EVALUATION

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

INTERIOR INCIDENT RESPONSE PROGRAM CALLS FOR IMPROVEMENT

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

Report No.: 2016-ITA-020

March 2018

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

Memorandum

MAR 0 8 2018

To: Sylvia Burns
Chief Information Officer

From: Mary L. Kendall Mary L Kendall
Deputy Inspector General

Subject: Final Evaluation Report – Interior Incident Response Program Calls for Improvement
Report No. 2016-ITA-020

This memorandum transmits the findings of our evaluation of the U.S. Department of the Interior's incident response program. We found that the Office of the Chief Information Officer had not fully implemented the capabilities recommended by National Institute for Standards and Technology (NIST) in its incident detection and response program. We make 23 recommendations to help the Department improve its incident response program, so it can promptly detect and fully contain cyber threats to maintain the availability, confidentiality, and integrity of Department and bureau computer systems and data.

In response to our draft report, the Department concurred with all recommendations and provided target dates and officials responsible for implementation. We consider all 23 recommendations resolved but not implemented. We will forward the recommendations to the Office of Policy, Management and Budget for tracking and implementation.

We understand that some of these recommendations may require significant investment in cyber security infrastructure as well as the recruitment of additional staff, but the intended timeframe to implement these recommendations remains a concern. Five recommendations will not be addressed for more than 5 years, and four recommendations will not be addressed for more than 3 years. In the interim, the Department should consider additional temporary or partial solutions.

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

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.

Table of Contents

Results in Brief

The U.S. Department of the Interior is a regular target of cyber attacks, both because of the large size of its computer networks, and because those networks contain technical and other sensitive information highly sought after by criminals and foreign intelligence services. We evaluated the Department's Office of the Chief Information Officer (OCIO) to determine whether it effectively follows the incident response lifecycle, as defined by the National Institute of Standards and Technology (NIST).

NIST guidance organizes the areas of an effective incident response program into four lifecycle phases: 1) Preparation; 2) Detection and Analysis; 3) Containment Eradication and Recovery; and 4) Post-Incident Activity. These phases are cyclical, continuously feeding results and performance strengths across the incident response lifecycle.

We found that the OCIO had not fully implemented the capabilities recommended by NIST in its incident detection and response program. The OCIO did not establish the foundation necessary for a mature incident response program—it did not determine objectives, define responsibilities, or manage the incident response program from an enterprise level. Without this foundation, the Department is unable to consistently perform incident response activities. Specifically, we found that the Department:

- Was not fully prepared to respond to incidents
- Did not promptly detect or fully analyze security incidents
- Did not fully contain or completely eradicate active cyber threats
- Did not continuously improve its incident response capabilities by learning from prior incidents

These issues occurred because the Department incident response program had not evolved to address today's often sophisticated cyber threats. For example, OCIO's incident response program followed an outdated model favoring the immediate remediation of a malware-infected computer and its prompt return to service over the current recommended model involving cyber threat analysis, assessment, and containment. As such, we found that the Department's approach to incident response and its focus on service delivery prevented incident responders from determining the extent of security incidents. Using a process that does not fully analyze and completely contain active cyber threats increases the risk that bureaus' sensitive data will be lost and mission operations disrupted.

Without a centralized program, Department and bureau incident response teams did not have an effective roadmap outlining policies, procedures, and responsibilities for handling incident response activities. We make 23 recommendations to help the Department improve its incident response program, so it can promptly detect and fully contain cyber threats to maintain the availability, confidentiality, and integrity of bureau computer systems and data.

Introduction

Objective

Our objective was to determine if the U.S. Department of the Interior effectively follows the incident response lifecycle, as defined by the National Institute of Standards and Technology (NIST).

In order to evaluate the Department's incident response program, we reviewed Department and bureau guidance for key elements recommended by NIST, as well as best practices. We conducted our fieldwork from March 2016 to June 2017. We interviewed staff responsible for incident response activities at selected bureaus and the Office of the Chief Information Officer (OCIO), and submitted a data call to all bureaus requesting specific capabilities and procedures. We analyzed prior incident response activities, using information available in the Department's official incident tracking system. Finally, we performed technical testing to simulate active internal threats to validate the Department's detection capabilities and response processes. See Appendix 1 for additional information on our scope and methodology and see Appendix 2 for details on our technical testing.

Background

The Department of the Interior protects and manages the Nation's natural resources and cultural heritage with nine technical bureaus and several offices. The Department accomplishes its diverse mission from more than 2,400 operating locations. These various locations and systems present a challenge to the Department in establishing and maintaining consistent security programs.

The Department is a regular target of cyber attacks both because of the large size of its computer networks and because those networks contain technical and other sensitive information highly sought after by criminals and foreign intelligence services. As such, the Department's incident response program should promptly detect and fully contain cyber threats to maintain the availability, confidentiality, and integrity of bureau computer systems and data.

The *Federal Information Security Modernization Act* (FISMA) requires that Federal agencies establish incident response capabilities for all systems that process, store, or transmit Federal data. Under Public Law 107-347, Section 303, NIST has the authority to develop standards and guidelines—including minimum requirements—for securing Federal information systems.

The Department's incident response capability was put to the test when a security incident occurred at a U.S. Department of the Interior data center. In October 2014, attackers moved through the U.S. Office of Personnel Management (OPM) environment through a trusted connection to the Department's data center, pivoting to human resources systems hosted by the Department. This incident was not detected until April 2015. In today's cyber threat landscape, security incidents that result in the loss of sensitive data and disruption of business operations occur on a daily basis. As such, the Department must be able to detect and respond to security incidents to protect sensitive data and maintain business operations.

Incident Response Lifecycle

NIST released Special Publication 800-61 Revision 2 (NIST SP 800-61r2) *Computer Security Incident Handling Guide*, in August 2012. This guidance was designed to assist agencies in establishing Incident Response programs that enable them to prepare for and respond to security incidents.

NIST SP 800-61r2 organizes the areas of an effective incident response program into four lifecycle phases:

- Preparation – involves limiting the number of incidents that may occur by using risk assessments in order to select and implement controls.

- Detection and Analysis – detecting and analyzing security breaches is necessary for alerting agencies when incidents occur, and evaluating the type, extent, and magnitude of the breach.

- Containment, Eradication, and Recovery – mitigating the impact of an incident by containing it and recovering from it. Activity in this phase often goes back to detection and analysis.

- Post-Incident Activity – conducting lessons learned activities and issuing a report detailing the cause and cost of the incident and the steps to be taken to prevent future incidents.

As shown in Figure 1 below, these phases are cyclical, continuously feeding results and performance strengths across the lifecycle.

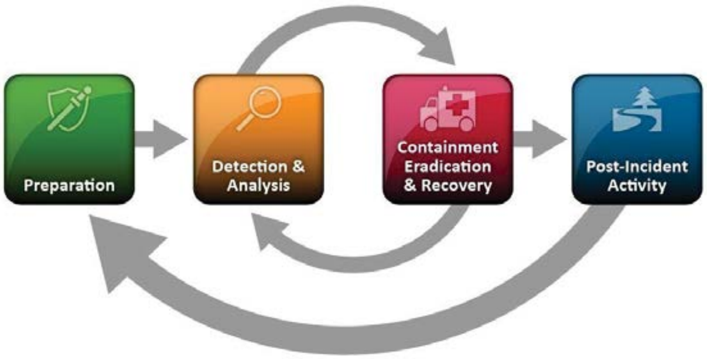


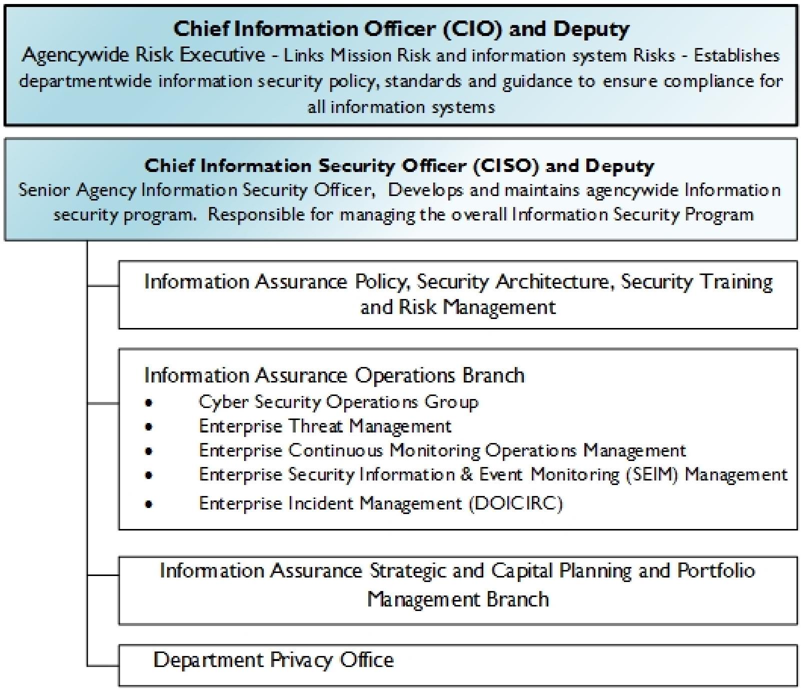
Figure 1. The NIST incident response lifecycle, as defined by NIST SP 800-61r2. Source: NIST

The incident response lifecycle also supports threat hunting activities in all phases. Threat hunting is an active, human driven activity focused on the identification of threats on the network that automated tools often fail to detect. Information generated by or documented in each phase is critical for threat hunters to have a complete view of the network environment's risks and threats.

In addition, NIST released guidance on recommended security controls in the form of Special Publication 800-53 Revision 4 (NIST SP 800-53r4) *Security and Privacy Controls for Federal Information Systems and Organizations*. This guidance was designed to assist agencies and system owners in selecting and implementing controls to improve all aspects of cyber security, including incident response planning, handling, monitoring, and testing.

History of the Department's Network and Security

The OCIO operates a large network with over 170,000 IT assets. Such large networks can provide a wide attack surface for malicious actors, if not properly designed. As such, the Chief Information Officer (CIO) delegates security responsibilities among its staff of information security professionals (see Figure 2).



Chief Information Officer (CIO) and Deputy
Agencywide Risk Executive - Links Mission Risk and information system Risks - Establishes departmentwide information security policy, standards and guidance to ensure compliance for all information systems

Chief Information Security Officer (CISO) and Deputy
Senior Agency Information Security Officer, Develops and maintains agencywide Information security program. Responsible for managing the overall Information Security Program

Information Assurance Policy, Security Architecture, Security Training and Risk Management

Information Assurance Operations Branch

- Cyber Security Operations Group
- Enterprise Threat Management
- Enterprise Continuous Monitoring Operations Management
- Enterprise Security Information & Event Monitoring (SEIM) Management
- Enterprise Incident Management (DOICIRC)

Information Assurance Strategic and Capital Planning and Portfolio Management Branch

Department Privacy Office

Figure 2. Security responsibilities within the OCIO. Source: OCIO

The OCIO's Information Assurance Operations Branch contains the Cyber Security Group and the Computer Incident Response Capability (DOICIRC) to provide a single IT security incident handling capability. The Information Assurance Operations Branch's roles and responsibilities states that the DOICIRC incident handlers coordinate response efforts when a critical breach, severe attack, or computer compromise occurs. They also send e-mail alerts to the OCIO, bureau, and office incident response staff describing emerging threats. This unit reports to the Chief Information Security Officer (CISO) and the CIO.

