Failures in the Department's Security Program Resulted in Exposure of Sensitive Trade Information to Unvetted Foreign Nationals

FINAL REPORT NO. OIG-20-018-A

FEBRUARY 11, 2020

U.S. Department of Commerce
Office of Inspector General
Office of Audit and Evaluation

February 11, 2020

MEMORANDUM FOR: Karen Dunn Kelley
Deputy Secretary of Commerce

FROM: Frederick J. Meny, Jr.
Assistant Inspector General for Audit and Evaluation

SUBJECT: *Failures in the Department's Security Program Resulted in Exposure of Sensitive Trade Information to Unvetted Foreign Nationals*
Final Report No. OIG-20-018-A

Attached is our final report on our audit of the Department of Commerce's (the Department's) Enterprise Web Solutions (EWS) system. Our audit objectives were to determine whether the (1) processes used to vet contract staff given administrative access to the EWS system are adequate; (2) Department followed a sufficient process to identify the impact level of the EWS system; (3) Office of the Chief Information Officer took appropriate actions to protect the information on the EWS system after it was granted an authorization to operate in 2018; and (4) contract used to procure EWS services and systems complied with Department acquisition regulations. Because of the serious nature of the cybersecurity issues identified, we determined that this audit report would address the first three objectives, while a separate, follow-on audit may address the fourth.

We found that the Department did not protect sensitive data on the EWS system. Many of the problems we identified indicated that the Department had serious and pervasive issues that allowed exposure of sensitive data.

Specifically, we found the following:

  I.   The Department exposed sensitive data to unvetted foreign nationals working outside the United States.

 II.   Unauthorized foreign nationals accessed and modified the EWS system after their contract had been terminated.

III.   The Department mishandled the response to unauthorized access by foreign nationals.

IV.   The Department failed to account for sensitive data on its systems.

In its December 18, 2019, response to our draft report, the Department indicated that it generally concurred with our findings and recommendations. The Department's formal response is included within the final report as appendix B.

Pursuant to Department Administrative Order 213-5, please submit to us an action plan that addresses the recommendations in this report within 60 calendar days. This final report will be posted on OIG's website pursuant to sections 4 and 8M of the Inspector General Act of 1978, as amended (5 U.S.C. App., §§ 4 & 8M).

We appreciate the cooperation and courtesies extended to us by your staff during our audit. If you have any questions or concerns about this report, please contact me at (202) 482-1931 or Kevin Ryan, Director for Audit and Evaluation, at (202) 695-0791.

Attachment

cc: André Mendes, Acting Chief Information Officer
    Richard L. Townsend, Director of Security
    Joselyn Bingham, Audit Liaison, OCIO
    Bharat Dass, Alternate IT Security Audit Action Officer, OCIO
    Jason Schwartz, IT Security Audit Support, OCIO
    MaryAnn Mausser, Audit Liaison

OFFICE OF THE SECRETARY

Failures in the Department's Security Program Resulted in Exposure of Sensitive Trade Information to Unvetted Foreign Nationals

OIG-20-018-A

WHAT WE FOUND

We found that (1) the Department exposed sensitive data to unvetted foreign nationals working outside the United States; (2) unauthorized foreign nationals accessed and modified the EWS system after their contract had been terminated; (3) the Department mishandled the response to unauthorized access by foreign nationals; and (4) the Department failed to account for sensitive data on its systems.

WHAT WE RECOMMEND

We recommend that the Deputy Secretary of Commerce ensure that OCIO does the following:

1. Implements additional checks into contract policies and procedures to ensure all access to Department systems and data is properly vetted by the Department's Office of Security (OSY).
2. Conducts a thorough review of the contractor and subcontractor access granted to all Department systems and ensures this access is limited and appropriate based upon the purpose of the system, data contained on the system, and the contractor's level of required duties.
3. Establishes and implements a process that ensures the information system security officer(s) or other assigned system staff regularly validate that user access to Department systems is appropriate.
4. Fully documents its rationale, based upon the outcome of the Department's investigation, for not reporting the exposure of sensitive data from the former Secretary's briefing book as a major incident, as defined by Office of Management and Budget guidance.

We recommend that the Deputy Secretary of Commerce ensure that OSY does the following:

5. Investigate the Department's mishandling of sensitive briefing book data in accordance with its security policies.

We recommend that the Deputy Secretary of Commerce ensure that OCIO does the following:

6. Establishes and follows clear procedures when revoking access to Department systems, a process that should include the system owner, information system security officer, and contracting officer's representative, when appropriate.
7. Reviews and revises incident response procedures so that appropriate communication protocols are established and enforced to ensure timely and accurate information sharing.
8. Identifies staff with incident response and system recovery roles and ensure that they have regular training regarding their responsibilities, the role of the Enterprise Security Operations Center, and the use of system backups.
9. Includes an additional step to review the completed task when revoking system access, with a requirement for assignment of an individual responsible for ensuring all access has been removed.
10. Reviews and revises the process used for system impact analysis to ensure that it is sufficiently rigorous and has adequate checks to ensure the process produces accurate results.
11. Reassess all OS systems to ensure that the designated impact level analyses are accurate and appropriate to protect Department systems.
12. Determines if any systems outside of OS produce data for the Secretary's briefing book and, if systems are identified, determines if these systems have accurate and appropriate system impact levels.

Contents

Cover: Herbert C. Hoover Building main entrance at 14th Street Northwest in Washington, DC. Completed in 1932, the building is named after the former Secretary of Commerce and 31st President of the United States.

