this data to the DOI's CDM dashboard. However, we were unable to do so because we encountered significant data quality issues.

We also found that the DOI did not implement software blacklists or whitelists to help ensure that unapproved, unsupported, or potentially malicious software was not present on [redacted] computing devices. In addition, we found that the USGS did not implement the configuration management controls for CDM effectively. Specifically, the USGS does not prohibit or restrict the use of ports, protocols, and services for the [redacted] system and did not establish and maintain secure operating system configurations for the [redacted] computer servers. We also found that the USGS did not timely mitigate vulnerabilities on USGS-owned [redacted] assets.

The USGS Did Not Follow Inventory Management Requirements

The DOI Did Not Establish the HWAM Control in [redacted]

We found that the DOI's implementation of the hardware asset management control did not support the National Institute of Standards and Technology (NIST) requirement to track and report the security posture of assets by individual information system. The DOI did not require bureaus and offices to associate hardware assets with the information system within [redacted] the DOI's hardware asset management solution, to enable ongoing monitoring of key security metrics through the DOI's CDM dashboard. Without real-time awareness of the status of key security controls within the hardware asset repository, bureaus and offices cannot prioritize activities such as vulnerability mitigation and incident response to ensure the confidentiality, integrity, and availability of their information systems.

At the time of our [redacted], we requested that USGS IT security staff produce a hardware asset inventory for the [redacted] system from [redacted] The USGS could not do so. Instead, USGS IT security staff were required to add a data element to "tag" each [redacted] hardware component in order to generate a [redacted] inventory report. Although we confirmed the accuracy of the [redacted] hardware asset repository at the [redacted] using [redacted] network traffic data we collected while onsite, USGS IT security staff had to manually compile an

inventory of [redacted] assets that should have been readily available and generated by [redacted] without the need to manually "tag" each [redacted] hardware component.

The objective of the CDM hardware asset management control is to accurately inventory and report on the security posture of all hardware devices, such as computers, routers and firewalls. Phase 1 of the CDM program requires implementation of the Configuration Management-8 control (CM-8), "Information System Component Inventory," from NIST Special Publication 800-53, Revision 4, *Security Controls for Federal Information Systems and Organizations*. CM-8 requires that the Department develop and document an inventory that accurately reflects the current information system components, including those within the designated authorization boundary. Further, CM-8 requires that the inventory be at the level of granularity deemed necessary for tracking and reporting and be accountable for information system components. In addition, CM-8 requires that inventories include system-specific information to support tracking and Bureau reporting of key security metrics such as vulnerability data by information system.

Recommendation

We recommend that the DOI:

1. Establish an ongoing process to ensure bureaus provide complete information for the hardware asset repository and enable the DOI's centralized hardware asset management system to track and report key security metrics by information systems, including systems designated as high-value assets

The DOI Did Not Implement the Required SWAM Control

We found that, although the USGS has a software approval process in place for requesting new or additional software to be installed on [redacted] devices with Windows operating systems, USGS IT security personnel had not implemented software blacklists or whitelists to help ensure that unapproved, unsupported, or potentially malicious software are not present on [redacted] computing devices. Application whitelisting is the implementation of an authorized software list to allow only approved software products to be installed on the system. Application blacklisting is the implementation of an unauthorized software list to enable validation for unauthorized software against this listing. Control over software installation helps to prevent unauthorized software products from being installed because they are checked against whitelisting or blacklisting applications.

The intent of the CDM's Software Asset Management (SWAM) capability is to address attacks that result from unauthorized software and from malicious software. According to USGS IT security personnel, the DOI has not implemented a CDM SWAM capability. The DOI's CDM Program Manager confirmed that a CDM tool is not in place for software blacklisting. This is inconsistent with Phase 1 of the CDM program, which requires implementation of the CM-7 "Least Functionality" control from NIST 800-53, Revision 4.
To identify unauthorized software programs (designated as Federal Information Processing Standard Publication 199 Moderate), CM-7(4), "Unauthorized Software/Blacklisting" from

NIST 800-53, Revision 4, requires the USGS to (1) identify software programs not authorized to execute on the information system; (2) employ an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the information system; and (3) review and update the list of unauthorized software programs.