The Cyber Security Operations Group was established in the OCIO to enhance prevention and provide early detection of security incidents, and coordinate agency-level information related to the Department's IT security posture. The OCIO developed a handbook for security incidents, and an official incident response tracking system for coordinating, tracking, and reporting incidents. As part of the Enterprise Services Network (ESN) contract, to manage security and network services, Verizon provides technical capabilities and staff resources to the Department's incident response program.

The Cyber Security Operations Group and Verizon operate incident response tools located at five Trusted Internet Connections (TICs) for the Department. The purpose of the TIC initiative is to improve and standardize security controls across individual external network connections currently in use by Federal agencies, including connections to the Internet.[1]

In the recent past, the OCIO desegregated the bureaus' networks to improve service delivery, resulting in the widespread removal of internal security segmentation and monitoring programs, such as firewalls and intrusion detection systems. This focus on improving service delivery across bureau and facility boundaries came with the consequence of weakened security. This significantly increased risk to the Department's IT assets by making it easier to access these systems without security monitoring. A network without security segmentation is commonly referred to as a flat network.

[1] OMB Memorandum M-08-05, "Implementation of Trusted Internet Connections (TIC)"

Findings

We found that the Department's incident detection and response program did not effectively follow the incident response lifecycle, as defined by NIST. Specifically, we found that the Department:

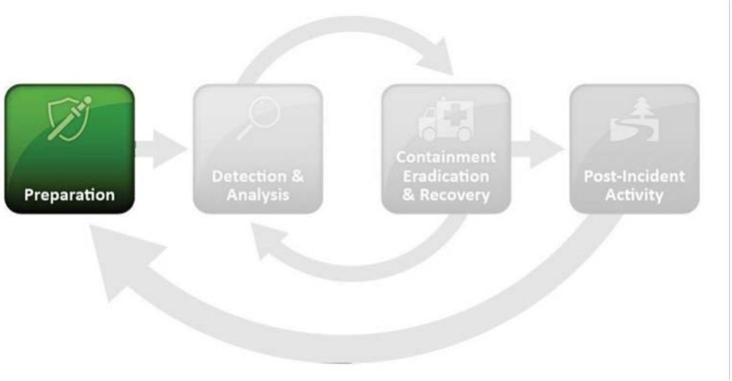
- Was not fully prepared to respond to incidents
- Did not promptly detect or fully analyze security incidents
- Did not fully contain or completely eradicate active cyber threats
- Did not continuously improve its incident response capabilities by learning from prior incidents

The OCIO did not establish the foundation necessary for a mature incident response program—it did not determine objectives, clearly define responsibilities, or manage the incident response program from an enterprise level. As such, OCIO's incident response program was not capable of detecting some of the most basic threats from inside the enterprise network. Without detecting these threats, the OCIO could not contain them in a timely manner, which left compromised systems on the network for months at a time.

These issues occurred because the Department's incident response program has not evolved to address today's often sophisticated cyber threats. For example, OCIO's incident response program followed an outdated model favoring the immediate remediation of a malware-infected computer and its prompt return to service over the recommended model of cyber threat analysis, assessment, and containment. As such, we found that the Department's approach to incident response and its focus on service delivery prevented incident responders from determining the extent of security incidents. Using a process that does not fully analyze and completely contain active cyber threats increases the risk that bureaus' sensitive data will be lost, and mission operations disrupted.

Department Not Fully Prepared to Respond to Incidents

The first phase of the NIST incident response lifecycle focuses on preparation. This phase includes the development of an incident response program as well as implementing measures to help prevent incidents from occurring.



We found that the Department's incident response program was not centralized, and the OCIO neither established roles and responsibilities nor disseminated guidance to the bureaus and offices. Specifically, the Department was not fully prepared to respond to incidents because:

- The design of the OCIO's incident response program did not follow NIST guidance. This adversely affected bureau incident response capabilities.

- The OCIO was slow to develop a comprehensive enterprise incident response plan.

- Incident response capabilities varied widely among the bureaus.

Program Design Impedes Enterprise Response Capabilities

We found that the OCIO did not have a fully developed incident response program because it had not established and communicated clear program roles and responsibilities to the bureaus. As a result, bureau incident response capabilities varied widely, which often resulted in active cyber threats not being fully analyzed and contained.

NIST[2] established primary elements for developing and documenting an incident response program, including specific recommendations for agencies to use when developing guidance for these programs. These primary elements include policies to define and structure an incident response program, such as defined roles and responsibilities, levels of authority, prioritization of incidents, and performance measures.

During our review, we did not find the NIST-defined elements for incident response in the Department's IT security policies. Our review found that the OCIO simply copied the NIST SP 800-53r4 Incident Response Controls section into its *Incident Response Security Control Standards.* The OCIO did not expand

[2] NIST SP 800-61r2, Section 2.3.1, "Policy Elements."

on the NIST-defined element to establish a Department policy that could be fully implemented and executed.

NIST[3] also recommends additional elements to assist in planning coordinated response activities, including metrics for measuring response capabilities and effectiveness, response teams and communications, and expected strategies. We found that these additional elements were also missing from the Department's policies and procedures.

Since 2015, annual FISMA reports have indicated management control deficiencies, areas of weakness, and missing disciplines throughout the Department related to incident response. In the OIG's 2016 FISMA audit report, an independent audit team described the Department's incident response program as an ad-hoc process, or at the lowest process maturity level, because it did not have adequate documentation and dissemination of authority, responsibilities, and expectations.[4] On October 31, 2017, the OIG FISMA audit upgraded the maturity level of the Department's incident response program from "ad-hoc" to "defined." The report noted the release of an incident response plan on August 28, 2017, and also stated that the Department's "incident response program is not effective."

In addition, we found that the OCIO had not developed an incident response team structure beyond OCIO staff. While the OCIO implemented incident detection and containment controls at the Department's five internet connections, all other responsibilities had been left to bureaus and offices with no central point of coordination. Without a centralized program, it is more difficult for bureaus and offices to coordinate and communicate with other bureaus and the OCIO.

For example, the OCIO's Cyber Security Operations Chief stated that his team was not privy to the Department's High-Value IT Asset list developed by OCIO due to its sensitive nature. 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 Department high-value IT asset may be expected to have a severe adverse effect on agency operations, assets, or individuals.

Since this list was not available to those responsible for monitoring and securing the Department's most important IT resources, incident response teams could not focus their resources where they were most needed.

[3] NIST SP 800-61r2, Section 2.3.2, "Plan Elements."

[4] Independent auditors' performance audit report on the U.S. Department of the Interior Federal Information Security Modernization Act (FISMA) for Fiscal Year 2016, March 10, 2017. https://www.doioig.gov/reports/independent-auditors-performance-audit-report-us-department-interior-federal-information

Slow Development of a Comprehensive Incident Response Plan

We found that the OCIO did not have an active incident response plan. The OCIO started drafting a plan in April 2015, but did not publish it until August 2017. Some basic incident response procedures were defined in the *Interior Computer Security Incident Response Handbook* (IR Handbook), but this document did not meet the standards of an incident response plan and had not been reviewed or updated every 2 years, as recommended by NIST.

The IR Handbook did not define bureau roles within the incident response program, which has led to inconsistent development of bureau-specific incident response plans. For example:

- BSEE used obsolete Department policy as templates for developing internal incident response plans and procedures.
- The USGS incorrectly referred to OCIO's IR Handbook as an enterprise-level policy, but it was actually an incomplete set of procedures.

Without a Department-level incident response plan, the OCIO cannot ensure that bureaus and offices are properly prepared to respond to incidents in accordance with OCIO's expectations. For example, during an incident at the USGS, incident responders did not adequately preserve forensic evidence for analysis, as OCIO expected. Specifically, we identified anomalous network traffic that was not generated by our tests.[5] The USGS team quickly found a compromised workstation, removed it from the network, and immediately began remediation activities in accordance with the USGS incident response standard operating procedure (SOP). USGS' incident response SOP prioritizes the prompt remediation of a malware-infected computer and its return to service. Based on available indicators such as foreign access attempts, our Computer Crimes Unit (CCU) began collecting data for forensic analysis, but necessary data was unavailable due to the remediation activities already performed.

The OCIO did not provide bureaus with updated guidance based on lessons learned from the 2015 OPM breach. As such, it was unaware that bureaus were still focusing on return to service priorities rather than analyzing the scope of the threat.

Inconsistent Incident Response Capabilities Across the Department

We found that bureau incident response programs evaluated and responded to cyber threats without considering the potential impact to the rest of the Department. This occurred because the OCIO had not managed the incident response program from an enterprise risk management perspective. The DOICIRC did not consistently coordinate incident response for incidents that

[5] This was the only facility where we analyzed regular Department traffic, or traffic that we did not generate.

affected one or more bureaus. Instead, DOICIRC opened individual tickets used for incident tracking for each affected bureau. We did find that bureaus met incident handling requirements when responding to the confirmed release of personally identifiable information (PII).

With incomplete or absent departmental guidance, bureaus and offices built separate internal incident response programs with varying capabilities in terms of staff and technical resources. Figure 3, below, shows the number of dedicated incident response staff for each bureau, as well as the number of users per staff member. The two bureaus without dedicated staff each stated that incident response is not a primary duty, but considered it part of the collateral duties for existing IT security staff.

Bureau	Number of End Users	Number of Dedicated IR staff	Users per Incident Response FTE
BSEE*	2,400	7 contractors	342.8
BIA	5,800	15 contractors	386.6
BLM	10,000	3 FTE	3,333.3
FWS	13,986	0	N/A
NPS	22,890	1 FTE	22,890
USBR	6,200	0	N/A
USGS	10,571	2 FTE	5,285.5

* Also includes ONRR's network devices.

Figure 3. Incident response staff at each of the bureaus we reviewed, as of November 2016. Source: Bureau data call.

Interconnected systems within the Department pose risks to the enterprise, not just a single bureau or office. Without intermediary security controls using least privilege, restricting access to resources based on need, or monitoring traffic between systems, a compromised host can be used to pivot and attack other systems with a greater chance of success and a lower likelihood of detection. In order to mitigate this risk, some bureaus with available staff and funding, such as the BIA and BSEE, have implemented Intrusion Detection Systems (IDS), Network Access Control (NAC) systems, and Security Information and Event Management (SIEM) systems. These controls are intended to protect the bureau's sensitive facilities from other bureaus and offices, and further enhance controls that may not be available at the Department's internet connections. This disparity in technical resources widens the gap of capabilities and effectiveness between bureaus. Figure 4 identifies bureau-level capabilities that enhance incident response capabilities, and shows the disparity of resources between the bureaus we reviewed. Bureaus with less developed incident response capabilities are at greater risk of having undetected security threats which increases risk to the rest of the Department due to absence of network segmentation and lack of internal network monitoring.

