U.S. DEPARTMENT OF TRANSPORTATION

OFFICE OF INSPECTOR GENERAL

The Maritime Administration's Information Technology Infrastructure Is at Risk for Compromise

FOR OFFICIAL USE ONLY

PUBLIC AVAILABILITY TO BE DETERMINED UNDER THE FREEDOM OF INFORMATION ACT, 5 U.S.C. § 552.

MARAD

Report No. FI2019057

July 24, 2019

U.S. DEPARTMENT OF TRANSPORTATION
OFFICE OF INSPECTOR GENERAL

Highlights

The Maritime Administration's Information Technology Infrastructure Is at Risk for Compromise

Self-initiated

Maritime Administration | FI2019057 | July 24, 2019

What We Looked At

The Maritime Administration's (MARAD) programs promote waterborne transportation and integration with other transportation modes and the viability of the U.S. Merchant Marine. MARAD works in many areas, including ship building and shipping, vessel and port operations, national security, and transportation safety. The Agency has 12 information systems and 1 local area network—excluding the U.S. Merchant Marine Academy's systems, which we did not include in our audit. MARAD also uses a number of web applications, some of which contain sensitive data and personally identifiable information (PII). We conducted this audit because of the importance of MARAD's programs to the Nation's transportation system and the sensitive nature of some of the Agency's information. Accordingly, our objective for this self-initiated audit was to determine whether MARAD's IT infrastructure contains security weaknesses that could compromise the Agency's systems and data.

What We Found

Through an old vulnerability that we identified, we gained unauthorized access to MARAD's network using a basic hacker technique. MARAD did not detect our access or our placement of hacking tools on the network, in part because it did not have an alert system configured to do this, which the National Institute of Standards and Technology (NIST) recommends. Using another hacker technique, we gained access to [redacted] records containing PII. While DOT policy requires the use of encryption to protect sensitive data, these records and other data we obtained were not encrypted. Had malicious attackers obtained these records, they could have used them to steal citizens' identities and MARAD could have lost $103 million in credit monitoring fees. Furthermore, the Agency does not always remediate vulnerabilities as quickly as DOT policy requires, and inadequate security awareness training may contribute to some personnel's susceptibility to social engineering. Lastly, MARAD's physical security controls did not prevent the installation of [redacted] These weaknesses, individually and together, put MARAD's network and data at risk for unauthorized access and compromise.

Our Recommendations

We made 8 recommendations to MARAD and 11 recommendations to OST. The Department concurred with all 19 recommendations. We consider all 19 recommendations resolved but open pending completion of planned actions.

Contents

U.S. DEPARTMENT OF TRANSPORTATION
OFFICE OF INSPECTOR GENERAL

Memorandum

Date: July 24, 2019

Subject: INFORMATION: The Maritime Administration's Information Technology Infrastructure Is at Risk for Compromise | Report No. FI2019057

From: Louis C. King
Assistant Inspector General for Financial and IT Audits

To: MARAD Chief Information Officer
DOT Chief Information Officer

The Maritime Administration's (MARAD) programs promote waterborne transportation and integration with other transportation modes and the viability of the U.S. Merchant Marine. MARAD works in many areas, including ship building and shipping, vessel and port operations, national security, and transportation safety. The Agency has 12 information systems and 1 local area network—excluding the U.S. Merchant Marine Academy's systems, which we did not include in our audit. MARAD also uses a number of web applications, some of which contain sensitive data and personally identifiable information (PII).[1] Information systems must be properly protected to prevent unauthorized access to data and systems.

Due to the importance of MARAD's programs to the Nation's transportation system and the sensitivity of some of the Agency's information, we conducted this audit of MARAD's information technology (IT) infrastructure. Our objective was to determine whether security weaknesses exist in MARAD's IT infrastructure that could lead to the compromise of MARAD's systems and data. During our audit, MARAD officials informed us that the Office of the Secretary of Transportation's (OST) Information Technology Shared Services (ITSS) manages MARAD's workstations. We therefore included the ITSS-managed workstations in our tests.

[1] Information that can be used to identify an individual, such as name, social security number, biometric records, in combination with other personal information, such date and place of birth, or mother's maiden name.