The Department of Homeland Security initially approved a CDM tool, Ivanti, for software whitelisting and blacklisting across the DOI. However, before deployment, the DOI found that Ivanti had a critical flaw—the software provided whitelisting and blacklisting capabilities for client computers (e.g., laptops, workstations, etc.) but was incompatible with computer servers. This limitation caused the DOI to engage with the Department of Homeland Security to acquire a new CDM tool for software blacklisting and whitelisting that was compatible with the DOI's entire computer environment. At the time of our evaluation, however, the DOI had not selected a new software blacklisting and whitelisting tool and had not established and implemented CDM controls over unapproved, unsupported, or potentially malicious software.

Recommendations

We recommend that the DOI:

2. Select and implement a CDM SWAM tool that is compatible with the DOI's computer environment

3. Establish, implement, and continuously review and update approved software lists (blacklists and whitelists) to ensure that unapproved, unsupported, or potentially malicious software is not present on bureau computer networks

The USGS Did Not Restrict Ports, Services, and Protocols

We found that the USGS did not prohibit or restrict the use of ports, protocols, and services for the [redacted] system. We captured 21 terabytes of network traffic at both the [redacted] system. We analyzed the network traffic for ports being used for network communications, and we identified 208 unique, active ports at the [redacted] and 84 unique, active ports at [redacted].[5] USGS IT security personnel could not provide a documented listing showing which ports were authorized.

USGS IT security personnel stated that they do not restrict usage of ports, protocols, and services at the host level, as they are relying on the firewall devices to block ports and services. While blocking ports and services through firewall devices may stop malicious traffic, it will not prevent attackers from exploiting protocols and active ports that should not be active on devices.

[5] [redacted]

Federal agencies, however, are required to adhere to NIST security control requirements, which include documenting ports and services that are necessary for operations. Phase 1 of the CDM program requires implementation of the CM-7 "Least Functionality" control from the NIST SP 800-53, Revision 4. CM-7 requires that the DOI configure information systems to provide only essential capabilities and limit the use of functions, ports, services, and protocols to those supporting essential organizational operations.

This deficiency occurred because the USGS did not have a list of authorized ports, services, and protocols and did not enforce the restriction of ports, services, and protocols at the host level for the [redacted] system. Authorization should only be granted for the functions necessary for the system to accomplish its tasks. The "attack surface" of a system—the points that an attacker might target when compromising a system—increases when the use of authorized ports, services, and protocols is not restricted. Reducing system functions to only those necessary to accomplish organizational objectives can minimize risk, resulting in fewer attack vectors and leaving fewer options for attack.

Recommendations

We recommend that the USGS:

4. Establish a listing of authorized ports, services, and protocols for the [redacted] system and restrict the use of unauthorized ports, protocols, and services at the host level for the [redacted] system

5. Monitor systems to ensure that only authorized ports, services, and protocols are used at the host level

The USGS did Not Establish Secure Operating System Configurations

We found that the USGS did not establish and maintain secure operating system configurations for the [redacted] computer servers running [redacted] We tested 11 Windows [redacted] servers using the Center for Internet Security Configuration Assessment Tool and observed a 39 percent average compliance rate.

NIST 800-53, Revision 4, requires the DOI to establish and document configuration settings for IT products employed within the information system using organization-defined security configuration checklists that are the most restrictive while meeting operational needs. Initializing computer operating systems to a secure state or baseline and ongoing configuration monitoring are essential for maintaining the security of USGS' high-value IT assets. The DOI's low compliance rate (39 percent) does not meet the criteria of securing the system by making sure the operating system configurations reflect the most restrictive mode as a countermeasure for protecting the high-value asset from potential loss of data or disruption or disruption of services.

The low compliance rate occurred because USGS IT staff did not initialize the operating system on [redacted] servers to a secure state or monitor the operating system's configurations to ensure the servers remained securely configured. Taking these additional steps is essential for maintaining the security of USGS' high-value IT assets. Computer operating systems that are improperly configured are susceptible to compromise and thus may potentially be used by intruders to gain unauthorized access to bureau computer networks. Once inside, the intruder can use the compromised computer to exploit other weaknesses, which could result in the loss or impairment of USGS' IT assets, including its high-value IT assets.

Recommendations

We recommend that the USGS:

6. Establish a process to ensure that operating system configuration settings are defined and consistently applied to hardware components

7. Monitor systems to ensure ongoing compliance and consistent application of configuration settings for all systems

The USGS Did Not Timely Mitigate Some Vulnerabilities on USGS-Owned [redacted] Assets

Although we found that the USGS performed periodic vulnerability assessments and mitigated a majority of vulnerabilities in accordance with NIST requirements, two USGS-owned [redacted] did not have patches applied in a timely manner. Specifically, we found 25 high-risk vulnerabilities associated with the two identified assets. In some instances, patches were not applied timely due to limited availability of USGS security staff during the 35-day furlough period that occurred from December 22, 2018, to January 25, 2019. In some instances, the patches were applied when the identified assets were taken off-line in the evenings. We confirmed that the vulnerabilities identified were appropriately patched by the next subsequent vulnerability scan in February 2019.