Bureau	Bureau Specific Incident Response Technology
BSEE	NAC
BIA	NAC, IDS, IPS, SIEM, Malware Analysis Sandbox
BLM	SIEM
FWS	None
USBR	SIEM
ONRR	NAC
USGS	None
NPS	None

Figure 4. Bureau-level incident response capabilities, not including tools that are common throughout the Department such as firewalls, antivirus, or intrusion detection tools. Source: Bureau data call and interviews.

We found that the OCIO's enterprise incident response tools and resources were not always available to assist bureau staff when responding to incidents. As part of our evaluation, we asked all bureaus to provide the number of staff with access to the OCIO's enterprise incident response tools. We found that some bureaus had a number of staff but no access to the tools, while others had access to the tools but no dedicated staff available to use them. In addition, many bureaus were unaware of what tools were available. For example, BLM incident responders were unaware of OCIO's enterprise incident response tools, while NPS incident responders had access to and took advantage of OCIO's enterprise incident response tools.

When asked why access had not been provided to all bureaus, the OCIO told us that the bureaus requested to have their data be segregated by bureau to limit who could view potentially sensitive information. Many of the tools are unable to provide this level of data segregation, so those tools were not offered to the bureaus. We found, however, that at least one bureau had access to tools containing other bureaus' data—further illustrating the inconsistent distribution of access to the OCIO's incident response tools throughout the Department.

The OCIO also stated that it planned a "virtual Advanced Security Operations Center" (vASOC) capability that would expand bureau access to the OCIO's enterprise incident response tools that previously required physical access, but has been unable to implement it. The vASOC was intended to provide a unified interface for all bureau and office incident responders to view data generated by the OCIO enterprise incident response tools. The OCIO began the vASOC project in 2013, but the hardware to support it was loaned to a different program in 2014. As of October 2017, the hardware required to implement the vASOC had not been returned to the Cyber Security Operations Group. Further, additional funding was not provided to purchase replacement equipment. The OCIO continues to pursue this capability, but has not acquired the resources to implement it.

Recommendations

We recommend that the Department:

1. Create comprehensive policy, as described by NIST guidance, for the incident response security program that prescribes:
    - Organizational priorities
    - Roles, responsibilities, and levels of authority
    - Performance measures
    - Reporting requirements

2. Utilize the Department's High-Value IT Asset list to develop prioritized event monitoring and incident response activities.

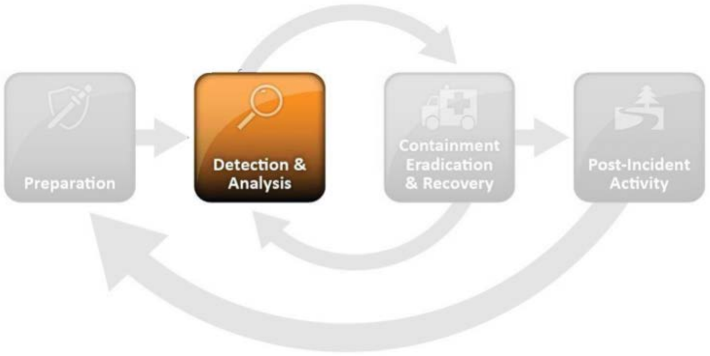
3. Develop a Department-level incident response plan and procedures that incorporate:
    - Strategies and goals, to include metrics for measuring effectiveness
    - Incident response team structure
    - Communication plans

4. Review bureau-specific incident response plans and procedures to ensure alignment with the Department's incident response plan.

5. Develop a solution for providing bureaus consistent access to the enterprise incident response tools, and provide additional event analysis in the interim.

Department Not Capable of Consistently Detecting and Analyzing Threats

The second phase of the incident response lifecycle focuses on detecting and analyzing potential and active threats. The faster a threat (e.g., a computer virus) can be recognized the quicker it can be mitigated. Early threat recognition can minimize the effect of an ongoing incident or prevent one altogether.



In order to evaluate OCIO's detection and analysis capabilities, we performed technical testing at several bureaus and locations within the Department's network. We found that the OCIO:

- Did not have visibility into the Department's entire enterprise infrastructure
- Chose not to address potential threats and dangerous user behavior
- Did not detect most of the security incidents produced from our testing including the simulated exfiltration of sensitive data

These issues occurred because the OCIO divided the responsibility for detection and analysis at an organizational level. The OCIO and several bureaus have the capabilities to share incident data across the enterprise to coordinate incident response, but incident response teams often did not have the authority or ability to analyze events across the enterprise. Operating independently without effective coordination between teams has left the Department and its bureaus unaware of—and vulnerable to—active threats within the enterprise.

Further, the OCIO did not have a team actively engaged in threat hunting—the active, human-driven search for anomalous events by dedicated, experienced team members. Each incident response team was limited to bureau priorities, focusing activities on alerts generated by tools.

No Visibility of the Department's Entire Enterprise

We found that the OCIO did not have an enterprise-wide view of incidents occurring within its network. The OCIO did not have visibility of bureau- and office-level incidents or event data. Further, OCIO did not have a single mechanism for tracking and evaluating data as incidents occur or after they have been resolved.

The OCIO was not able to correlate the event data from all OCIO and bureau systems that was generated by our tests, which simulated the exfiltration of sensitive data, compromised machines, and active malicious threats. By aggregating this data and analyzing as a whole, incident responders would have been able to more quickly identify our behavior as a potential threat. To determine if OCIO staff could detect or prevent our activity, we analyzed data from the OCIO's enterprise incident response tools.[6] We requested data from the OCIO's incident responders to determine if there was a human response to our activity, and we also used our own tools to monitor our testing activity. We found that event data was segregated across multiple systems that were separately operated and funded—making it nearly impossible to automatically correlate and analyze anomalies across the enterprise. This practice increased costs because some systems had duplicate functionality and agents, while the human element was still missing.

The OCIO's ability to correlate incident information across the enterprise was limited. USGS maintains an official incident tracking system for all bureaus and offices for the OCIO. Most bureaus, however, hosted their own internal incident tracking systems, and only informed the OCIO of incidents that met a bureau-determined threshold. This threshold was usually a bureau's interpretation of the mandatory US-CERT[7] (U.S. Computer Emergency Readiness Team) reporting after the confirmed loss of PII. This left the OCIO unaware of incidents that may have been crossing organizational boundaries, and minimized opportunities for the OCIO to provide advanced warnings to bureaus not yet affected.

NIST SP 800-53r4 recommends practices for manual and automated audit log practices. Audit logs must be retained for adequate support of after-the-fact investigation of security incidents. Enterprise threat detection via event correlation is typically accomplished with a Security Information and Event Manager (SIEM) and a group of knowledgeable and engaged responders. A SIEM provides real-time correlation and analysis of logged events generated by any device on the network from which it receives data. The OCIO, bureaus, and Verizon worked independently to implement separate SIEM solutions—these standalone systems did not share or collect data from each other.

In its DOI Cybersecurity Strategic Plan for fiscal year 2016, the OCIO documented the need for an enterprise SIEM for incident response, but it was not a funded priority. The Cyber Security Operations Group has begun testing a log aggregation tool that will collect log data from multiple OCIO systems. The OCIO plans to feed this data directly into an enterprise SIEM solution in the future. We noted the following disparate SIEM installations:

- Event logs from departmental VPN servers were sent to a SIEM operated by Verizon.

[6] We did not have access to all of the OCIO's enterprise incident response tools.

[7] https://www.us-cert.gov/about-us

- Event logs from Active Directory were sent to a SIEM operated by the OCIO.
- Event logs from bureau-operated systems were correlated in multiple disparate SIEM operated by individual bureaus.

As a result, some bureaus acquired and implemented their own SIEM solutions. In addition, the U.S. Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) program includes plans and funding for implementing a SIEM.

In addition, we found that the OCIO did not engage in active threat-hunting activities, searching for potential threats across organizational boundaries within the Department. The OCIO's enterprise cyber security operations teams had not been assigned the responsibility to track down incidents that pose a risk to the entire Department. Threat-hunting teams require experienced cybersecurity personnel with backgrounds in multiple information technology fields, such as digital forensics, networking, system administration, and security. Instead of building a threat hunting team, OCIO relied on automated alerts. Automated alerts can only detect anomalies based on pre-determined signatures and are often filled with minimal relevant data. Automated threat detection systems not properly tuned for their environment typically have a large number of false positives and negatives. The Department was missing the human interaction when analyzing alerts, events, and active processes across the environment necessary to find well-hidden intruders and tune systems to capture the most relevant event data.

In addition, the OCIO did not consolidate enterprise tools that could share event management servers. For example, each bureau operated a separate antivirus system that logged to separate management servers within each bureau, while using the same product.

Dangerous User Behavior and Potential Threats Not Addressed

We found that the OCIO's incident response teams did not always notify their bureau counterparts of security alerts, which may indicate that a bureau computer may be compromised. Some of these alerts were generated when a bureau user engaged in inappropriate conduct, such as browsing a website hosting pornography or one that streamed pirated videos. This occurred because the OCIO considered end-user behavior policy and enforcement to be a bureau-level responsibility. A policy that does not include inappropriate usage as a potential cyber threat can adversely affect information security. Websites containing pornographic and pirated material often host malicious software. Frequenting such websites may result in malware infections which, if unaddressed, can quickly spread throughout an organization.

Moreover, computer network traffic originating from a bureau computer, which was blocked because it was headed to a known malware command and control site, can also be a potential indicator that the computer is compromised. According to the OCIO, its standard practice was not to notify bureaus of this potentially malicious traffic.

During our technical testing at a USGS facility, we discovered suspicious traffic originating from a user workstation. Our device, which was monitoring USGS network traffic, identified a USGS workstation attempting to communicate with IP addresses of known malware command and control websites in Russia. After we alerted the bureau team of the anomalous traffic, they discovered that the machine in question had been compromised.

We assisted the team with network forensics and reviewed the machine's network activities based on data recorded by the TIC security devices. A review of network traffic showed that the user had been frequenting websites that hosted pornography. The CCU later confirmed that the user had been downloading pornographic material and saving it to an external drive. This behavior triggered security alerts that were logged by OCIO-level incident response tools, but not by the USGS incident response tools. Moreover, the OCIO incident responders failed to notify their USGS counterparts of this potential security incident on the USGS network. We also discovered machines on the USGS network that were actively streaming pirated media from Russian and Ukrainian websites.

As another indicator of compromise, event logs from internal facility network devices showed that a machine was regularly transmitting NetBIOS[8] lookup requests to computers in Russia. The NetBIOS traffic was blocked before leaving the network, but the USGS facility staff did not analyze the alerts. Since the USGS network security devices blocked the NetBIOS traffic, it was never seen by OCIO incident response tools. CCU later found that this machine had also been infected with malware.