We conducted this audit in accordance with generally accepted Government auditing standards. Exhibit A details our scope and methodology and exhibit B lists the entities we visited or contacted.

We appreciate the courtesies and cooperation of Department of Transportation (DOT) representatives during this audit. If you have any questions concerning this report, please call me at (202) 366-1407, or Abdil Salah, Project Director, at (202) 366-8543.

cc: The Secretary
MARAD Audit Liaison, MAR-392
DOT Audit Liaison, M-1

Results in Brief

MARAD's IT infrastructure is not secure from compromise.

Through an old vulnerability that we identified, we gained unauthorized access to MARAD's network using a basic hacker technique. Per DOT policy, this vulnerability should have been remediated several years ago. MARAD did not detect our access or our placement of hacking tools on the network, in part because it did not have an alert system configured to do this, which the National Institute of Standards and Technology (NIST) recommends. Using another hacker technique, we gained access to [redacted] records containing PII. While DOT policy requires the use of encryption to protect sensitive data, these records and other data we obtained were not encrypted. An OST official could not explain why employees did not encrypt sensitive information since the information security awareness training they received included a section on the protection of sensitive information. Had malicious attackers obtained these records, they could have used them to steal citizens' identities and MARAD could have lost $103 million in credit monitoring fees. Furthermore, we found that the Agency does not always remediate vulnerabilities as quickly as DOT policy requires. On MARAD's [redacted] servers, we identified [redacted] critical and [redacted] high vulnerabilities.[2] On [redacted] workstations that OST's ITSS manages, we identified [redacted] critical and [redacted] high vulnerabilities. Sixty-five percent of these critical vulnerabilities and 32 percent of the high vulnerabilities were over a year old. DOT policy requires remediation of critical and high vulnerabilities within 30 days of detection. An OST official attributed some of these vulnerabilities to old systems that OST has modernized since our audit. We also found that inadequate security awareness training may contribute to some personnel's susceptibility to social engineering, and that physical security controls did not prevent the installation of [redacted] These weaknesses, individually and together, put MARAD's network and data at risk for unauthorized access and compromise.

We are making recommendations to assist MARAD and OST in securing their data and systems.

[2] Critical vulnerabilities require immediate attention because they are relatively easy for attackers to exploit and may provide full control of affected systems. High vulnerabilities are more difficult to exploit but their exploitation can result in significant data loss or downtime.

[redacted]

Background

MARAD's mission is to promote and maintain the national maritime industry. This industry consists of a network of ports, shipyards, waterways, shippers, and carriers that participate in domestic and international waterborne commerce. MARAD also focuses on marine transportation policies to improve security, address the Nation's maritime infrastructure gaps, and use technology to meet the needs of the marine transportation system.

MARAD maintains a variety of information systems to support its mission and operations. Four systems contain PII—[redacted].

OST's ITSS provides management services for MARAD's workstations, wireless access, websites, and network and system security to protect data and devices. MARAD's employees and contractors operate and maintain the servers and databases for MARAD information systems.

DOT's Cybersecurity Compendium[5] and other departmental policy state standards, processes, and procedures for the Department's information system security. MARAD's security policies and processes must adhere to these departmental policies, as well as NIST's guidelines.

The Compendium requires users of all departmental systems to complete and sign the DOT Rules of Behavior. These Rules of Behavior require users to

- choose passwords that are at least 12 characters long and have a combination of letters (upper and lower case), numbers, and special characters;
- protect passwords and personal identification numbers for logons from disclosure, not record passwords or access control numbers on paper or in electronic form, or store them on or with DOT workstations, laptop computers, or portable electronic devices; and
- not provide personal or official DOT information solicited by e-mail, and forward to the appropriate DOT security help desk any e-mail requesting

[redacted]

[5] DOT, *Cybersecurity Compendium*, 2018.

personal information, or account or security settings verifications, and then delete the email.

DOT's Cybersecurity Compendium and NIST guidelines[6] also require that DOT operating administrators use strong passwords, implement automated incident detection and response tools,[7] and use encryption to prevent unauthorized disclosure of information during transmission. They also require Operating Administrations (OA) to protect PII, employ the principle of least privilege,[8] conduct periodic exercises against security awareness training, and monitor for physical access.