Phase 1 of the CDM program requires implementation of the Risk Assessment-5 control (RA-5), "Vulnerability Scanning," from the NIST SP 800-53, Revision 4. RA-5 requires the DOI to scan for vulnerabilities on a monthly basis and remediate critical and high-risk vulnerabilities within 30 days and medium-severity risks within 90 days of identification.

Computer operating systems that go unpatched with unmitigated vulnerabilities increase the attack surface and the likelihood that an intruder could compromise and gain unauthorized access to systems. This, in turn, could result in the loss or impairment of USGS' IT assets, including its high value IT assets.

To validate that the vulnerabilities were adequately remediated, we performed threat hunting procedures to confirm the presence of threat actors on [redacted]. Our

limited procedures to hunt for threats and indicators of compromise included the collection and analysis of network traffic and computer memory. We reviewed 21 terabytes of network traffic to identify anomalous behavior such as command and control beaconing traffic, long connections, malicious DNS traffic and user agent strings. We did not identify any active threats in the network traffic for the period analyzed. In addition, we collected 182 gigabytes of RAM from 14 computer servers and workstations for the high-value asset located at the [redacted] Center. To determine whether these computers and servers had evidence of compromise, we analyzed the RAM for anomalies such as rogue processes, Dynamic Link Libraries (DLLs) and handles, network artifacts (e.g., suspicious ports and connections), evidence of code injection, and signs of rootkits[6]. Based on our analysis, we did not identify indicators of compromise or malware on these devices at the time of our project.

Recommendation

We recommend that the USGS:

8. Ensure that the process to identify and mitigate high-risk vulnerabilities within 30 days, as required by OCIO policy, is followed.

[6] A rootkit is a malicious piece of software that grants a remote operator complete access to a computer system.

Conclusion and Recommendations

Conclusion

Since the DOI's CDM program began 7 years ago, and after spending $28 million, the DOI has made little progress in implementing Phase 1 of the CDM program for the [redacted] system. The DOI must fully implement Phase 1 controls of the CDM program—including hardware asset management, software asset management, and configuration management controls—before it can move forward to successfully implement future required phases of the program.

We found that the DOI did not require bureaus and offices to maintain accurate hardware asset inventories for information systems, which prevented them from monitoring key security metrics through the DOI's CDM dashboard. The lack of any requirement for bureaus and offices to maintain accurate system inventories diminished the effectiveness of other required CDM controls, as there is no way to monitor security metrics for DOI-operated systems that are not accounted for within hardware asset inventories. Such practices could leave many systems exposed to vulnerabilities that could otherwise be easily patched with known fixes.

We also found that the DOI did not implement software blacklists or whitelists to help ensure that unapproved, unsupported, or potentially malicious software was not present on [redacted] computing devices. In addition, we found that the USGS failed to require systems to operate with only those ports, protocols, and services necessary for essential operations, leaving them vulnerable to attack. Furthermore, we found that the USGS did not timely mitigate vulnerabilities on USGS-owned [redacted] assets.

These deficiencies occurred because: (1) the DOI failed to require bureaus and offices to associate hardware assets to the information systems they comprise to enable monitoring of key security metrics through the CDM dashboard; (2) the DOI failed to establish and implement CDM controls to prevent unapproved, unsupported, or potentially malicious software from being installed and executed; (3) the USGS did not enforce the restriction of ports, services, and protocols at the host level for the [redacted] system; and (4) USGS IT staff did not initialize operating system configurations on Windows servers to a secure state or monitor them.

The DOI plans to spend an additional $43 million over fiscal years 2020 and 2021. Until the DOI strengthens its CDM program implementation, IT assets such as the [redacted] system will remain at high risk of compromise, which could have a severe adverse effect on departmental operations and cause the loss of sensitive data.

In response to our draft report, the DOI and the USGS concurred with all eight recommendations and identified steps that they are taking to implement them. They also provided a description of the actions they plan to take, target dates for completion, and the officials responsible for implementation. The DOI's full response is included in Appendix 2.