Introduction

Enterprise Web Solutions (EWS) is a document management system used by the Department of Commerce's (the Department's) Office of the Secretary (OS), and is located in Department headquarters in Washington, DC. EWS is provided by a U.S.-based contractor that had a subcontract with a Canada-based company. The Canadian subcontractor was specifically selected to support the EWS system because it was the developer of the document management software. Accordingly, the Canadian subcontractor maintained EWS software and provided user training. The Office of the Chief Information Officer (OCIO) manages the servers hosting EWS, which includes patching the operating system and backing up the system's data. OCIO is also responsible for the overall security of EWS with the exception of vetting contract staff, which is overseen by Department contracting officers.

EWS provides four primary functions for the Department, each within a separate *instance*[1] of the document management software (see figure 1).

1. **Executive Correspondence**—provides document processing, routing, and tracking to administratively support the Secretary of Commerce (the Secretary), Deputy Secretary of Commerce, and executive leadership's official correspondence. This instance processes unclassified correspondence between Department senior leadership and the White House, Congress, other federal agencies, private companies, corporations, foreign governments, and U.S. citizens. For example, the instance facilitates the routing of incoming correspondence (e.g., official letters, Congressional requests) to the appropriate office for review and response.

2. **Grants Notification**—provides grant notification management for the Department. The grants notification instance facilitates an automated process to ensure that affected state and Congressional leaders are notified and provided a summary of the awarded grant details.

3. **Internal Control Management System (ICMS)**—provides similar functionality to the executive correspondence instance, but only for the Department's Chief Information Officer (CIO).

4. **Secretary's Briefing Book Archive**—provides a searchable index of former Secretary Penny Pritzker's briefing book. The Secretary's briefing book is a repository of resources and information used by the Secretary to perform executive duties. This includes preparation materials used for interaction with public and foreign officials, as well as information that prepared the Secretary to address sensitive issues related to trade and foreign relations. At the end of Secretary Pritzker's tenure, she requested ongoing access to her briefing book documents. For this reason, the Department developed an archive of the briefing book to provide the former Secretary access to the documents after she had left office in January 2017.

---

[1] EWS *instances* are separate deployments of the document management software application. An instance is capable of being used for different business functions, each with a separate group of users. In the case of the EWS system, all four instances were operating on the same virtual servers.

Figure 1. Data Processed by EWS Instances[a]
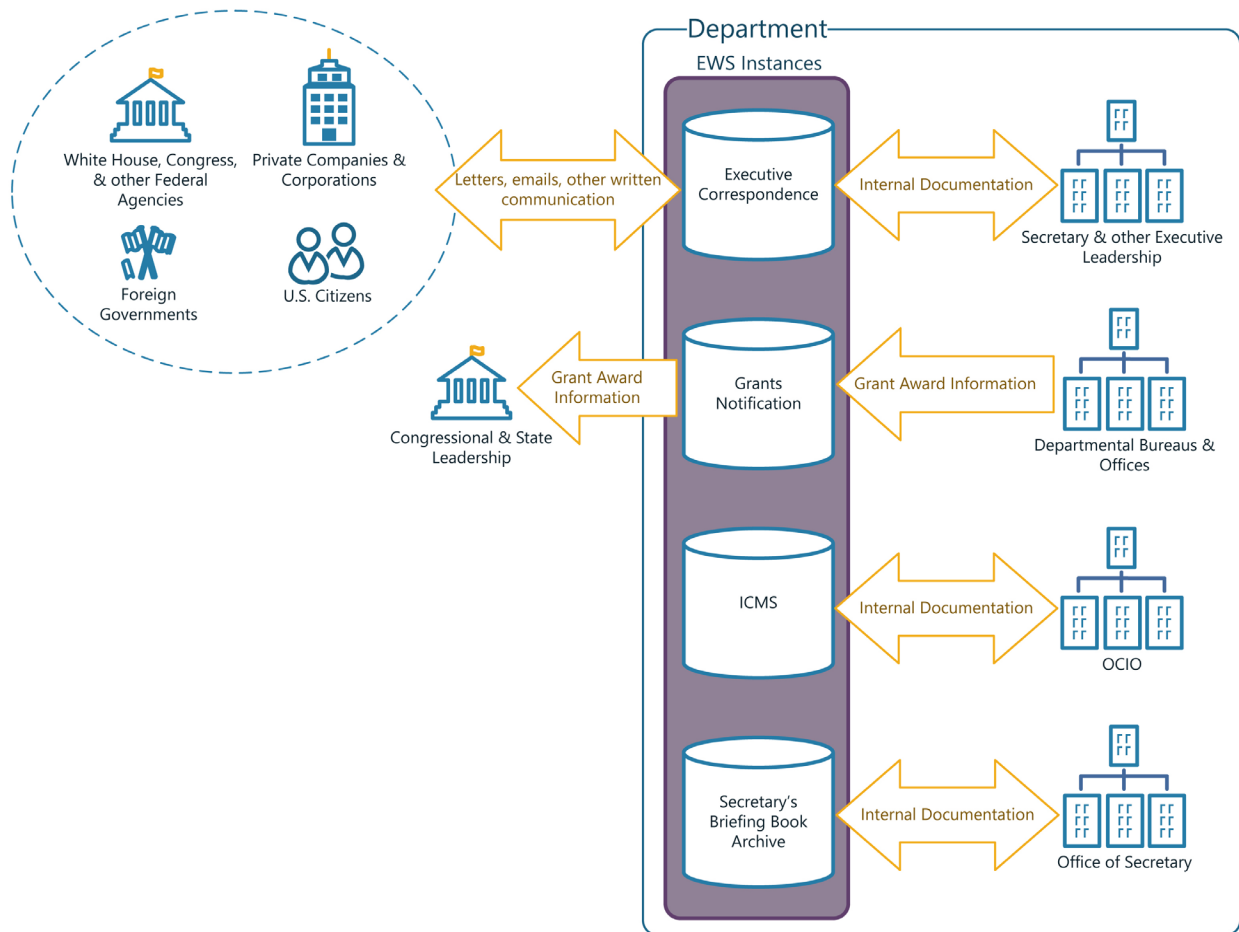
Source: Created by OIG based upon the data processed by EWS application instances.