Our discussions with the USGS and OCIO's Cyber Security Operations staff revealed that blocked potential threats and dangerous or inappropriate user behavior were not investigated. Instead, the OCIO's Cyber Security Operations Group had been instructed to focus on widespread or confirmed incidents.

Industry data shows that the impact of a security breach is directly proportionate to the amount of time taken to detect and respond to that breach (see Figure 5).[9] OCIO's blocking of anomalous traffic from bureau computer networks without alerting the affected bureau of the potential cyber threat can result in threats going undetected. Undetected threats increase the risk of losing sensitive data or a

[8] NetBIOS is an acronym for Network Basic Input/Output System and is used for allowing computers to communicate over a local area network. NetBIOS traffic that attempts to exit an organization's network is a common indicator of malicious activity.

[9] Cybersecurity: For Defenders, It's About Time, Aberdeen Group report commissioned by McAfee based on data provided by Verizon, dated April 2017.

disruption to bureau operations. This directly led to multiple compromised machines remaining on the Department's network for an indeterminate amount of time.

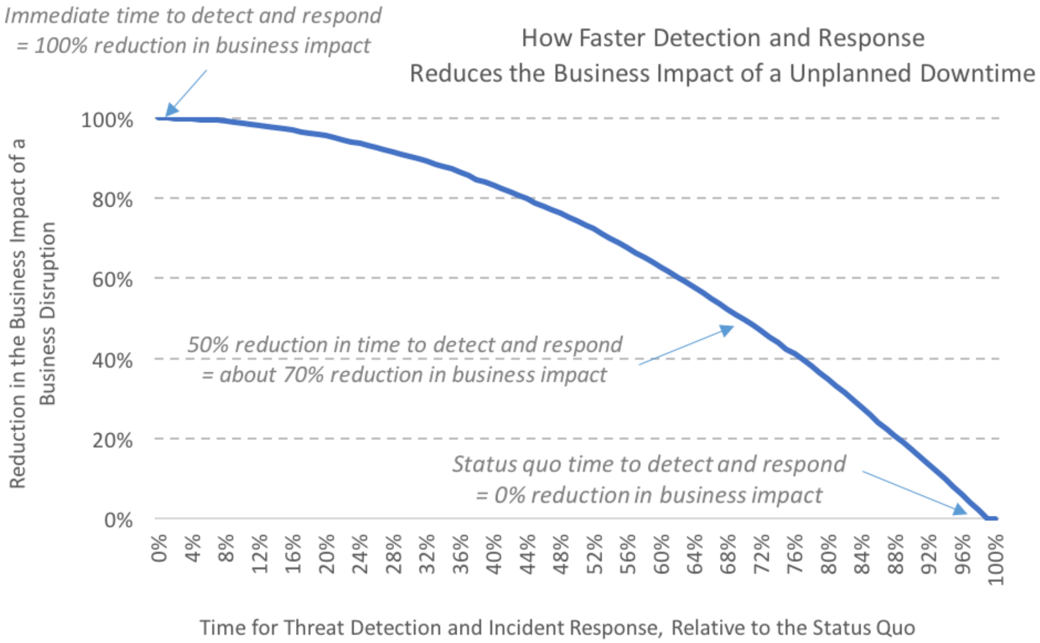


Figure 5. Analysis performed by Aberdeen Group shows that faster detection and response reduces the business impact of a data breach. Source: *Cybersecurity: For Defenders, It's About Time*, Aberdeen Group report commissioned by McAfee based on data provided by Verizon, dated April 2017.

After completing our technical testing, we returned to the USGS facility to work with local information security staff to validate the extent of the previously identified threats, and to assist with developing internal threat-hunting techniques. The USGS facility staff have since added active threat hunting to the regular duties of the local information security staff, which we consider a best practice.

Testing Unnoticed by the Department

While OCIO's enterprise incident response tools detected many of our tests, most of the alerts went unnoticed by OCIO staff. This occurred because OCIO incident response staff did not analyze alerts generated by all tools.

Over a 4-week period, we tested the Department's incident response capabilities by simulating active cyber threats on bureau computer networks. One of our tests, though benign, generated hundreds of thousands of security alerts that were recorded by an OCIO enterprise incident response tool. We found, however, that OCIO incident response staff did not review or respond to these alerts until 2 weeks later, March 20, 2017, when a different tool alerted incident response staff of a potential security incident. Although the second tool is more heavily relied on, it was slower to recognize our activity, and generated less than 20 alerts for the same test. When we asked for a summary of their response activities, the OCIO staff described the alerts from the first tool as not significant enough to warrant additional research, and also noted that blocked events do not normally trigger human activity. Once these tests were finally recognized as a threat by the second tool, the OCIO took actions to contain them.

OCIO incident response staff also did not react to any of our other tests until US-CERT identified and alerted the Department of a potential insider threat.[10] We began performing multiple ransomware file transfers on February 27, 2017. On March 22, 2017 US-CERT identified our activity as a potential insider threat. US-CERT then analyzed our activity and notified the Department of the potential threat on March 28, 2017.

We found that multiple OCIO tools began recognizing our tests on March 22, 2017. Due to a misunderstanding of the various alerts generated, the OCIO mistakenly concluded that all activity was blocked when in fact, several of the tests successfully downloaded ransomware. The OCIO's first incident response ticket for our ransomware tests was created on March 28, 2017—more than a month after our testing began.

[10] US-CERT Amber Alert, reference no. INAR-17-000008

Recommendations

We recommend that the Department:

6. Identify areas of high risk on the Enterprise Services Network (ESN), (e.g. data centers, science centers, DMZ networks) and extend enterprise incident response tool visibility to those areas.

7. Require all security incidents be tracked in a single enterprise system that allows Departmentwide incident correlation.

8. Accelerate plans to implement a Security Incident and Event Manager (SIEM) that can analyze and correlate events across multiple, disparate systems that incorporates data feeds from all security tools and infrastructure systems, to include those managed by the bureaus or third-party contractors.

9. Evaluate security tools with overlapping capabilities, such as antivirus and firewalls, for consolidation to reduce the number of disparate log management and alerting systems.

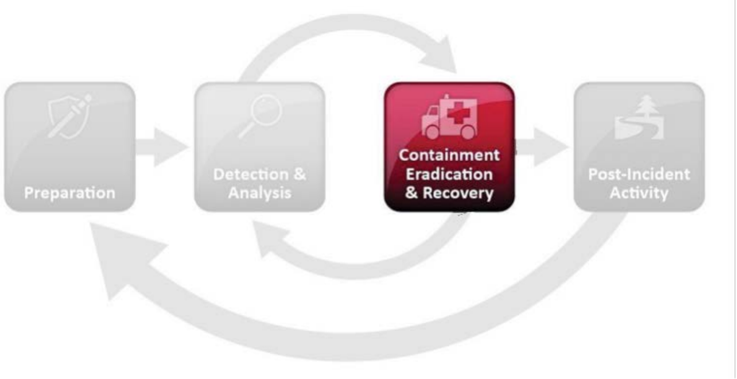
10. Define and enforce minimum Departmentwide standards on log collection and retention that are sufficient for performing event and security incident analysis.

11. Develop a dedicated group of incident responders to perform threat hunting and containment activities with:
    - Advanced analytical experience across multiple disciplines
    - Authority to access Departmentwide event data
    - Authority to engage organizationally segregated IT staff

12. Develop a Departmentwide methodology to address inappropriate and prohibited internet usage, to include departmental monitoring and a risk analysis of events.

Risks Not Contained or Eradicated

The third phase of the incident response lifecycle, containment, eradication, and recovery, is key to responding to an incident. After the foundation has been established to prepare for an incident, informed decisions can be made on how best to respond when an incident occurs. Fast detection of threats on the network is critical to effective containment—a review of public, high-profile security incidents over the past 2 years revealed that the longer a system is compromised, the higher the risk of a disruption to operations or the loss of sensitive data.



Because our tests, which simulated actual cyber threats, often went undetected by the OCIO and bureaus, we were unable to fully measure the Department's capabilities to contain and eradicate cyber threats. As such, we found that:

- Sensitive data could be exfiltrated without detection.
- Containment and eradication was slow or did not occur.
- Firewall rules do not comply with basic security principles.

Firewall configurations and the use of publicly routable IP addresses to the desktop generated a significant amount of log events, which overloaded incident responders with too much data. As a result, it was difficult for the OCIO to determine which inbound traffic was legitimate, and which was an indicator of compromise.

Sensitive Data Can Be Exfiltrated Without Detection

During our testing, the OCIO did not detect or prevent the exfiltration of sensitive information such as PII. As part of our technical testing, we created sample Microsoft Word and Microsoft Excel documents that contained simulated PII. These documents each had 10, 100, 1,500, and 10,000 fake names, credit card numbers, and social security numbers. Each document also had a cover page that contained our project number and a request to contact us directly if recovered. We simulated data exfiltration by transferring these documents to a cloud-based system managed by our team using several methods. The OCIO did not detect any of these tests.

We found that the new web Data Loss Prevention (DLP) tool used by OCIO did not block our attempts to exfiltrate sensitive data from bureau computer networks, nor did it generate alerts containing sufficient information for incident responders to analyze our activity. To save costs, the OCIO transferred web DLP responsibilities to a tool included in its Verizon contract. We analyzed reports from both the old and new DLP tools, and found that the new web DLP tool did not have the same functionality available in the old tool, which was critical for analyzing the incident. For example, reports from the new web DLP tool did not contain enough information to allow an incident responder to understand the extent of a potential data loss incident. The reports included the date and time, the file name, and the URL. The reports did not include information such as a copy of the transferred file which would allow responders to determine what type of PII was included, how many instances of PII were transferred, or whether the incident is a false positive.

The new web DLP tool was configured to allow all traffic and generate a log entry if PII is detected above a specific threshold. After each site test, we logged into the OCIO's web DLP tool and downloaded reports of all activity discovered by the tool. The web DLP only detected when we exfiltrated test documents with 100 or more PII entries over common network services, such as HTTP or FTP. The web DLP tool did not detect any unencrypted file transfers disguised by other network services—a popular tactic for malicious actors to hide their network traffic in plain sight.

Containment and Eradication Was Slow or Did Not Occur

We found that the OCIO was unaware of our testing to simulate a malicious actor on the network looking to burrow further into the Department's infrastructure. Working from within the Department network, we targeted servers for easily detectable reconnaissance and vulnerability scans. These servers were hosted within DMZ[11] networks operated by the OCIO or the bureaus. The OCIO did not respond to these tests. After testing, we noticed that some bureau-operated logs contained evidence of our tests, but this data was not visible to the OCIO and elicited no response.

In addition, we were able to hide much of our activity from the Department using encrypted remote access sessions. The OCIO did not contain encrypted outbound traffic commonly used to create remote access sessions. Intruders use these sessions to disguise their network activity from automated detection tools, remotely control compromised devices in the Department, or simply bypass controls intended to protect the Department from malicious websites and inappropriate content.