DOT policy[9] also requires technical, physical and administrative safeguards to protect PII collected or maintained by the Department regardless of format or media. This policy also calls for OAs to protect all records against reasonably anticipated threats and hazards that could result in harm, embarrassment, inconvenience, or unfairness to individuals about whom PII is maintained. At a minimum, all PII must be protected with controls that provide moderate confidentiality.[10]

MARAD's IT Infrastructure and Information Are Not Secure From Compromise

Using a [redacted], we were able to gain access to MARAD's network. We then used a common hacking technique to obtain a username and password that allowed us to access unencrypted PII. [redacted]

[6] NIST Special Publication 800-53 Rev. 4, 2015.
[7] These tools provide incident detection and monitoring for IT systems to detect and prevent intrusions.
[8] A principle that states that users should have access only to the programs and systems necessary to complete their assigned tasks. The military rule of "need-to-know" is an example of this principle.
[9] Chief Information Officer Departmental Privacy Risk Management Policy 1351.8 18.4.7, 2014.
[10] Moderate confidentiality complies with Federal Information Processing Standard 199.

Using an Old Vulnerability, We Gained Access to MARAD's Network

Because MARAD was not following DOT policy and NIST guidelines on vulnerability mitigation, password establishment, and monitoring, we gained unauthorized access to the Agency's network and systems. We found a known high vulnerability, [redacted] —and gain access to the device's administrator account.[12] Using this administrator account, we installed hacking tools on the device. MARAD did not detect our unauthorized access.

DOT policy[13] requires remediation or mitigation of IT vulnerabilities within 30 days of detection for critical and high vulnerabilities. NIST guidelines and DOT policy also call for agencies to require the use of strong passwords—ones that include, for example, a minimum number of characters and mixes of upper and lower case letters, numbers, and special characters. NIST also recommends not using easily-guessed passwords. DOT policy requires agencies use automated incident detection and response tools for IT systems.

When we asked why MARAD was not following password requirements, an OST official explained that these requirements are managed through group policy—a technology within Microsoft Windows used to centrally manage and control user and computer settings for IT infrastructure. The OST official stated further that it was possible that without authorization, an employee with a privileged account[14] made a password change that deviated from the group policy's password complexity requirements. However, OST has provided no evidence that an employee actually made such an unauthorized change. [redacted]

[redacted].

[12] Administrators' access allows them to view system information and perform maintenance tasks such as upgrades.
[13] DOT, *Security Weakness Management Guide*, March 2018.
[14] A system account with authorizations to perform security-relevant functions that ordinary users are not authorized to perform.

[redacted]

Vulnerabilities in MARAD's Network Expose It and the PII It Contains to Compromise

Vulnerabilities, including a lack of encryption, expose MARAD's network and the PII it contains to unauthorized access. [redacted]. We then accessed:

- accounts and PII for all MARAD users;
- some OST accounts that gave us access to executives' PII;
- databases and files containing [redacted] unencrypted PII records, including contact and medical information, and license information for mariners; and
- databases that contained unencrypted social security numbers for midshipmen and cadets in the Merchant Marine Academy and MARAD employees.

MARAD administrators also had not adequately protected passwords to devices and applications such as those that manage network storage, power supplies, temperature sensors, and network traffic. [redacted]. We also found a list of OST accounts for 34 executives and staff that joined the Agency during the change in the Presidential Administration. The users of thirteen of these 34 accounts—which were assigned in January 2017—had not changed their temporary account passwords to

[redacted]

permanent ones. We then used one of these accounts to access OST network drives and found unencrypted files containing PII [redacted]

DOT policy requires OAs to use encryption to prevent unauthorized disclosure of sensitive information during transmission, and to employ least privilege controls. Furthermore, the policy requires technical, physical, and administrative safeguards to protect PII. Lastly, the policy requires that users adequately protect passwords, and change temporary passwords during first logon.

An OST official could not explain why employees did not encrypt sensitive information since the information security awareness training they received included a section on the protection of sensitive information. This OST official also could not explain why administrators had not applied least privilege controls to the MARAD service account we accessed. The same OST official acknowledged that users were not following DOT policy and security awareness training to adequately protect passwords. The official informed us that OST is transitioning to the use of personal identification verification cards[17] for network and facility access.