[a] The EWS instances are only accessible from the Department's network.

Objectives, Findings, and Recommendations

Our audit objectives were to determine whether the (1) processes used to vet contract staff given administrative access to the EWS system are adequate; (2) Department followed a sufficient process to identify the impact level of the EWS system; (3) OCIO took appropriate actions to protect the information on the EWS system after it was granted an authorization to operate in 2018; and (4) contract used to procure EWS services and systems complied with Department acquisition regulations. Because of the serious nature of the cybersecurity issues identified, we determined that this audit report would address the first three objectives, while a separate, follow-on audit may address the fourth. See appendix A for further details regarding our objectives, scope, and methodology.

Due to the seriousness of the issues we identified throughout the course of our audit fieldwork, we periodically briefed the Department on our observations. We provided these briefings so that the Department could immediately begin addressing the issues we had identified.

We found that the Department did not protect sensitive data on the EWS system. Many of the problems we identified indicated that the Department had serious and pervasive issues that allowed exposure of sensitive data. Notably, sensitive global trade and foreign affairs data contained within the system was exposed to foreign entities around the time of international negotiations of the Trans-Pacific Partnership (TPP) and the North American Free Trade Agreement (NAFTA). The exposed sensitive data made thousands of references to Canada and its Prime Minister during these sensitive negotiations.

Specifically, we found the following:

    I.   The Department exposed sensitive data to unvetted foreign nationals working outside the United States.

   II.   Unauthorized foreign nationals accessed and modified the EWS system after their contract had been terminated.

  III.   The Department mishandled the response to unauthorized access by foreign nationals.

  IV.   The Department failed to account for sensitive data on its systems.

The issues identified within this audit report demonstrate that significant attention from senior management is needed to ensure that deficiencies in protecting Department data and systems do not reoccur. Our recommendations, if fully implemented, will help the Department better safeguard its sensitive data and, therefore, fulfill its mission in a more secure manner.

I. The Department Exposed Sensitive Data to Unvetted Foreign Nationals Working Outside the United States

OS employees provided more than 18,000 records from former Secretary Pritzker's briefing book to a subcontractor based in Canada. The Department also granted the subcontractor's employees (hereafter, *subcontractors*) administrative access to EWS and the

sensitive data contained within the system. These subcontractors—who were also foreign nationals—had never undergone security vetting by the Department. Though the data contained on the EWS system was highly sensitive, the Department did not fully consider the risks of providing this data to unvetted foreign nationals.

A. The Department did not vet foreign national subcontractors

The subcontractors supporting EWS did not meet the contract requirements to work for the Department. Under the terms of the contract the Department had with the primary contractor, non-U.S. citizens could be employed if they met certain criteria. Specifically, "Non-U.S. citizens to be employed under this contract must: (1) Have legal visa status with the Immigration and Naturalization Service" and "(2) Have advance approval from the servicing Security Officer in consultation with the Office of Security."[2] However, the Canadian subcontractors were residing outside the United States. The Department never verified the visa status of these subcontractors, nor were the subcontractors vetted by the Department's Office of Security (OSY). Based upon Department policy, the contracting officer and contracting officer's representative should have followed OSY-required processes to vet contracting staff brought on to an awarded contract.[3] In addition to these contract management failings, the system owner and contracting officer's representative did not sufficiently perform required risk management duties that should have identified these risks, such as ensuring the appropriate background screening of contractors and subcontractors accessing EWS.

B. The Department granted the subcontractors administrative access to the EWS system and its sensitive data

The Canadian subcontractors had remote administrative access to the EWS system servers, application, and database from June 2014 until July 19, 2018. During this time, the subcontractors could access all data contained within EWS. This access ultimately included all four EWS instances, and contained data involving negotiations of foreign trade conducted by Department senior leadership. These EWS instances contained sensitive data relating to global trade and foreign affairs, as well as National Security Affairs calendars, Committee on Foreign Investment in the United States (CFIUS) records, and Department OCIO system vulnerabilities.

We found that the reason the Department had granted the subcontractors administrative access was to remotely install EWS application updates. However, we also found that the subcontractors did not need remote access to these EWS servers in order to do their work. Although other authorized Department system administrators could have installed the application updates, the U.S.-based prime contractor insisted that the subcontractors required access. Department staff granted the subcontractors

---

[2] U.S. Department of Commerce Office of the Chief Information Officer, June 24, 2015. *Contract No. GS-35F-5814H*. Washington, DC: DOC OCIO, order number SA1301-15-NC-0056, sec. C.14.1, *Personnel Background Investigation Requirements*, 18.