We found that the OCIO also did not detect or block the use of remote desktop sharing tools. These tools create a bridge between a computer on the Department's internal network and one connected to the internet outside the Department. Once configured, computers may be operated remotely by malicious actors or typical helpdesk support scam operations. These external bridges pose

[11] Demilitarized Zone (DMZ) is a technical term for an isolated network that is used to allow public access to services while protecting internal resources such as local area networks. Our evaluation report on "Security of the U.S. Department of the Interior's Publicly Accessible Information Technology Systems," Report No: ISD-IN-MOA-0004-2014 found that the Department did not properly configure its DMZ networks to protect its internal resources. https://www.doioig.gov/reports/security-us-department-interior%E2%80%99s-publicly-accessible-information-technology-systems

additional threat entry points into the Department’s network and additional data exfiltration methods.

We used three remote desktop sharing tools to connect to computers on the Department’s network from computers outside the network. One of these remote access tools was not detected by Department security devices, and Department incident responders did not respond to the alerts generated by the other two. These tools can often be used for remote access by well-meaning employees, but the OCIO has an official policy, published in August 2006, requiring that all remote access connections use the OCIO-managed VPN solution. The TIC security controls had the ability to enforce this policy by containing this activity, but were not configured to do so.

We also found that the OCIO’s enterprise incident response tools did not block use of The Onion Router Browser (TOR Browser). The TOR Browser is used to anonymize web-based network traffic and to access the dark web.[12] A Verizon tool detected one of our tests using the TOR Browser, and Verizon promptly contacted DOICIRC to investigate. DOICIRC contacted the bureau via email, but did not open a ticket or document the investigation in the official tracking system. Most of our TOR Browser testing went undetected. In addition, CCU’s investigation into the compromised machine at USGS found that the TOR Browser executable was present, and may have been executed.

We found that the OCIO was unable to detect and prevent common malware within a reasonable timeframe. It took 26 days for the OCIO to react to our infection simulation, because it relied more heavily on network-based IPS tools. The executable ransomware file we used for the test was identified by 45 of 58 analysis tools[13] prior to our testing, including Verizon’s web-based antivirus. Verizon’s web-based antivirus successfully blocked our transmission of the malware, but was unable to detect and block the ransomware when we hid it inside of a compressed file that exceeded 5 Megabytes (Mb). The OCIO chose not to address the alerts from the web-based antivirus because OCIO routinely does not investigate blocked events. The network-based IPS began detecting and alerting on the 5Mb file on March 23, 2017. This triggered OCIO’s first acknowledgement of the alert only, erroneously believing it had been blocked, which was 26 days after we began testing. The network-based IPS did not block our 5Mb ransomware file transfers until the final day of our testing, March 30, 2017.

[12] The dark web consists of websites that are visible to the public, but whose direct locations are intentionally hidden. This supports legitimate privacy concerns, but also enables criminal activity such as gambling, illegal drug sales, and the sharing of child pornography.

[13] To ensure we were testing with easily detectable malware, we submitted the malware sample to VirusTotal.com. VirusTotal is a website that facilitates antivirus scanning of uploaded files. At the time we uploaded the malware, VirusTotal tested it against 58 tools, and 45 of those tools successfully identified the malware.

Further, at the NPS, we discovered that audit logs were being overwritten by new events due to inadequate storage space. The NPS reported that by the time they received an alert regarding possible threats, log data was no longer available for analysis. This prevented the NPS and Department staff from identifying compromised systems. The NPS has been aware of the issue since 2008, and the identified risk was later accepted with the expectation that the OCIO would provide a Departmentwide solution. As part of a briefing in August 2017, the NPS agreed that this was no longer an acceptable risk and that it would work with the OCIO to find an interim solution in accordance with guidance within NIST SP 800-53r4.

Firewall Rules Do Not Comply With Basic Security Principles

We analyzed the Department's TIC firewall rules and found that they permitted excessive inbound and outbound traffic. This significantly reduced the OCIO's ability to contain potential incidents, as we demonstrated with our technical testing.

The *TIC Reference Architecture 2.0* establishes the minimum TIC standards required for all Federal agencies. This document states that packet filtering (e.g. firewalls) on external connections (e.g. internet) is both mandatory and required to be performed by the TIC access point. The TIC Reference Architecture 2.0 also states that firewall policies should:

- Block unsolicited inbound services by default
- Allow only approved inbound and outbound services
- Only permit approved source and destination IP addresses

When the OCIO consolidated network access under the initial TIC requirements, the USGS requested authorization to maintain its own firewalls instead of being subject to the TIC firewall rules. The OCIO agreed, and exempted USGS from the default TIC firewall rules. The additional permitted traffic caused confusion among incident responders during the compromised workstation incident at a USGS facility. We notified the USGS of this issue and it concurred that this does not meet TIC requirements, and agreed to work with the OCIO to ensure that compliant default rules will be implemented at the TIC.

We also found that excessive outbound traffic was permitted through the TIC firewalls. This occurred because of the OCIO's lax change management procedures for firewall rules. We reviewed the change management requests and justifications for all outbound traffic rules. While some change requests included narrowly defined requirements, these changes were applied Departmentwide rather than limiting the scope of these changes to the defined requirements. By not following the basic security principle of least privilege when implementing firewall rules, the risk of data exfiltration increased.

In addition, at ONRR we found a circuit connecting a Denver facility with a third-party hosting facility that bypassed the TIC architecture – including the firewalls. Traffic flowing across this circuit was not visible to the OCIO or the enterprise incident response tools. We notified ONRR of the risk this posed to the rest of the Department, including enterprise interconnected bureaus who were not aware of the connection or able to analyze and consider compensating controls. ONRR concurred with our assessment and agreed to work with the OCIO to relocate the circuit from the ONRR internal network to a TIC protected interface.

Recommendations

We recommend that the Department:

13. Configure all DLP systems to block the transfer of sensitive information.

14. Ensure all DLP systems provide sufficient data to allow incident responders to accurately identify and assess the impact of potential incidents.

15. Ensure DMZs are configured to log and report events to a centralized SIEM.

16. Define a Departmentwide baseline of inbound and outbound TIC firewall rules that incorporates:
    - Least privilege principle
    - Inbound rules to terminate at a DMZ, not internal networks
    - Periodic testing to validate that rules are operating as intended

17. Validate that all TIC firewall rules have a currently valid business case and a risk analysis, and remove those that do not.

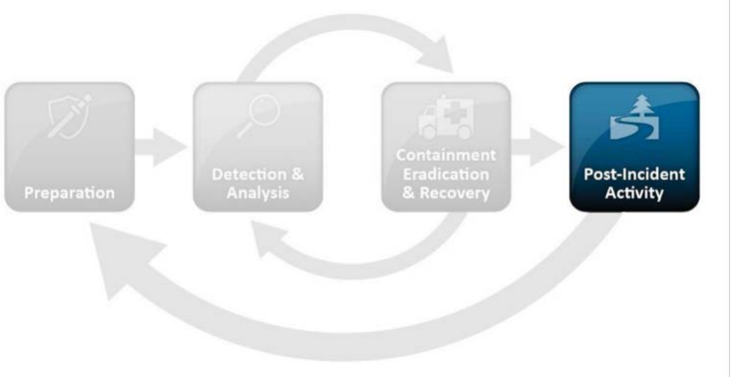
18. Identify external connections that are not visible to enterprise incident response tools and migrate them to the TIC.

Department Not Learning From Prior Incidents

The fourth phase of the incident response lifecycle, Post-Incident Activity, helps improve an organization’s incident response capability by incorporating “lessons learned” on prior incidents. According to NIST[14], well-documented incident response activities using appropriate metrics are critical for learning from the past and improving for the future. Lessons-learned exercises determine the effectiveness of the incident handling process and identify necessary improvements for existing security controls and practices. Because the Department has a flattened network, this phase should be conducted from an enterprise view to reduce the risk of incidents repeating across bureau networks.

[14] NIST SP 800-61 R2

The NIST guidance provides a suggested list of metrics that should be recorded, at a minimum, to successfully conduct post-incident activities.[15] Further, the NIST guidance states that lessons-learned activities should be performed using both objective and subjective metrics gathered during the incident reporting process.



We found that:

- The OCIO's official incident tracking system was not designed to support post-incident analysis.
- The OCIO did not perform post-incident analysis.
- The OCIO did not provide oversight to ensure that past incidents were analyzed, resolved, and documented.

These issues occurred because the OCIO did not monitor the official incident tracking system to ensure data being input was timely, complete or accurate because it considered these activities to be a bureau responsibility. Without proper use and quality assurance, the data within the tracking system cannot be fully analyzed to support the phases of the incident response lifecycle. Further, the OCIO's official incident tracking system was not designed in accordance with NIST guidance, and its poor design has led to inconsistent and unreliable data.

Without reliable metrics, the OCIO cannot accurately measure the efficacy of its incident response program. Management has not defined or developed incident response metrics and, as a result, the OCIO has missed opportunities for improving the Department's overall security posture.

Incident Tracking Data Not Designed to Support Post-Incident Analysis

We found that OCIO's official incident tracking system was not designed with the data elements and metrics required for performing post-incident analysis. For

[15] NIST SP 800-61 R2, Section 3.4.2, "Using Collected Incident Data."

example, we could not determine the amount of time spent on different aspects of analysis, containment, and recovery for each incident. In addition, OCIO staff could not assess incidents and their resolution because indicator information, incident documentation, analysis data, or impact valuations were not always available. The system does not require that these key elements be conducted, documented, or submitted prior to closing an incident ticket.

Without appropriate metrics, OCIO cannot identify successes or opportunities for improvement. Threats are changing daily, which in turn requires response activities to continuously adapt in order to detect and mitigate malicious activity in a timely manner. Changing incident response processes and controls without appropriate measurement could have a detrimental impact on the controls already in place, as demonstrated during our technical testing.

In addition to the poor design, we found that the official incident tracking system was not being used as intended due to inadequate training and guidance. For example, each bureau interpreted the incident reporting requirements differently, resulting in inconsistent data in the system.

In addition, the OCIO's incident response team routinely documented firewall rule changes in the incident response system. This information belongs in the official change management database, where an appropriate enterprise risk analysis can be performed. As a result, future risk analyses may be based on incomplete information.

Further, existing database fields were used inappropriately, resulting in inaccurate information. For example, the OCIO's official incident tracking system had three "Incident Type" categories that do not represent types of incidents. These three incident types are labeled as "DOICIRC," "ASOC," and "US-CERT." The OCIO used these incident types to show who reported the incident, rather than the type of incident that occurred. By using the incident type field in this manner, the OCIO mischaracterized the incidents, which reduced the effectiveness of the official incident tracking system because it had no assurance of accuracy. Some system discrepancies included:

- 18 percent of analyzed tickets that were labeled incorrectly would not appear in reports generated by incident type. For example, a phishing incident labeled as "ASOC" would not appear in a report for all "phishing" incident types.