MARAD's lack of adherence to DOT policy on encryption, use of least privilege, protection of PII, and password storage creates a risk for unauthorized access to MARAD and other OA information. If our attacks had been malicious, the damage could have required credit monitoring for affected individuals, costing $41.73 per person and approximately 103,073,100 in tax dollars.[18] Citizens' identities could also have been stolen, causing victims serious financial and emotional distress. Furthermore, the disclosure of [redacted] PII, [redacted], could cause serious public embarrassment to the Department.

[17] A physical artifact, such as an identity card or a smart card, issued to Federal employees and contractors that contains stored credentials, such as photographs, cryptographic keys, or digitized fingerprint representations, so that the cardholder's claimed identity can be verified against the stored credentials by another person or an automated process.

[18] We calculated the credit monitoring cost per person per year to be $41.73, based on an average of three vendors providing identity protection services on the General Services Administration's blanket purchase agreement. The single year cost that could result from a compromise of 2.47 million PII records would total $103,073,100 ($41.73 times 2.47 million).

MARAD Does Not Remediate Vulnerabilities in Its Servers and Workstations in a Timely Manner

MARAD's and OST's vulnerability management does not remediate vulnerabilities, including critical ones, as quickly as DOT policy requires. The policy requires remediation or mitigation of critical and high vulnerabilities within 30 days of detection. On MARAD's [redacted] servers, we identified [redacted] critical and [redacted] high vulnerabilities. On [redacted] workstations that OST's ITSS manages, we identified [redacted] critical and [redacted] high vulnerabilities. Sixty-five percent of these critical vulnerabilities and 32 percent of the high vulnerabilities were over a year old. We also found that 23 percent of MARAD's [redacted] websites had [redacted] vulnerabilities [redacted]. MARAD officials informed us that the Agency was in the process of transitioning to new websites and shutting down the old ones. However, the Agency is still responsible for maintaining a reasonable degree of security over the old websites until they are no longer in use.

MARAD officials also informed us that the Agency was not aware of all the vulnerabilities we detected, and that it is coordinating with DOT to investigate them. Furthermore, an OST official informed us that some of the vulnerabilities we identified in servers and workstations may be attributable to old systems that OST has modernized since our audit. However, OST has not provided evidence of which vulnerabilities were attributable to these old systems.

This OST official also informed us that the Department and MARAD cannot reproduce all our vulnerability scanning results because of either differences in tools or the absence of a specific capability in the Department's security architecture.

We do not agree that the results of our vulnerability scanning of servers and workstations are not reproducible due to differences in tools. DOT policy requires OAs to scan for system vulnerabilities using tools that produce assessment results and assign a severity to each weakness based on the common vulnerability expression (CVE).[19] A variety of tools comply with these requirements. For our server and workstation scanning, we used Tenable Nessus—a tool that DOT uses. For the websites, we used Acunetix, which the Department does not use. We have provided the Department with the CVEs and the names of the affected servers

[19] A dictionary-type list of standardized names for vulnerabilities and other information related to security exposures to allow for easy sharing of data across separate vulnerability databases and security tools. The list is maintained by the federally funded national cybersecurity research and development center operated by MITRE Corp.

and workstations. The OST official further stated that the Department would address weaknesses identified by its scanning software. A MARAD official informed us that the Department would research the vulnerabilities we discovered.

OST has not provided evidence that the absence of a specific capability in the Department's security architecture could cause the inability to reproduce our scanning results.

MARAD's and OST's lack of adherence to DOT policy on security vulnerability mitigation puts servers and workstations, information systems, and sensitive information at risk for compromise.

MARAD Personnel Are Vulnerable to Social Engineering

MARAD personnel are vulnerable to social engineering emails.[20] We performed two social engineering tests—phishing and spear phishing.

- **Phishing.**[21] In this test, we sent emails to 226 users.[22] Fifty-three (23 percent) responded and provided their usernames and passwords. We surveyed the 53 and asked why they had responded to the email; 40 did not respond to our survey, 2 denied submitting any information, 7 said the emails appeared valid, 3 did not recall the emails, and 1 recalled the email but not that he/she responded to it.

- **Spear phishing.**[23] In this test, we sent emails to 10 specific users.[24] Three users opened the emails, clicked on the links, and disclosed their usernames and passwords. Of the three, one could not remember submitting information, one denied submitting information, and one said he/she was in a hurry.