Recommendations Summary

We recommend that the DOI:

1. Establish an ongoing process to ensure bureaus provide complete information for the hardware asset repository and enable the DOI's centralized hardware asset management system to track and report key security metrics by information systems, including systems designated as high-value assets

2. Select and implement a CDM SWAM tool that is compatible with the DOI's computer environment

3. Establish, implement, and continuously review and update approved software lists (blacklists and whitelists) to ensure that unapproved, unsupported, or potentially malicious software is not present on bureau computer networks

We recommend that the USGS:

4. Establish a listing of authorized ports, services, and protocols for the [redacted] system and restrict the use of unauthorized ports, protocols, and services at the host level for the [redacted] system

5. Monitor systems to ensure that only authorized ports, services, and protocols are used at the host level

6. Establish a process to ensure that operating system configuration settings are defined and consistently applied to hardware components

7. Monitor systems to ensure ongoing compliance and consistent application of configuration settings for all systems

8. Ensure that the process to identify and mitigate high-risk vulnerabilities within 30 days, as required by OCIO policy, is followed.

Appendix 1: Scope and Methodology

Scope

The scope of this evaluation includes the U.S. Geological Survey's (USGS') Phase 1 "Manage Assets" of the Continuous Diagnostics and Mitigation (CDM) program implementation for the [redacted] system, operated by the USGS. We evaluated the USGS' progress in developing inventories of computer hardware and software, managing operating system configurations, and detecting and mitigating technical vulnerabilities. We also evaluated the USGS' malicious code protections over its high-value assets by developing scripts and network tests to obtain network and system data. We conducted our technical testing between March 25, 2019 and August 30, 2019.

Methodology

To accomplish our evaluation objectives, we:

- [redacted]
- [redacted]
- Reviewed system security policies and procedures
- Assessed system configurations
- Assessed various system-generated logs
- Executed PowerShell scripts to pull artifacts for analysis
- Compared the network traffic data to the USGS' system inventory to determine whether it had a complete IT asset inventory for [redacted]
- Analyzed network traffic for the presence of malware
- Analyzed RAM captures for the presence of malware

We assessed the DOI's compliance with selected controls from the National Institute for Standards and Technology Special Publication (SP) 800-53, Revision 4, *Security Controls and Assessment Procedures for Federal Information Systems and Organizations*.

Prior to technical testing, we created, and the USGS reviewed and approved, a Rules of Engagement document to govern the terms of the assessment activities. Our work was limited to noninvasive testing and was based on information the USGS provided.

Network forensics is the capture, recording, and analysis of network events in order to discover the source of security attacks or other problem incidents. As part of our technical testing, we collected more than 21 terabytes of network traffic from the [redacted] We analyzed the network traffic data using open-source tools—Zeek, RITA (Real Intelligence Threat Analytics), and Wireshark—to identify any indicators of compromise, which are artifacts observed on a network or operating system that, with high confidence, indicate a computer intrusion may have occurred.

Zeek is an open-source network security monitor tool used to detect and identify the presence of malware from anomaly-based analysis. Its analysis engine converts network traffic captured into a series of events, which we used with its own scripting language. RITA is an open-source framework for network traffic analysis and supports the ingestion of Zeek logs to detect indicators of command and control beaconing, Domain Name System (DNS) tunneling and IP address blacklist checking. Wireshark is a widely used network protocol analyzer used to analyze network packet captures for anomalies. We analyzed all network traffic for evidence of command and control beaconing and strobing, malicious DNS traffic, blacklisted IP addresses or hostnames, malicious long connections and HTTP user agents. In addition, we used network forensics to analyze asset inventory and assess open ports, services, and protocols present in network traffic.

Operations performed on a computing device by both legitimate users and adversaries modify the device's memory (RAM), leaving evidence of their actions on the device. Memory forensics is an integral part of threat hunting and involves acquiring RAM from network devices and analyzing its contents to identify artifacts that may indicate compromise— such as sophisticated malware, malicious code and processes, and abnormal network connections—and assess the impact of the compromise on the network.

As part of our technical testing, we collected 182 gigabytes of RAM from 14 computer servers and workstations for the high-value asset located at the [redacted] Center and 318 gigabytes of RAM from 17 servers and workstations at [redacted]. We used open-source tools, including the SANS Investigative Forensics Toolkit (SIFT) workstation, Volatility, RegRipper, Bulk Extractor, Strings, and Wireshark to extract digital artifacts from the RAM for analysis. In order to determine whether these computers and servers had evidence of compromise, we analyzed the RAM for anomalies such as rogue processes, Dynamic Link Library (DLLs) and handles, network artifacts (e.g., suspicious ports and connections), evidence of code injection, and signs of rootkits. Based on our analysis, we did not identify indicators of compromise or malware on these devices at the time of our project.