[3] DOC Office of Security, December 2012. *Manual of Security Policies and Procedures*. Washington, DC: DOC OSY, sec. II, chaps. 11.3 & 11.4.

complete access to the EWS system without ensuring they had been properly vetted. By granting this access, the Department exposed highly sensitive data involving the United States' global trade and foreign affairs interests to foreign nationals based in Canada. This access had the potential to be particularly damaging considering the United States' trade negotiations and imposition of tariffs involving Canada during this period of time.

C. *The Department provided the former Secretary's briefing book containing sensitive data to the subcontractors*

OS employees coordinated the transfer of an electronic copy of former Secretary Pritzker's briefing book to the subcontractor based in Canada. Access to the briefing book was granted despite the fact that the subcontractor's network was not authorized by the Department to store or process Department data. More than 18,000 records—some of which contained global trade and foreign affairs data—were provided in several file transfers between December 2016 and January 2017. The Department provided the briefing book to the subcontractor so the documents could be stored in a newly created instance of the document management software. While the Department used a secure file transfer capability to send the documents and obtained a limited number of signed non-disclosure agreements, we found no evidence that the Department considered whether the sensitive data should be given to a foreign-based company and its foreign national employees.

EWS security staff,[4] including the system owner, information system security officer (ISSO), and OS information technology security officer (ITSO), were involved in the discussions regarding this data transfer. We also found that senior Department officials were aware of this data transfer, including the Director of Administration and the Director for the Office of Enterprise Solutions and Services. One of the limited precautions the OS ITSO took to protect the sensitive data was to have four subcontractors sign a non-disclosure agreement. However, we found that another subcontractor employee, who was not one of the original four and thus had not signed a non-disclosure agreement, received a portion of the former Secretary's briefing book. Due to limitations of OIG access to the subcontractor and its network, confirmation of whether the Department's data was exposed to additional subcontractors after the company received the data was not possible without full cooperation of the subcontractor. Additionally—without full access to the subcontractor's network—it was not possible to confirm whether the subcontractor had retained the briefing book data.

The sensitive global trade and foreign affairs data contained in the former Secretary's briefing book was sent to the Canadian subcontractor during TPP negotiations and just prior to renegotiations of NAFTA. Of the more than 18,000 records contained in the briefing book, more than 2,000 of those records contained references to Canada as part of the subject matter. These references included the Canadian Prime Minister, NAFTA, and the TPP. Further, this subcontractor had ongoing business relations with the

---

[4] The EWS system owner was from OS; ISSO was from the OCIO; and the OS ITSO was from the OCIO.

Canadian Prime Minister's Office, and previously held contracts with the Canadian Department of National Defence.

Given the strong potential for demonstrable harm to foreign relations and the national economy, the transfer of the former Secretary's briefing book likely constitutes a major security incident as defined under the Office of Management and Budget's (OMB's) guidance for reporting security incidents.[5] In accordance with this guidance, agencies are required to report major incidents to Congress and their respective OIG no later than 7 days after the date on which the agency has a reasonable basis that such an incident has occurred.[6]

We briefed the Department's Acting CIO on April 9, 2019, regarding the transfer of the Secretary's briefing book to Canadian subcontractors as well as the types of data the briefing book contained. After the briefing, Department incident responders reported this exposure to the Department of Homeland Security (DHS) and, based on feedback received from DHS, chose to subsequently downgrade its severity from "major" to "moderate." The decision to downgrade was based on the fact that the exposure did not involve a certain threshold of personally identifiable information records. Because the Department decided to follow DHS' aforementioned guidance, it chose not to consider OMB's criteria regarding harm to foreign relations and the national economy that was posed by the release of sensitive trade and foreign relations data to unvetted foreign nationals based in a country with which the U.S. government was negotiating. However, the Department indicated to our office that it continues to investigate the matter and will comply with all incident response requirements after it has established a full record.

Recommendations

We recommend that the Deputy Secretary of Commerce ensure that OCIO does the following:

1. Implements additional checks into contract policies and procedures to ensure all access to Department systems and data is properly vetted by OSY.

2. Conducts a thorough review of the contractor and subcontractor access granted to all Department systems and ensures this access is limited and appropriate based upon the purpose of the system, data contained on the system, and the contractor's level of required duties.

3. Establishes and implements a process that ensures the ISSO(s) or other assigned system staff regularly validate that user access to Department systems is appropriate.

---

[5] Office of Management and Budget, October 25, 2018. "Fiscal Year 2018-2019 Guidance on Federal Information Security and Privacy Management Requirements," M-19-02. Washington, DC: Executive Office of the President, 6.

[6] *Ibid*, 7.

4. Fully documents its rationale, based upon the outcome of the Department's investigation, for not reporting the exposure of sensitive data from the former Secretary's briefing book as a major incident, as defined by OMB guidance.

We recommend that the Deputy Secretary of Commerce ensure that OSY does the following:

5. Investigate the Department's mishandling of sensitive briefing book data in accordance with its security policies.

II. Unauthorized Foreign Nationals Accessed and Modified the EWS System After Their Contract Had Been Terminated

In July 2018, the Department's Acting CIO at that time determined that the Canadian subcontractor should no longer have access to the EWS system. In response, the U.S.-based prime contractor terminated its agreement with the subcontractor. However, the Department failed to disable the subcontractors' network accounts and an administrator account, which allowed the subcontractors to access and modify the EWS system after the subcontract was terminated.