DOT policy requires all personnel to take annual security awareness training that addresses security exposures such as social engineering. The employees in our tests completed DOT's 2018 security awareness training. The training identified

[20] Deceptive emails meant to cause the recipients to violate security procedures and provide to the attackers proprietary information such as passwords and account numbers.
[21] An attempt by an untrustworthy entity using electronic communication to obtain sensitive information such as usernames, passwords, and credit card details.
[22] We sent emails to 43 percent of MARAD's 526 users.
[23] Phishing directed at a specific individual.
[24] We identified these users from a list of personnel on MARAD's public website.

phishing as a security concern and contained an example on phishing, but did not contain an example of spear phishing or scenarios of either. These omissions may have contributed to the rate of response to our phishing tests.

DOT policy also requires OAs to conduct periodic exercises to determine whether personnel are applying the policies learned during security awareness training. These exercises may include sending emails that contain suspicious links and requesting sensitive information by telephone. MARAD officials stated that OST had conducted a phishing test on MARAD staff and that management was confident that MARAD staff could recognize emails that they should not respond to. However, 23.7 percent of the employees we sent our test emails responded incorrectly.

Had our phishing tests actually come from an attacker, the emails would have allowed the attacker to gain access to and compromise MARAD's network.

MARAD's Physical Security Controls Are Not Sufficient to Prevent Installation of [redacted]

MARAD's physical security controls for offices and workstation computers did not prevent our installation of [redacted] on the Agency's systems. Using a bypass tool,[25] we entered one user's locked office and installed a [redacted] on the workstation. [redacted]. The workstation users did not detect the [redacted] for a week. [redacted], we gathered sensitive data, including personal identification numbers, usernames, and passwords on computers that did not require access using personal identity verification cards, and login information to websites.

NIST guidelines and DOT policy require agencies to monitor physical access to information systems to detect and respond to physical security incidents, including ones that may result from the installation of [redacted]. Additionally,

[25] A tool used to defeat a door's lock without actually operating the lock.

industry best practice[26] recommends using whitelisting[27] tools to detect [redacted] and mitigate their effects. The industry best practice also recommends monitoring computer file systems for modifications to the Windows Registry and driver installation. The Windows Registry serves as an archive for collecting and storing configuration settings of Windows components, and installed hardware and software. A driver is a software component that lets Microsoft Windows and a hardware device—[redacted]—communicate with each other. [redacted] can modify the Windows Registry and install device drivers. An organization that monitors its file systems may detect these modifications and [redacted].

[redacted] have been used in successful data breaches in both private industry and the public sector. For instance, in 2015, a large insurance company had approximately 80 million records stolen when an attacker convinced 5 users to install [redacted]. However, DOT's annual security awareness training does not include information on [redacted] and the damage that their installation on Federal workstations can cause.

An OST official informed us that that OST has implemented a "layered defense" against [redacted] at MARAD workstations, and that the Agency's facilities security program determines which controls and countermeasures are implemented. The official also stated that MARAD's building security was operating as designed and that we were granted access to the facility within the operational parameters of that design. The official stated further that the only physical security control we tested was the door lock on a closed office.

However, we conducted this test as an "insider"[28] attack that simulated [redacted] installation that any employee at DOT headquarters could do on MARAD workstations. Our test demonstrated that MARAD lacked a software solution to detect and [redacted], and that insider threats could exist at the Agency.

MARAD's and OST's current weaknesses in physical security create the risk that attackers, including insiders, can capture sensitive data on MARAD's computers, such as usernames, passwords and personal identification numbers, and use this information to gain unauthorized access to MARAD systems.

---

[26] MITRE Corp., John Lambert, *The MITRE Att&ck Framework - Input Capture*, 2018.

[27] An application whitelist is a list of applications and application components that are authorized for use in an organization. Application whitelisting technologies use whitelists to control which applications are permitted to execute on a host, helping to stop the execution of malware, unlicensed software, and other unauthorized software.

[28] An entity or individual with authorized access that could harm an information system or enterprise through destruction, disclosure, modification of data, and/or denial of service.