We conducted our 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 performed provides a reasonable basis for our conclusions and recommendations.

Appendix 2: Response to Draft Report

The U.S. Department of the Interior's response to our draft report follows on page 18.

United States Department of the Interior

OFFICE OF THE SECRETARY
Washington, DC 20240

February 10, 2021

Memorandum

To: Mark Lee Greenblatt
Inspector General

From: William E. Vajda
Chief Information Officer

WILLIAM VAJDA Digitally signed by WILLIAM VAJDA
Date: 2021 02 10 11:02:16 -05'00'

Subject: Office of the Chief Information Officer Response to Draft Evaluation Report – *Weaknesses in the* [redacted] *System Leave Assets at Increased Risk of Attack*, Report No. 2019-ITA-003

Please find attached the Office of the Chief Information Officer (OCIO) Management Response. We listed all attachments below for your reference and review.

I am pleased to report that the U.S. Department of the Interior concurs with all the Office of Inspector General's (OIG) recommendations. Each recommendation is assigned a Deputy or Associate Chief Information Officer as the responsible official and a target completion date. We appreciated working with you and your office on these recommendations.

If you have questions, please contact me at [redacted] Staff may contact Jack Donnelly, Chief Information Security Officer, at [redacted].

Attachment: OCIO Management Response for OIG Draft Report No. 2019-ITA-003

cc: Jack Donnelly, Chief Information Security Officer
Deputy Chief Information Officers
Associate Chief Information Officers
Richard Westmark, Chief, OCIO Compliance Management Section
Dr. Chadrick Minnifield, Chief, Internal Control and Audit Follow-up, Office of Financial Management
Alan T. Wiser, USGS Associate Chief Information Security Officer

Attachment: OCIO Management Response for OIG Draft Report No. 2019-ITA-003

OIG Recommendations for the U.S. Department of the Interior (DOI, Department):

Recommendation 1. Establish an ongoing process to ensure bureaus provide complete information for the hardware asset repository and enable the DOI's centralized hardware asset management system to track and report key security metrics by information systems, including systems designated as high-value assets.

> **OCIO Response:** Concur. Bureaus and offices across the Department are to update and associate hardware within the DOI networks limited by the capabilities of the Continuous Diagnostic and Mitigation (CDM) tools in place and in accordance with program guidance. Specifically, the Chief Information Security Officer (CISO) will conduct a review of the guidance, procedures, and tools in place to resolve this report's recommendation.
>
> **Responsible Official:** CISO; Target Completion Date: March 31, 2022

Recommendation 2. Select and implement a CDM SWAM tool that is compatible with the DOI's computer environment.

> **OCIO Response:** Concur. New CDM Software Asset Management (SWAM) tool(s) are being considered to replace previous CDM tools with the intention of fully addressing gaps. This selection, from Department of Homeland Security (DHS) funding through implementation, does not have a projected resolution date. The Department will utilize the CDM and other tools currently in place to maintain reasonable software inventory focusing on managing vulnerabilities, risks, and critical configuration requirements. Specifically, CISO will conduct a review of the guidance, procedures, and tools in place to resolve this report's recommendation.
>
> **Responsible Official:** CISO; Target Completion Date: March 31, 2022

Recommendation 3. Establish, implement, and continuously review and update approved software lists (blacklists and whitelists) to ensure that unapproved, unsupported, or potentially malicious software is not present on bureau computer networks.

> **OCIO Response:** Concur. New CDM SWAM tool(s) are being considered to replace previous CDM tools with the intention are fully addressing gaps. This selection, from DHS funding through implementation, does not have projected resolution date. The Department will utilize the CDM and other tools currently in place to maintain reasonable software inventory focusing on risk managing vulnerabilities and critical configuration requirements. Specifically, CISO will conduct a review of the guidance, procedures, and tools in place to resolve this report's recommendation.
>
> **Responsible Official:** CISO; Target Completion Date: March 31, 2022

Attachment: OCIO Management Response for OIG Draft Report No. 2019-ITA-003

OIG Recommendations for the US Geological Survey (USGS):

Recommendation 4. Establish a listing of authorized ports, services, and protocols for the [redacted] system and restrict the use of unauthorized ports, protocols, and services at the host level for the [redacted] system.