A. OCIO failed to fully revoke Canadian subcontractors' access to the EWS system after the Acting CIO determined that sensitive data was at risk

On July 10, 2018, during the EWS system reauthorization meeting, the Acting CIO determined the subcontractors' access to the system should be revoked. The Acting CIO made this decision solely based on the potential that sensitive data had been stored on the EWS system.[7] However, following the meeting, OCIO disabled only application accounts (figure 2, label 2) and a limited number of server accounts (figure 2, label 3) belonging to the subcontractors. Virtual private network[8] (VPN) accounts (figure 2, label 1), used by the subcontractors to access the Department network, were not disabled. The VPN accounts were not disabled because the task order to remove access was not sent to the proper individuals and was inaccurately marked as completed after only system level accounts had been disabled.

Additionally, a shared administrator account for the EWS servers was not disabled. OCIO did not disable this account because it had been hardcoded[9] into the application and could not be changed without affecting system functionality. According to our interview with an EWS system administrator, the credentials for this shared administrator account were known to the subcontractors. By not completely revoking the subcontractors' access to the network, the Department placed its systems and sensitive data at unnecessary risk of unauthorized access and exposure.

---

[7] The fact that the subcontractors had not been vetted was not a factor in this decision, because no one in the Department was aware of this risk at this time.

[8] A *VPN* uses encryption so that the connecting user may be treated as part of the internal network. In this case, the Department had issued the Canadian subcontractors laptops with VPN software to allow them to securely access the Department's network remotely via an encrypted connection from their offices in Canada.

[9] *Hardcoded* is a piece of code within a software program that cannot be changed without modifying the program.

Figure 2. Data Processed by EWS Instances
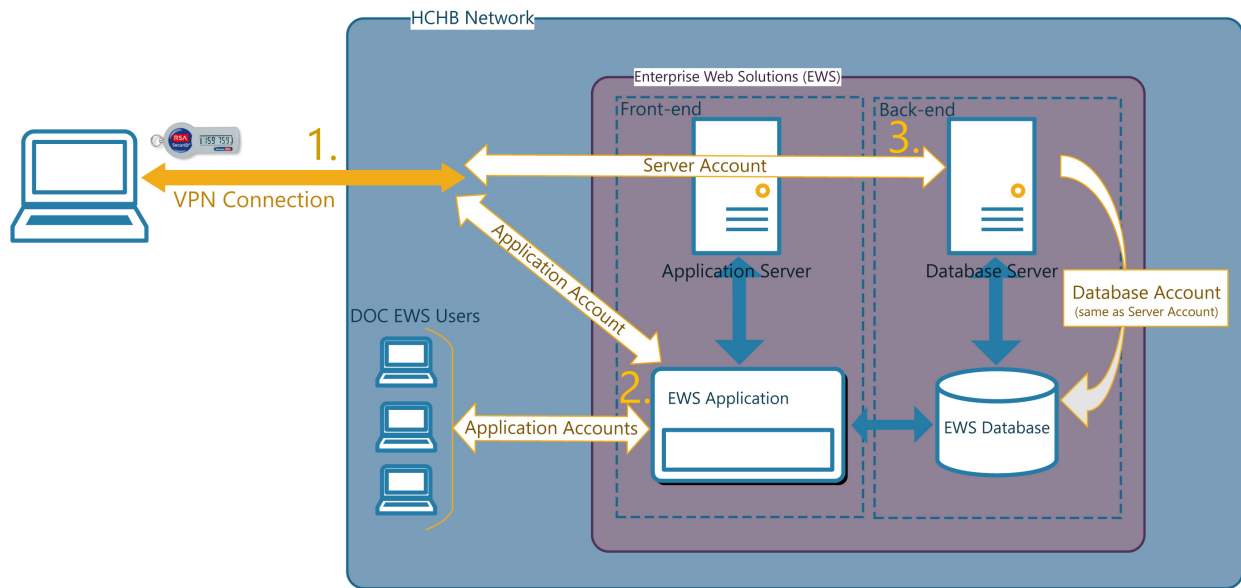
Source: Figure created by OIG based upon the access methods available for the EWS system

B. *Canadian subcontractor accessed and modified the EWS system after the contract was terminated*

On the morning of July 17, 2018, the EWS prime contractor terminated its subcontract with the Canadian company. However, at three different times shortly after the termination, a subcontractor used their still-active VPN account to access the Department's network. During these VPN sessions, the subcontractor used remote desktop connections to access the EWS application server and database server. It was during these sessions that the subcontractor's application account, which OCIO had disabled a week earlier, was re-enabled.

Following this unauthorized access, the system owner and application administrator, both Departmental employees, reported the loss of administrator privileges on the system. Specifically, the legitimate system owner and application administrator lost functionality to manage accounts and to adjust the document routing schedules. Additionally, the application administrator could no longer remedy EWS application errors, which resulted in a loss of communications between EWS and other grant processing systems within the Department.

We also found evidence of abnormal behavior in the EWS database. Specifically, the Enterprise Security Operations Center (ESOC) found that a full backup of the EWS database was made during the period when the subcontractor accessed the EWS system after its termination notice. The backup of the database was saved to the database server itself. However, the Department's Network Operations Center, whose duty it is to perform backups for the system, does not save databases in this manner as part of its backup process. The Department was unable to determine whether this database backup was exfiltrated from its network.