Conclusion

MARAD uses a large amount of sensitive information—residing on a network that is connected to the Department's network—to complete its mission. As our tests have demonstrated, MARAD's network has serious vulnerabilities that create a risk that hacking attempts against the network will succeed. Furthermore, once compromised, MARAD's information can provide access to interconnected networks.

Recommendations

To improve the security of MARAD's IT infrastructure, we recommend Maritime Chief Information Officer (CIO):

1. Change the password for the compromised server management device account to a strong password that meets DOT's Cybersecurity Compendium requirements and NIST guidelines.
2. Configure alerts on server management devices to notify staff of unusual activity and when the system reboots.
3. Change the password for the compromised MARAD service account.
4. In coordination with DOT CIO develop and implement a training program for administrators to adequately protect passwords that includes the DOT Policy requirement to not record passwords in electronic form.
5. Encrypt PII data on personal and network drives in accordance with DOT Chief Information Officer Departmental Privacy Risk Management Policy.
6. [redacted]
7. Develop a plan and address identified high and medium vulnerabilities on any remaining legacy websites and verify that new websites are being assessed for vulnerabilities.
8. In coordination with DOT CIO develop and implement a training program for MARAD personnel who provided credentials during the phishing test on security awareness, with a focus on phishing attacks.

To further improve the security of MARAD's IT infrastructure, we recommend Department of Transportation CIO:

9. Update the departmental annual security awareness training to include information on encryption using approved technological methods.

10. Change the passwords for OST's compromised social media accounts.

11. Change the passwords for MARAD's compromised social media accounts managed by OST.

12. Change the temporary passwords for the executives and staff that joined the Department during the change in the Presidential Administration.

13. Encrypt PII data on personal and network drives in accordance with DOT Chief Information Officer Departmental Privacy Risk Management Policy.

14. Examine service account permissions and remove unnecessary rights using the principle of least privilege so that service accounts have access to intended resources.

15. Develop a plan and address identified critical and high vulnerabilities on MARAD workstations managed by OST that are older than June 19, 2017 (1 year prior to the ending of our scanning period).

16. Update fiscal year 2019 Department of Transportation Security Awareness Training to include spear phishing and phishing examples and scenarios.

17. Update fiscal year 2019 Department of Transportation Security Awareness Training to include information about [redacted] and their detection.

18. Incorporate a routine step for IT help desk personnel to check for [redacted] any time request for assistance requires a technician to physically service a workstation.

19. Implement a software solution that would assist in the detection of [redacted] and the prevention of [redacted] installation and operation.

Agency Comments and OIG Response

We provided the Department with our draft report on May 17, 2019, and received its formal response on July 1, 2019. The Department's response is included in its entirety as an appendix to this report. In its response, the Department concurred

with all 19 our recommendations and provided appropriate actions and completion dates for implementing the recommended actions.

Actions Required

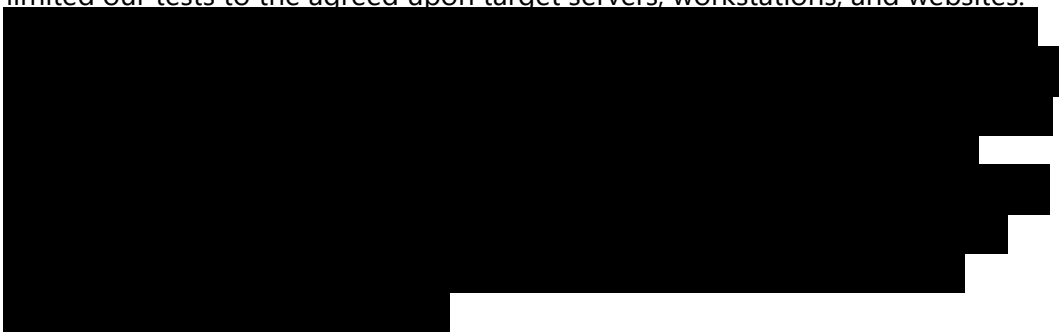
We consider all 19 recommendations resolved but open pending completion of planned actions.

Exhibit A. Scope and Methodology

We performed our network security assessment between March 2018 and May 2019, at DOT Headquarters in Washington, DC. We conducted this 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.

Our objective was to determine whether security weaknesses exist in MARAD's IT infrastructure that could lead to the compromise of the Agency's systems and data.