USGS Response: Concur. The USGS Information Security Office (ISO) will update procedures for reviewing authorized ports, services, and protocols and restricting the use of unauthorized ports, protocols, and services at the host level. The USGS ISO will also work to determine if a Plan of Action and Milestones is needed to track compliance.

The USGS [redacted] Project will utilize the procedures provided by the USGS ISO to establish a listing of authorized ports, services, and protocols for the [redacted] system. Where host-level restrictions may cause mission operational impact, the USGS [redacted] Project will develop a Plan of Action and Milestones to ensure compliance.

Responsible Official: USGS ACIO; Target Completion Date: March 31, 2022

Recommendation 5. Monitor systems to ensure that only authorized ports, services, and protocols are used at the host level.

USGS Response: Concur. The USGS ISO will update procedures for monitoring systems to ensure that only authorized ports, services, and protocols are used at the host level. The USGS ISO will also work to determine if a Plan of Action and Milestones is needed to track compliance.

As of September 2019, USGS [redacted] Project monitoring is supported by the USGS [redacted] Data Center security team and Security Incident Event Management (SIEM) monitoring is performed 24X7. The USGS [redacted] Data Center Security team has also established a Threat Hunting program since the audit to help perform these monitoring actions. The USGS [redacted] Project will continue to utilize DOI and USGS Continuous Diagnostics and Mitigation (CDM) tools to monitor network ports, protocol, and services at the host level on [redacted] Project systems. The USGS [redacted] Project will audit and document compliance with updated USGS ISO procedures for monitoring systems.

Responsible Official: USGS ACIO; Target Completion Date: March 31, 2022

Recommendation 6. Establish a process to ensure that operating system configuration settings are defined and consistently applied to hardware components.

USGS Response: Concur. The USGS ISO will update procedures for establishing a process to ensure that operating system configuration settings are defined and consistently applied to hardware components. The USGS ISO will also work to determine if a Plan of Action and Milestones is needed to track compliance.

The [redacted] specific finding in the report was corrected on November 19, 2019 when alerted by the Inspector General.

The USGS [redacted] Project will continue to utilize DOI and USGS CDM tools to ensure USGS ISO operating system configuration guidance. The USGS [redacted] Project will audit and document operating system configuration settings within the [redacted] Project to ensure they are defined and consistently applied to hardware components.

Responsible Official: USGS ACIO; Target Completion Date: March 31, 2022

Recommendation 7. Monitor systems to ensure ongoing compliance and consistent application of configuration settings for all systems

USGS Response: Concur. The USGS ISO will update procedures for monitoring systems to ensure ongoing compliance and consistent application of configuration settings for all systems. The USGS ISO will also work to determine if a Plan of Action and Milestones is needed to track compliance.

The [redacted] specific finding in the report was corrected on November 19, 2019 when alerted by the IG.

The USGS [redacted] Project will work with USGS ISO to utilize the [redacted] compliance tool to automate and schedule compliance checks and reporting. The USGS [redacted] Project will implement the Center for Internet Security (CIS) CIS-CAT tool to ensure ongoing compliance and consistent application of USGS Security Technical Implementation Guide (STIG) standards.

Responsible Official: USGS ACIO; Target Completion Date: March 31, 2022

Recommendation 8. Ensure that the process to identify and mitigate high-risk vulnerabilities within 30 days, as required by OCIO policy, is followed.

USGS Response: Concur. The USGS ISO will update procedures to ensure that the process to identify and mitigate high-risk vulnerabilities within 30 days, as required by OCIO policy, is followed. The USGS ISO will also work to determine if a Plan of Action and Milestones is needed to track compliance.

The [redacted] specific finding in the report was corrected when alerted by the OIG and validated in February 2019 Enterprise Vulnerability Management System (EVMS) scan reports.

The USGS [redacted] Project has taken steps since the audit to improve vulnerability management compliance. The USGS [redacted] Project will continue to follow all DOI and USGS vulnerability management guidelines. The USGS [redacted] Project will audit and report that high-risk vulnerabilities are being mitigated within 30 days, as required by OCIO policy.

Responsible Official: USGS ACIO; Target Completion Date: March 31, 2022

Appendix 3: Status of Recommendations

In its response to our draft report, the U.S. Department of the Interior and the U.S. Geological Survey concurred with our findings and recommendations (see Appendix 2). Based on the response, we consider Recommendations 1 through 8 resolved but not implemented.

Recommendations	Status	Action Required
1 – 8	Resolved but not implemented	We will refer these recommendations to the Office of Policy, Management and Budget to track their implementation.

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