- 69 percent of analyzed tickets assigned the "DOICIRC" incident type were not incidents, and instead were operational management notes.

- 74 percent of analyzed tickets assigned the "ASOC" incident type were not incidents, and instead were firewall rule changes.

During our evaluation, we briefed the OCIO of our potential findings related to the official incident tracking system. In response, the CISO stated that the OCIO “does not need metrics to perform incident response.” While metrics are not necessary to respond to a single incident, they are necessary for improving detection, analysis, containment, mitigation, and recovery for all future incidents. Having clearly defined metrics to review can help reduce delays in future detection and mitigation results.

Post-Incident Analysis Not Performed

We found that the OCIO did not conduct post-incident analysis on any of the tickets we reviewed. We selected a sample of 328 of the 3,159 tickets opened in the OCIO’s official incident tracking system between January 1, 2014, and February 28, 2016, representing approximately 10 percent of all tickets opened during our selected timeframe.

Of the incidents we reviewed, only 82 percent were adequately documented for us to understand the incident and its resolution. None contained documentation of a review for lessons-learned activities by the OCIO. One ticket had documentation of additional security controls implemented by a bureau to prevent a repeat of the incident. We could not find any evidence of enterprise-level analysis for lessons learned in the official incident tracking system.

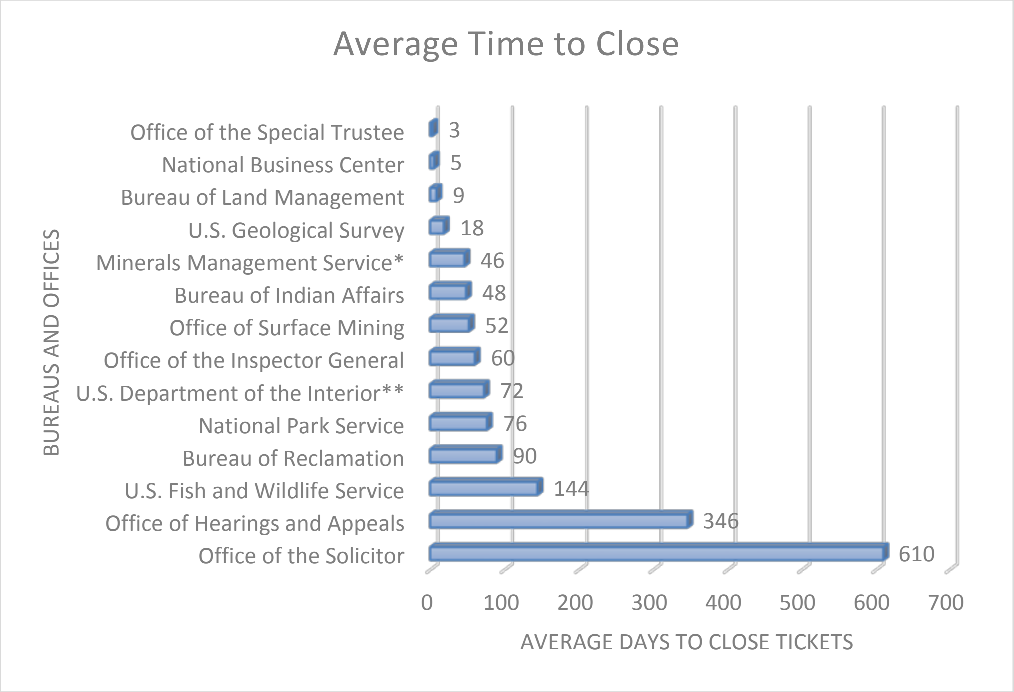
The OCIO’s Cyber Security Operations teams stated that they do not have time to perform adequate incident documentation or to document lessons learned. Further, 43 of the 3,159 tickets remained open without resolution as of August 21, 2017—more than a year after being created.

No Enterprise-Level Oversight of Incident Analysis, Resolution, and Documentation

We found that the OCIO did not monitor open incident tickets to ensure they were resolved with appropriate analysis and mitigation. Instead, the OCIO only monitored the amount of time tickets were open in the official incident tracking system.

The absence of defined incident response team roles has contributed to the misuse of the official incident tracking system. The OCIO’s Cyber Security Operations Group did not think they had the authority to require bureaus and offices to use the system and did not effectively communicate expectations. Without official guidance, bureaus relied on their own interpretations of what type of information or level of detail should be documented in the official incident tracking system.

The DOICIRC staff generated monthly reports regarding the number of open incidents and forwarded this information to the bureaus, requesting that the reported tickets be closed at the bureaus’ “earliest convenience.” It did not appear, however, that the bureaus were responding to these reports. The OCIO did not analyze bureau updates to tickets because it did not consider bureau incident activities to be under its purview. As a result, we found a disparity in the length of time taken to resolve incidents, as shown in Figure 6 below.



Note: The labels in this graph came directly from OCIO's official incident tracking system. Tickets maintained in bureau-level systems were not included.
**The BOEM, BSEE, and ONRR were still combined under the Minerals Management Service label in this system.*
***The U.S. Department of the Interior label represented groups or offices within the Department's purview.*

Figure 6: The average number of days between incident start to resolution varies by bureau. Source: OCIO.

Most bureaus hosted their own internal incident tracking systems and only copied incident data into the OCIO's official incident tracking system if they met a bureau-determined threshold. This threshold was usually the bureau's interpretation of mandatory US-CERT reporting after the confirmed loss of PII. This left the OCIO unaware of current incidents that may have been crossing organizational boundaries, and limited opportunities for advanced warnings to bureaus not yet affected. This also limited the OCIO's ability to correlate events that may have indicated a related incident occurring elsewhere.

Recommendations

We recommend that the Department:

19. Replace or redesign the official incident tracking system, as described by NIST guidance, to include:
    - All required metrics
    - All phases of the incident response lifecycle
    - Security controls applicable to all stored data types

20. Provide periodic training to incident response teams on the appropriate and consistent use of the incident tracking system.

21. Require change control events be processed and recorded in official change control management systems instead of in the official incident tracking system.

22. Develop processes for periodically performing lessons-learned activities and implement program improvements where warranted.

23. Develop and implement a quality control program that periodically reviews tracked incidents to ensure they include documentation and analysis of the extent, impact, and mitigation activities.

Conclusion and Recommendations

Conclusion

The NIST incident response lifecycle is cyclical, continuously feeding results and performance strengths back into each phase. Since the OCIO did not establish the foundation necessary to successfully prepare for responding to incidents, the Department could not detect, contain, or recover from incidents in a timely manner. The Department did not perform post-incident analysis activities and, therefore, did not complete the feedback loop to improve its incident response program.

The Department's decentralized management and authority across the OCIO and bureaus, combined with the flattened internal networks has eliminated many of the technical boundaries within the Department's network. Malicious actors use these blind spots to hide for extended periods of time, allowing the exfiltration of sensitive information.

The bureaus and offices had varying levels of capabilities, resources, and approaches to incident response. Even those with more incident response resources relied heavily on the OCIO for perimeter security controls and monitoring services, which were inconsistently shared with the bureaus. Tools, however, are not enough. Human interaction is needed to monitor and respond to incidents, which would truly elevate the Department's incident response capabilities.

The impact of security incidents is amplified because the OCIO has accepted the risk of operating a flattened enterprise network with decentralized management controls. As such, it is imperative that the Department's incident response program promptly detect and fully contain cyber threats to maintain the availability, confidentiality, and integrity of bureau computer systems and data.

Recommendations Summary

In response to our draft report, the Department concurred with all recommendations, and provided target dates and officials responsible for implementation. The Department's full response is included in Appendix 3.

We recommend that the Department:

1. Create a comprehensive policy, as described by NIST guidance, for the incident response security program that prescribes:
    - Organizational priorities
    - Roles, responsibilities, and levels of authority
    - Performance measures
    - Reporting requirements

2. Utilize the Department’s High-Value IT Asset list to develop prioritized event monitoring and incident response activities.

3. Develop a Department-level incident response plan and procedures incorporate:
    - Strategies and goals, to include metrics for measuring effectiveness
    - Incident response team structure
    - Communication plans

4. Review bureau-specific incident response plans and procedures to ensure alignment with the Department’s incident response plan.

5. Develop a solution for providing bureaus consistent access to the enterprise incident response tools, and provide additional event analysis in the interim.

6. Identify areas of high risk on the Enterprise Services Network (ESN), (e.g. data centers, science centers, DMZ networks) and extend enterprise incident response tool visibility to those areas.

7. Require all security incidents be tracked in a single enterprise system that allows Departmentwide incident correlation.

8. Accelerate plans to implement a Security Incident and Event Manager (SIEM) that can analyze and correlate events across multiple, disparate systems that incorporates data feeds from all security tools and infrastructure systems, to include those managed by the bureaus or third-party contractors.

9. Evaluate security tools with overlapping capabilities, such as antivirus and firewalls, for consolidation to reduce the number of disparate log management and alerting systems.

10. Define and enforce minimum Departmentwide standards on log collection and retention that are sufficient for performing event and security incident analysis.

11. Develop a dedicated group of incident responders to perform threat hunting and containment activities with:
    - Advanced analytical experience across multiple disciplines
    - Authority to access Departmentwide event data
    - Authority to engage organizationally segregated IT staff

12. Develop a Departmentwide methodology to address inappropriate and prohibited internet usage, to include departmental monitoring and a risk analysis of events.

13. Configure all DLP systems to block the transfer of sensitive information.

14. Ensure all DLP systems provide sufficient data to allow incident responders to accurately identify and assess the impact of potential incidents.

15. Ensure DMZs are configured to log and report events to a centralized SIEM.

16. Define a Departmentwide baseline of inbound and outbound TIC firewall rules that incorporates:
    - Least privilege principle
    - Inbound rules to terminate at a DMZ, not internal networks
    - Periodic testing to validate that rules are operating as intended

17. Validate that all TIC firewall rules have a currently valid business case and a risk analysis, and remove those that do not.

18. Identify external connections that are not visible to enterprise incident response tools and migrate them to the TIC.

19. Replace or redesign the official incident tracking system, as described by NIST guidance, to include:
    - All required metrics
    - All phases of the incident response lifecycle
    - Security controls applicable to all stored data types

20. Provide periodic training to incident response teams on the appropriate and consistent use of the incident tracking system.

21. Require change control events be processed and recorded in official change control management systems instead of in the official incident tracking system.

22. Develop processes for periodically performing lessons-learned activities and implement program improvements where warranted.

23. Develop and implement a quality control program that periodically reviews tracked incidents to ensure they include documentation and analysis of the extent, impact, and mitigation activities.

Appendix 1: Scope and Methodology

Scope

The scope of this evaluation includes enterprise incident response program and capabilities throughout the Department. We conducted our evaluation from March 2016 to June 2017. We analyzed the incidents entered into the Office of the Chief Information Officer's (OCIO's) official incident tracking system from January 1, 2014, through February 28, 2016. Our methodology for analysis varied based on the Incident Type category in the official incident tracking system.