Although the evidence of unauthorized changes to the system could not be directly attributed to one or more specific individual(s), we conclude that these changes were likely made by the subcontractor. We based this conclusion upon evidence of the subcontractor accessing the Department network and EWS servers after the contract was terminated, as well as the subcontractor having knowledge of the hardcoded administrator account capable of making the unauthorized changes. This conclusion is also supported by the timing of the subcontractor's unauthorized access during the days just before OS administrators reported losing privileges to control the system.

Recommendation

We recommend that the Deputy Secretary of Commerce ensure that OCIO does the following:

6. Establishes and follows clear procedures when revoking access to Department systems, a process that should include the system owner, ISSO, and contracting officer's representative, when appropriate.

III. The Department Mishandled the Response to Unauthorized Access by Foreign Nationals

Department staff did not properly investigate and recover from the unauthorized access by the former subcontractor. During the Department's investigation, ESOC, which is responsible for Department incident response, failed to gain a basic understanding of EWS and the unauthorized access that occurred. This was caused by a lack of cooperation between ESOC, EWS system staff, and OS security staff. Additionally, ESOC did not perform a forensically sound examination of the laptops presumably used by the unauthorized foreign nationals. Instead, ESOC's examination contaminated the evidence of potential criminal wrongdoing.

ESOC's initial conclusion was that the unauthorized access had not occurred. Without our requests for ESOC to reexamine the matter, the Department would not have acknowledged that unauthorized access and modification of EWS had occurred. In addition, the Department's inadequate incident response practices forfeited the opportunity to recover lost system functionality.

A. The Department's investigation of the incident was inadequate

ESOC's investigation suffered from fundamental errors and a flawed forensic investigation. ESOC's inadequate investigation hindered the Department from discovering basic details regarding the unauthorized access of EWS. The EWS system owner, application administrator, and ISSO reported unauthorized access and system changes to ESOC on July 20, 2018. On July 25, 2018, ESOC incorrectly concluded that there had been no compromise or access of government resources from outside the United States. After we questioned this conclusion on July 26, 2018, and asked ESOC to consider additional evidence that we discovered during our audit work, ESOC revised its findings and continued its investigation. ESOC's mistakes made immediately after this

incident—a critical period during incident response—deprived the Department of the opportunity to effectively identify and recover from the impact of the unauthorized access.

Although we repeatedly provided clarifying information with regard to EWS and its functionality, ESOC's confusion of basic details about the system persisted throughout its investigation. For example, ESOC misidentified EWS as an OIG system on numerous occasions during its investigation. ESOC even submitted a US-CERT notification that erroneously identified EWS as an OIG system instead of an OS system.

Not only did ESOC misidentify which bureau the EWS system operated under, it also performed inadequate analysis of evidence. As part of its investigation, ESOC sequestered two Department laptops that were returned by the Canadian subcontractor following contract termination. ESOC's forensic analysis concluded that there was no evidence of data spillage[10] or exfiltration.

However, we later discovered that ESOC had not performed a forensically sound analysis of the laptops. Instead, with no subject matter expert on staff, an inexperienced ESOC analyst performed local analysis (i.e., logging into the laptop to review logs and internet history) on the laptops. This analysis violated digital forensics best practices,[11] which require the analyst to create a copy of the original hard drive. Analysis should then be performed on the copy, instead of the laptop itself, in order to preserve the integrity of the evidence and eliminate the possibility of cross contamination (i.e., damaging the drive's contents or evidence tampering). ESOC's analysis conducted directly on the laptops rendered the evidence unusable in the event of a criminal investigation into the unauthorized access by the Canadian subcontractor. However, in August 2018 we created forensically clean copies of the laptops during our survey work before the laptops were sent to ESOC. These copies continue to remain available to the Department for any future forensic investigations.

Department staff did not adequately communicate and coordinate during the incident response process. We found that for an entire month after the incident was reported (July 20, 2018, through August 20, 2018) ESOC never communicated with affected system staff to gain a basic understanding of the incident. In addition to ESOC's lack of communication, OS security staff took little or no action to assist in the investigation of the incident. When ESOC did finally start inquiring about needed information, the EWS system owner and application administrator were unresponsive, according to electronic communications we reviewed. Eventually, EWS security staff directed ESOC to contact our office for help with several unanswered questions.

---

[10] Data spillage occurs when either classified or sensitive information is inadvertently placed on information systems that are not authorized to process such information. *See* DOC National Institute of Standards and Technology, April 2013. *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST SP 800-53, Rev. 4. Gaithersburg, MD: NIST, F-110.

[11] DOC NIST, August 2006. *Guide to Integrating Forensic Techniques into Incident Response*, NIST SP 800-86. Gaithersburg, MD: NIST, 3–4.

However, ESOC never contacted our office in regards to the questions, causing its investigation to stagnate.

With the lack of communication between ESOC and OS security staff, key questions remained unanswered for nearly 4 months after the incident. Finally, on November 9, 2018, ESOC requested a meeting with OS security staff to obtain clarifying information. After all parties involved were able to coordinate, ESOC staff recognized the significance of the circumstances and submitted a new incident report to US-CERT. However, the new incident report included only irrelevant information (i.e., a summary of an unrelated request from our audit team), indicating ESOC continued to misunderstand the details of the incident. Ultimately, on November 21, 2018, ESOC concluded that unauthorized access had occurred but was unable to attribute who modified the system or what modifications had occurred. ESOC cited the lack of security controls in place—specifically the use of shared administrator accounts—as the reason it could not come to a definitive conclusion. The Department's inability to sufficiently communicate or coordinate effectively wasted time and, therefore, the opportunity to understand and address the incident properly, especially during the critical period immediately following the reported incident.

B. *Ineffective incident management and unutilized system backups prevented the Department from restoring EWS after unauthorized access occurred*

When the EWS system owner and application administrator discovered that their access to the EWS applications had been altered, they promptly reported this to the OCIO security staff. However, the security staff did not follow required OS incident response procedures to ensure that the system could be restored to its prior state. They did not attempt to coordinate a system recovery with OCIO operations staff (i.e., server or system backup administrators), nor did they make any effort to ensure that backup media was preserved to facilitate a future recovery. When asked why they did not take these actions, the ITSO stated that restoration from backups was never discussed.

We found that backup staff had performed regular backups, which would have enabled the recovery of the system from unexpected change or loss of system data. However, when this significant security incident occurred, the Department failed to use the backups to restore the system state or to retain an unaltered copy of the system. This failure had serious ramifications. For example, by not restoring the system to a previous state, the EWS system owner and application administrator lost the ability to manage the system as detailed in finding II, which hindered the Department's operational needs. Additionally, by delaying proper incident response procedures, restoring from system backups became infeasible due to the large number of ongoing transactions facilitated by the system. The Department's response to this incident showed significant weaknesses in OCIO's capabilities to respond and recover from a serious incident.

The Department's failure to restore EWS to an unaltered state from backups ultimately resulted in the partial loss of system functionality. In April 2019, the Department was contacted by the former Canadian subcontractor and informed that the system would

not operate beyond May 30, 2019. The Department took steps to try to avert a system shutdown by this deadline; however, these efforts were unsuccessful. On May 30, 2019, the Department lost access to all four of the document management software instances on EWS. Subsequently, on June 5, 2019, the Department was able to get the system running again, but with workarounds that affected the accuracy of dates within the system. The Department's workaround involved setting the system date to the year 2013, which correlates with 2019's calendar in terms of the days of the week and months. As a result, the Department is conducting its operations on a system that is not accurately recording the time of document management events unless system users make additional, manual entries. This has not only affected OS's operations, but has also hindered the Department's investigation of the incident.

Recommendations

We recommend that the Deputy Secretary of Commerce ensure that OCIO does the following:

7. Reviews and revises incident response procedures so that appropriate communication protocols are established and enforced to ensure timely and accurate information sharing.

8. Identifies staff with incident response and system recovery roles and ensure that they have regular training regarding their responsibilities, the role of ESOC, and the use of system backups.

9. Includes an additional step to review the completed task when revoking system access, with a requirement for assignment of an individual responsible for ensuring all access has been removed.

IV. The Department Failed to Account for Sensitive Data on Its Systems

The Department failed to properly identify the types and sensitivity of the data processed and stored in EWS. This failure significantly contributed to the security breaches described in this report. During 2017, the system's functionality and the sensitivity of the system's data increased. However, the Department failed to account for the impact these changes would have on the security measures needed to protect the system and its data.

A. The Department failed to identify EWS' sensitive data

Department staff responsible for EWS failed to consider the sensitive data the system processed when securing the system. All federal information systems must undergo analysis to determine the system impact level (i.e., low, moderate, or high impact) based on the data stored, processed, or transmitted by the system.[12] A system may process many types of data with varying levels of sensitivity, but the most sensitive data drives the overall system impact level. Federal agencies are also required to periodically

---

[12] DOC NIST, February 2004. *Standards for Security Categorization of Federal Information and Information Systems*, FIPS PUB 199. Gaithersburg, MD: NIST, 1–4.

reassess the impact level of a system to ensure that the assigned impact level is still appropriate, as systems can change over time.

The Department originally categorized EWS as a moderate impact system based solely on the data believed to be in the executive correspondence and grants notification instances. However, the Department had added additional instances to the system subsequent to the initial categorization. For example, the Department created the Secretary's briefing book archive and ICMS instances in January and July of 2017, respectively. Unfortunately, the Department neither scrutinized the sensitivity of the former Secretary's briefing book and ICMS data when it was first stored in EWS in 2017, nor during a routine reassessment of the EWS system impact level in January 2018.

Our analysis of the data types processed on EWS found that the Secretary's briefing book archive contained large amounts of global trade (e.g., documents addressing trade with foreign nations) and foreign affairs data (e.g., documents to prepare the Secretary to address sensitive topics when meeting with foreign officials). Both of these data types are provisionally high impact according to NIST.[13] Additionally, there was global trade data on the executive correspondence and ICMS instances.

We also found that the Department had never accounted for Secretary Pritzker's digital briefing book prior to its migration into EWS. The Department could neither identify on which system the Secretary's briefing book had resided, nor who was responsible for its security. We conclude that both before and after this sensitive data was migrated to EWS, the Department did not ensure sufficient security controls were in place to protect the data.

B. *Department officials took no action after being informed of potentially sensitive data on EWS*

In the July 2018 EWS reauthorization meeting, the Department's Acting CIO at that time was informed that Canadian subcontractors had access to the EWS system, and that sensitive trade data was potentially stored in the executive correspondence instance. However, neither the Acting CIO nor any other Department personnel took steps to determine if the EWS system actually contained sensitive trade data. In fact, with no additional analysis, the Acting CIO re-authorized the system to continue to operate at a moderate impact level in November 2018.