Methodology

To accomplish our evaluation objectives, we—

- conducted interviews with subject matter experts at the OCIO, bureaus, and Verizon
- conducted a data call to the bureaus
- reviewed system security and incident response documentation for the OCIO and all bureaus
- reviewed firewall rule configurations for each of the five Trusted Internet Connection (TIC) gateways
- reviewed past security incidents
- developed scripts and network tests for technical testing
- analyzed the results of our technical tests

We selected the Department's OCIO, Verizon, and five bureaus for interviews based on their geographical locations of incident response staff:

- U.S. Fish and Wildlife Service (FWS)
- Office of Natural Resources Revenue (ONRR)
- Bureau of Land Management (BLM)
- National Park Service (NPS)
- Bureau of Safety and Environmental Enforcement (BSEE)

We selected sites to ensure that our technical testing covered the OCIO and Verizon security monitoring and enforcement tools installed at each of the four primary departmental TICs located in Denver, CO; Reston, VA; Sioux Falls, ID; and Menlo Park, CA. The sites we visited included the following:

- U.S. Bureau of Reclamation (USBR) Headquarters, Denver Federal Center
- U.S. Geological Survey (USGS) Patuxent Wildlife Research Center
- USGS Earth Resources Observation and Science (EROS) Center
- BSEE Headquarters
- FWS National Conservation Training Center (NCTC)
- FWS San Luis National Wildlife Refuge
- NPS Yosemite National Park
- BLM Central California District Office
- Bureau of Indian Affairs (BIA) CONOPS Networks at FWS NCTC

Additional details on our technical testing can be found in Appendix 2.

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

Appendix 2: Technical Testing Details

We performed technical testing at nine bureau locations within the Department's network to determine the Office of the Chief Information Officer's (OCIO's) ability to detect, prevent, and respond to various types of incidents.

The Department's Cyber Security Operations Section Chief and bureau Associate Chief Information Security Officers (ACISOs) were aware of the testing, but individual incident responders were not informed of the type testing we were performing, or when and where we would conduct the tests. We performed three types of tests, and analyzed the results using both our own tools and our limited access to the OCIO's tools. We were not granted access to all of the OCIO's enterprise incident response tools.

Our tests were designed to simulate exfiltration of sensitive data, compromised machines on the network, and an active malicious threat inside of the network. We analyzed data from the OCIO's tools to determine if it was able to detect or prevent our activity. We requested data from the OCIO's incident responders to determine if there was a human response to our activity. We also used our own tools to monitor our testing activity.

Data Exfiltration Simulation

We created sample Microsoft Word and Microsoft Excel Documents that contained simulated Personally Identifiable Information (PII). These documents each had 10, 100, 1,500 and 10,000 fake credit card numbers and social security numbers. Each document also had a cover page that contained our project number and a request to contact us if recovered. We simulated data exfiltration by transferring these documents to a cloud-based system managed by our team using several methods.

Malware Simulation

During our initial site visits, we configured vulnerability scanning software to use known malware user agents and performed a scan against our cloud-based system. We did this to determine what was necessary to gain the attention of incident responders. We stopped performing this test after we were identified by incident responders.

We used a copy of an easily detectable, generic ransomware executable for the malware download simulation. We disguised the malware by embedding it within several zip files containing other non-malicious files of varying sizes and folder depths, and changing the name of each file after each visit. To simulate malware being delivered to a Department machine, we transferred the ransomware executable and various zip files between our test machines and our cloud-based test system. Because we did not use an infected system, we utilized online tools to determine the behavior the ransomware would exhibit, if executed, and then performed manual tests to simulate execution.

We also used an open source SSL and SSL IP blacklist to obtain a list of current malicious websites acting as command and control servers for compromised systems. We performed manual tests to simulate an end user connecting to and successfully establishing an encrypted session.

Malicious Actor Simulation

We performed tests to simulate a malicious actor on the network. This scenario includes both a local intruder that gains physical access to the network or a remote intruder that gains access through hacking. We simulated network reconnaissance and pivoting activities against targets on the local network, the bureau's network, and other bureau networks. We used vulnerability scanning software to scan specific Intranet servers located in bureau DMZ networks.

Appendix 3: Response to Draft Report

The Department's response to our draft report follows on page 39.

United States Department of the Interior

OFFICE OF THE SECRETARY
Washington, DC 20240

FEB 14 2018

Memorandum

To: Mary L. Kendall
Deputy Inspector General

From: Sylvia Burns
Chief Information Officer

Sylvia Burns

Subject: Management Response to the *Draft Evaluation Report - Interior Incident Response Program Calls for Improvement*, 2016-ITA-020 (Report)

Thank you for the opportunity to review and comment on the January 2, 2017, draft report. The Office of the Chief Information Officer (OCIO) concurs with the report recommendations. OCIO is pleased to provide a coordinated Department and bureau-office response with Corrective Action Plans (CAP) and Target Completion dates as Attachment 1.

Please contact me at (202) 208-6194, if you have questions. Your staff may contact Richard Westmark, Chief, Compliance and Audit Management (CAM) Branch at (202) 513-0749.

Attachment:

1. The Department of the Interior's Management Response to the Draft Evaluation Report - Interior Incident Response Program Calls for Improvement, 2016-ITA-020 (Report)

cc: Douglas A. Glenn, Deputy Chief Financial Officer and Director Office of Financial Management
[redacted], KPMG LLP, 1676 International Drive, McLean, VA 22102
Richard Westmark, Chief, Compliance and Audit Management
Morgan Aronson, Director, Financial Audits, Office of Inspector General

Office of the Chief Information Officer
Statement of Actions to Address Office of Inspector General Draft Evaluation Report
Interior Incident Response Program Calls for Improvement, Report No. 2016-ITA-020

We recommend that the Department:

Recommendation 1: ***Create a comprehensive policy, as described by NIST guidance, for the incident response security program that prescribes:***

- ***Organizational priorities***
- ***Roles, responsibilities, and levels of authority***
- ***Performance measures***
- ***Reporting requirements***

Response: Concur. OCIO, along with bureau-office information assurance leadership, will take a unified approach to creating a standard comprehensive policy to be followed DOI-wide. The updated policy will include guidance on how priorities, roles, responsibilities, authorities, measures and reporting will be defined, implemented, and managed across all bureaus and offices within the DOI. Similar bureau-specific policies will be retired.

Responsible Official & Title: Stacy Richkun, Branch Chief, Information Assurance Policy, Security Architecture, Security Training and Risk Management (IAPATRM)

Lead Contact & Title: Robert Porter, Information Security Policy, IAPATRM

Target Completion Date: 12/1/2018

Recommendation 2: ***Utilize the Department's High-Value IT Asset list to develop prioritized event monitoring and incident response activities.***

Response: Concur. The DOI OCIO, together with bureau and office IMT leadership, are currently working, as part of the Continuous Diagnostics and Mitigation (CDM) Phase 3 initiative, to implement a single enterprise Security Incident and Event Manager (SIEM) solution. The Department will develop prioritized monitoring and incident response activities for all DOI and bureau and office High Value Assets (HVAs) and other mission-critical systems as part of this initiative. See response to Recommendation 8.

Responsible Official & Title: Stacy Richkun, Branch Chief, IAPATRM

Lead Contact & Title: Maria Clark, Enterprise Risk Management

Target Completion Date: 06/30/2023 (This date is estimated based on DHS deployment of anticipated enterprise SIEM capabilities as part of CDM Phase 3: Boundary Protection and Event Management for Managing the Security Lifecycle)

Recommendation 3: Develop a Department-level incident response plan and procedures that incorporate:

- Strategies and goals, to include metrics for measuring effectiveness
- Incident response team structure
- Communication plans

Response: Concur. The Department of the Interior-Computer Incident Response Center (DOI-CIRC) team developed a Department-level Incident Response (IR) Plan following NIST's guidelines in 2017. The plan was signed on August 28, 2017, by the Department CIO. The IR Plan will be updated to incorporate the centralized requirements described in the policy in Recommendation 1: Strategies and goals, including metrics for measuring effectiveness; incident response team structure; and communication plans.

Responsible Official & Title: Quentin Cheuk, Cybersecurity Operations Manager

Lead Contact & Title: Scott Frye, Enterprise Incident Response Manager

Target Completion Date: 06/01/2019

Recommendation 4: ***Review bureau-specific incident response plans and procedures to ensure alignment with the Department's incident response plan.***

Response: Concur. Bureaus will abide by the updated the DOI incident response plan. Bureau-specific incident response requirements will be incorporated into the DOI's incident response plan. Once complete, all bureau-specific incident response plans and procedures will be retired.

Responsible Official & Title: Quentin Cheuk, Cybersecurity Operations Manager

Lead Contact & Title: Scott Frye, Enterprise Incident Response Manager

Target Completion Date: 06/01/2019

Recommendation 5: ***Develop a solution for providing bureaus consistent access to the enterprise incident response tools, and provide additional event analysis in the interim.***

Response: Concur. A solution is currently being developed to provide bureaus and offices secure remote access to unified incident response tools and event analysis.

Responsible Official & Title: Quentin Cheuk, Cybersecurity Operations Manager

Lead Contact & Title: Robert Lewis, Enterprise Threat Manager

Target Completion Date: 12/1/2018

Recommendation 6: ***Identify areas of high risk on the Enterprise Services Network (ESN), (e.g. data centers, science centers, DMZ networks) and extend enterprise incident response tool visibility to those areas.***

Response: Concur. The DOI will identify areas of high risk on the ESN. The DOI will extend enterprise tools to higher risk enclaves, such as data centers and key ESN points, to improve coverage as indicated in the report. See response to Recommendation 8.

Responsible Official & Title: Stacy Richkun

Lead Contact & Title: Robert Lewis, Enterprise Threat Manager

Target Completion Date: 6/30/2023 (This date is estimated based on DHS deployment of anticipated enterprise SIEM capabilities as part of CDM Phase 3: Boundary Protection and Event Management for Managing the Security Lifecycle.)

Recommendation 7: ***Require all security incidents be tracked in a single enterprise system that allows Department-wide incident correlation.***

Response: Concur. The recently released DOI enterprise IR plan contains a mandate to use the current centralized security incident portal for all incidents defined by NIST. The DOI will reinforce this by issuing guidance to bureau CSIRT personnel.

Responsible Official & Title: Quentin Cheuk, Cybersecurity Operations Manager

Lead Contact & Title: Scott Frye, Enterprise Incident Management Manager

Target Completion Date: 12/1/2018

Recommendation 8: ***Accelerate plans to implement a Security Incident and Event Manager (SIEM) that can analyze and correlate events across multiple, disparate systems that incorporates data feeds from all security tools and infrastructure systems, to include those managed by the bureaus or third-party contractors.***

Response: Concur. Current and previous fiscal constraints precluded the DOI from acquiring an enterprise SIEM within fiscal years 2016-2021. The DOI will obtain a centrally managed enterprise SIEM through CDM Phase 3, for which DHS will provide initial funding. CDM Phase 3 addresses boundary protection and event management for managing the security lifecycle. Specifically, Phase 3 will provide DOI with the ability to strengthen the management of cybersecurity events/incidents and enhance protection of our internet-facing network perimeter borders and security lifecycle. OCIO will seek funding through the Working Capital Fund to support ongoing operations and maintenance costs after the implementation of CDM Phase 3.

Responsible Official & Title: Kris Caylor, Chief, Strategic and Capital Planning & Portfolio Management Branch

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

Target Completion Date: 6/30/2023 (This date is estimated based on DHS deployment of anticipated enterprise SIEM capabilities as part of CDM Phase 3: Boundary Protection and Event Management for Managing the Security Lifecycle)

Recommendation 9: ***Evaluate security tools with overlapping capabilities, such as antivirus and firewalls, for consolidation to reduce the number of disparate log management and alerting systems.***

Response: Concur. The DOI will develop an architectural roadmap for overlapping and unique capabilities at the Department, bureau and office levels, indicating the tools used at each level, and a migration path to unify consistent tool usage without overlap, where possible. Centralizing and reducing the number of log management and alerting systems will result in cost savings, including labor reduction.

Responsible Official & Title: Al Foster, Chief, Information Assurance Operations Branch

Lead Contact & Title: Quentin Cheuk, Cybersecurity Operations Manager

Target Completion Date: 12/31/2021 (This date is estimated based on DHS deployment of anticipated enterprise SIEM capabilities by 6/20/2023 as part of CDM Phase 3: Boundary Protection and Event Management for Managing the Security Lifecycle. This earlier date is based on pre-work needed to inform the CDM Phase 3 deployment scope.)

Recommendation 10: ***Define and enforce minimum Departmentwide standards on log collection and retention that are sufficient for performing event and security incident analysis.***

Response: Concur. A Department-wide standard for log collection and retention has been created and is currently under review. It will support the planned centralized SIEM. See response to Recommendation 8.

Responsible Official & Title: Stacy Richkun, Branch Chief, IAPATRM

Lead Contact & Title: Robert Porter, Information Security Policy, IAPATRM

Target Completion Date: 6/30/2023 (This date is estimated based on DHS deployment of anticipated enterprise SIEM capabilities as part of CDM Phase 3: Boundary Protection and Event Management for Managing the Security Lifecycle)

Recommendation 11: ***Develop a dedicated group of incident responders to perform threat hunting and containment activities with:***

- ***Advanced analytical experience across multiple disciplines***
- ***Authority to access Department-wide event data***
- ***Authority to engage organizationally segregated IT staff***

Response: Concur. The DOI will leverage existing resources to develop an enterprise threat hunting capability focused on advanced analytical experience across multiple disciplines with authority to access Department-wide event data, and authority to engage organizationally segregated IT staff.

Responsible Official & Title: Al Foster, Chief, Information Assurance Operations Branch

Lead Contact & Title: Quenten Cheuk, Cybersecurity Operations Manager

Target Completion Date: 12/31/2018

Recommendation 12: ***Develop Department wide methodology to address inappropriate and prohibited internet usage, to include departmental monitoring and a risk analysis of events.***

Response: Concur. The DOI will address this recommendation through a combination of additional user training, and policy review of current internet usage policy with focus on what protocols and sites are allowed for user access, as well as more reliance on automated monitoring of user activity. Automated centralized monitoring of user activity will be provided by future deployment of an SSL/TLS visibility capability and FortiGate follow-on phases that will include Digital Loss Protection (DLP) functionality.

Responsible Official & Title: Stacy Richkun, Branch Chief, Information Assurance Policy, Security Architecture, Security Training and Risk Management (IAPATRM)

Lead Contact & Title: Robert Porter, Information Security Policy, IAPATRM

Target Completion Date: 6/30/2019

Recommendation 13: ***Configure DLP systems to block the transfer of sensitive information.***

Response: Concur. Enabling unified DLP capabilities of the FortiGate appliances at the DOI's Trusted Internet Connection (TIC) is on a future phase of the current implementation.

Responsible Official & Title: Stuart Ott, Chief, Enterprise Infrastructure Services

Lead Contact & Title: Dana Hanson, EIS Project Manager

Target Completion Date: 6/30/2019

Recommendation 14: ***Ensure all DLP systems provide sufficient data to consolidate information for incident responders to accurately identify and assess the impact of potential incidents.***

Response: Concur. Enabling DLP capabilities of the FortiGate appliances at the DOI's TICs will provide consolidated information in a future phase of our current implementation.

Responsible Official & Title: Stuart Ott, Chief, Enterprise Infrastructure Services

Lead Contact & Title: Dana Hanson, EIS Project Manager

Target Completion Date: 6/30/2019

Recommendation 15: ***Ensure DMZs are configured to log and report events to a centralized SIEM.***

Response: Concur. Logs from Demilitarization Zones (DMZ's) will be sent to a centrally managed SIEM solution as described in the response to Recommendation 8.

Responsible Official & Title: Kris Caylor, Chief, Strategic and Capital Planning & Portfolio Management Branch

Lead Contact & Title: Ben Liberty, CDM Program Manager

Target Completion Date: 6/30/2023 (This date is estimated based on DHS deployment of anticipated enterprise SIEM capabilities as part of CDM Phase 3: Boundary Protection and Event Management for Managing the Security Lifecycle)

Recommendation 16: ***Define a Department-wide baseline of inbound and outbound TIC firewall rules that incorporates:***

- ***Least privilege principle***
- ***Inbound rules to terminate at a DMZ, not internal networks***
- ***Periodic testing to validate that rules are operating as intended***

Response: Concur. The DOI will define a singular baseline/standard for TIC firewall rules based on current NIST best practice, ports, protocols, and services documentation. The DOI will engineer a solution that terminates inbound rules at the DOI DMZ. The DOI will remove outdated firewall rules. The DOI will test and validate firewall rules periodically.

Responsible Official & Title: Stuart Ott, Chief, Enterprise Infrastructure Services

Lead Contact & Title: Dana Hanson, EIS Project Manager

Target Completion Date: 6/30/2021 (DOI will incorporate this requirement into the Enterprise Infrastructure Services (EIS) contract recompete, including implementing a new firewall change management system.)

Recommendation 17: ***Validate that all TIC firewall rules have a currently valid business case and a risk analysis, and remove those that do not.***

Response: Concur. The DOI will initiate a project to validate and cleanup all TIC firewall rules.

Responsible Official & Title: Quentin Cheuk, Cybersecurity Operations Manager

Lead Contact & Title: Michael Klosterman, Enterprise Software, SIEM, Analytics, and Testing (SWAT) Manager

Target Completion Date: 6/30/2021 (DOI will incorporate this requirement into the Enterprise Infrastructure Services (EIS) contract recompete, including implementing a new firewall change management system.)

Recommendation 18: ***Identify external connections that are not visible to enterprise incident response tools and migrate them to the TIC.***

Response: Concur. The DOI will identify connections not traversing the TICs and migrate them to one of the DOI TIC gateways.

Responsible Official & Title: Stuart Ott, Chief, Enterprise Infrastructure Services

Lead Contact & Title: Dana Hanson, EIS Project Manager

Target Completion Date: 6/30/2021 (DOI will incorporate this requirement into the Enterprise Infrastructure Services (EIS) contract recompete, including implementing a new firewall change management system.)

Recommendation 19: ***Replace or redesign the official incident tracking system, as described by NIST guidance, to include:***

- ***All required metrics***
- ***All phases of the incident response lifecycle***
- ***Security controls applicable to all stored data types***

Response: Concur. The DOI will survey existing bureau and office ticketing systems to find a suitable enterprise replacement tracking system that meets NIST requirements, above. Additionally, the DOI will closely monitor the CDM program for the availability of an advanced incident tracking system.

Responsible Official & Title: Kris Caylor, Chief, Strategic and Capital Planning & Portfolio Management Branch

Lead Contact & Title: Scott Frye, Enterprise Incident Management Manager

Target Completion Date: 12/31/2019

Recommendation 20: ***Provide periodic training to incident response teams on the appropriate and consistent use of the incident tracking system.***

Response: Concur. The DOI will provide standard periodic training to all bureau and office incident response teams on the appropriate and consistent use of the incident tracking system. A link with further guidance will be placed into the Department IR Plan to further aide bureaus in the consistent use of the incident portal.

Responsible Official & Title: Quentin Cheuk, Cybersecurity Operations Manager

Lead Contact & Title: Scott Frye, Enterprise Incident Management Manager

Target Completion Date: 12/30/2018

Recommendation 21: ***Require change control events be processed and recorded in official change control management systems instead of in the official incident tracking system.***

Response: Concur. The DOI will no longer input change control events into the DOI-CIRC portal and will leverage the centralized ESN Change Management portal instead.

Responsible Official & Title: Quentin Cheuk, Cybersecurity Operations Manager

Lead Contact & Title: Scott Frye, Enterprise Incident Management Manager

Target Completion Date: 02/28/2018

Recommendation 22: ***Develop processes for periodically performing lessons-learned activities and implement program improvements where warranted.***

Response: Concur. The DOI will develop processes for periodically performing DOI-wide lessons learned activities with bureau/office participation and implement program improvements. These processes will include augmenting the Enterprise IR plan with additional lessons learned guidance and adding a capability within the IR portal to record details of lessons learned activity.

Responsible Official & Title: Quentin Cheuk, Cybersecurity Operations Manager

Lead Contact & Title: Scott Frye, Enterprise Incident Management Manager

Target Completion Date: 12/31/2018

Recommendation 23: ***Develop and implement a quality control program that periodically reviews tracked incidents to ensure they include documentation and analysis of the extent, impact, and mitigation activities.***

Response: Concur. The DOI will implement an enterprise quality control program that will include periodic reviews of incident tickets to ensure that they are remediated properly, in a timely manner, and that mitigation activities are adequately documented when incident tickets are closed.

Responsible Official & Title: Quentin Cheuk, Cybersecurity Operations Manager

Lead Contact & Title: Scott Frye, Enterprise Incident Management Manager

Target Completion Date: 12/31/2018

Appendix 4: Status of Recommendations

In response to our draft report, the Department concurred with all 23 recommendations and stated that it was working to implement them. The response included target dates and an official for each recommendation (see Appendix 3). Based on this response, we consider all 23 recommendations resolved but not implemented. We will forward them to the Office of Policy, Management and Budget to track their implementation.

We understand that some of these recommendations may require significant investment in cyber security infrastructure as well as the recruitment of additional staff, but the intended timeframe to implement these recommendations remains a concern. Five recommendations will not be addressed for more than 5 years, and four recommendations will not be addressed for more than 3 years. In the interim, the Department should consider additional temporary or partial solutions.

Recommendations	Status	Action Required
1 - 23	Resolved but not implemented	We will refer these recommendations to the Assistant Secretary for 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