The Department never accounted for a large volume of sensitive data on the EWS system, which was a significant factor in the data being exposed to foreign nationals. The Department's failure to identify this sensitive data on EWS significantly increased the chance that security controls would be insufficient to protect the data. For example, high impact data is required to have a significantly higher level of access controls and system monitoring for unauthorized access. These failures also indicated the process used by OCIO to determine the impact level of OS's systems was significantly flawed.

---

[13] DOC NIST, August 2008. *Information Security*, NIST SP 800-60, Vol. II, Rev. 1. Gaithersburg, MD: NIST, 125–127 & 121–123.

We observed that even with many opportunities, the Department never accurately identified the sensitive data on the EWS system.

Recommendations

We recommend that the Deputy Secretary of Commerce ensure that OCIO does the following:

10. Reviews and revises the process used for system impact analysis to ensure that it is sufficiently rigorous and has adequate checks to ensure the process produces accurate results.

11. Reassess all OS systems to ensure that the designated impact level analyses are accurate and appropriate to protect Department systems.

12. Determines if any systems outside of OS produce data for the Secretary's briefing book and, if systems are identified, determines if these systems have accurate and appropriate system impact levels.

Summary of Agency Response and OIG Comments

In response to our draft report, the Department indicated that it generally concurred with our findings and recommendations. The Department also provided technical comments from the OCIO and an Office of General Counsel report of its management review of EWS. The Department's formal response is in appendix B.

We considered OCIO's technical comments and the Office of General Counsel's report and made changes to our final report, where appropriate. We are pleased that the Department generally concurs with our findings and recommendations, and look forward to reviewing its proposed audit action plan.

Appendix A: Objectives, Scope, and Methodology

On June 28, 2018, we initiated research regarding security controls implemented to protect the Department's EWS system. The objective of this research was to identify the types of information maintained on the Department's EWS system and determine if appropriate security controls to protect this system had been implemented. The intent of our research was to better understand the EWS system's current cybersecurity posture and determine if further audit work was needed.

Based upon the results of our research, we initiated an audit on December 19, 2018. Our audit objectives were to determine whether the (1) processes used to vet contract staff given administrative access to the EWS system are adequate; (2) Department followed a sufficient process to identify the impact level of the EWS system; (3) OCIO took appropriate actions to protect the information on the EWS system after it was granted an authorization to operate in 2018; and (4) contract used to procure EWS services and systems complied with Department acquisition regulations.

We briefed the Department's Acting CIO regarding conditions we identified during the survey portion of our work related to issues identified in findings II and III on February 5, 2019. We also briefed the Acting CIO about conditions identified related to findings I, II, III, and IV on April 9, 2019.

We interviewed Department officials responsible for operating, securing, and managing the contract for this system, and reviewed system security documentation.

To do so, we

- reviewed system-related artifacts, including policy and procedures, planning documents, and security control documentation;

- retrieved, analyzed, and correlated system logs and other artifacts regarding the EWS system; and

- interviewed Department officials, including system owners, IT security and operations staff, and management.

We reviewed the Department's compliance with the following applicable internal controls, provisions of law, and mandatory guidance:

- Federal Information Processing Standard (FIPS) PUB 199, *Standards for Security Categorization of Federal Information and Information Systems*

- Pub. L. No. 113-283, *The Federal Information Security Modernization Act of 2014*

- NIST Special Publications:

  o 800-37, Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*

  o 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*

  o 800-53A, Rev. 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*

  o 800-60, Vol. I, Rev. 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*

  o 800-60, Vol. II, Rev. 1, *Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories*

We collected computer-generated data directly from Department systems, including system logs and application user lists. We determined that the data were sufficiently reliable for the purposes of this report.

We conducted our review from June 2018 through July 2019 under the authority of the Inspector General Act of 1978, as amended (5 U.S.C. App.), and Department Organization Order 10-13, April 26, 2013. We performed our fieldwork at Department of Commerce headquarters in Washington, DC.

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

Appendix B: Agency Response

UNITED STATES DEPARTMENT OF COMMERCE
Chief Information Officer
Washington, D.C. 20230
DEC 1 8 2019

MEMORANDUM FOR: Peggy E. Gustafson
                Inspector General

FROM: André V. Mendes
                Acting Chief Information Officer
                and Authorizing Official

ANDRE MENDES

Digitally signed by
ANDRE MENDES
Date: 2019.12.18
10:21:37 -05'00'

SUBJECT: Notification of Department of Commerce Response to the Inspector
                General's Draft Report, *Failures in the Department's Security
                Program Resulted in Exposure of Sensitive Trade Information to
                Unvetted Foreign National.*

This memorandum transmits the Department's response to the draft Office of Inspector General
(OIG) report "*Failures in the Department's Security Program Resulted in Exposure of Sensitive
Trade Information to Unvetted Foreign Nationals.*"

The Office of the Secretary generally concurs with the IT audit findings and the
recommendations provided within the draft report. However, the Department's Office of the
Chief Information Officer has reviewed the draft and offers the attached comments for OIG's
consideration.

Thank you for the opportunity to review this draft. Should you have any questions, please
contact Bharat Dass, Office of Cyber Security and IT Risk Management, at bdass@doc.gov or
202-482-6046.

Attachment

cc: Jun Kim
    Antoinette Brown
    Nathan Thweatt
    William Bradd
    Michelle Barnes
    Michael Bonner
    Michelle Holland
    Jim Eatmon

011200000337