To accomplish our objective, we performed a series of internal and external vulnerability assessments and penetration tests on MARAD's workstations, servers, infrastructure devices, and websites. Per Rules of Engagement (ROE), we limited our tests to the agreed upon target servers, workstations, and websites.



To address our audit objectives, we used NIST Special Publication 800-115, *Technical Guide to Information Security Testing and Assessment*, to perform a penetration test and vulnerability assessment of the MARAD IT infrastructure using widely available tools and techniques. Specific test dates and targets were agreed upon in a signed ROE prior to conducting our tests.

We conducted the internal assessment inside MARAD's network, behind MARAD's firewalls, with full knowledge of MARAD's IT infrastructure as agreed to in the ROE. We used OIG-owned and licensed hardware and software, including Tenable Nessus and Acunetix for vulnerability scanning. We also used open source software including Kali Linux and GoPhish. During our tests, we notified

MARAD information security staff of issues we discovered and believed were indicative of serious problems that would require immediate attention.

We coordinated with MARAD and ITSS management staff to conduct our physical security and social engineering tests. We conducted limited tests of physical security by attempting to enter MARAD employees' offices and install [redacted] While at Office of Inspector General (OIG) Headquarters, we performed social engineering tests by email to determine whether MARAD's employees were susceptible to phishing attacks.

We performed external vulnerability assessments of MARAD's websites from OIG Headquarters using OIG hardware and software and information available to the general public. In accordance with the Announcement Letter we excluded U.S. Merchant Marine Academy systems, and, per the ROE, did not use tests that could adversely affect operations and result in denial of service to MARAD employees and customers.

Upon completion of our tests, we provided MARAD's information technology audit liaison with the reports generated by our automated assessment tools so that MARAD could take timely corrective actions. The reports provided details on the vulnerabilities we detected and exploited, and the necessary actions suggested by the tools we used to resolve the vulnerabilities. After our testing, we briefed MARAD management on our activities and the access we had gained, including our analysis of the issues reported by the tools we used.

While staying within the bounds of the scope laid out in the ROE, we conducted additional testing to determine whether we could access OST resources. We used the same tools and techniques that we applied during our test of MARAD's infrastructure.

Exhibit B. Organizations Visited or Contacted

Department of Transportation

Maritime Administration, DOT Headquarters, Washington, DC

Office of the Chief Information Officer, DOT Headquarters, Washington, DC

Exhibit C. List of Acronyms

CIO	Chief Information Officer
CVE	common vulnerability expression
DOT	Department of Transportation
IT	information technology
ITSS	Information Technology Shared Services
MARAD	Maritime Administration
NIST	National Institute of Standards and Technology
OA	Operating Administration
OIG	Office of Inspector General
OST	Office of the Secretary of Transportation
PII	personally identifiable information
ROE	Rules of Engagement

Exhibit D. Major Contributors to This Report

ABDIL **SALAH**	PROGRAM DIRECTOR
DANIEL **JOPLIN**	PROJECT MANAGER
ZACHARY **LEWKOWICZ**	IT SPECIALIST
JUSTIN **UBERT**	IT SPECIALIST
ANTIONE **SEARCY**	IT SPECIALIST
RIFAT **MAJUMDAR**	IT SPECIALIST
SUSAN **NEILL**	WRITER-EDITOR
AMY **BERKS**	SENIOR COUNSEL

Appendix. Agency Comments

Memorandum

U.S. Department of Transportation

Office of the Secretary of Transportation

Subject: INFORMATION: Management Response to Office of Inspector General Report – The Maritime Administration's Information Technology Infrastructure

From: Andrew R. Orndorff
Associate CIO / Chief Information Security Officer
ANDREW R ORNDORFF Digitally signed by ANDREW R ORNDORFF Date: 2019.07.01 15:57:45 -04'00'

To: Louis C. King
Assistant Inspector General
for Financial and Information Technology Audits

The practices of good cybersecurity hygiene and protection of sensitive information on agency networks and systems are fundamental elements of the Department of Transportation's (DOT) cybersecurity program. DOT is committed to continued management attention upon the cost-effective improvement of controls, enhancement of cybersecurity capabilities, and maturation of DOT policy, processes, and governance to ensure the mitigation of risks and the remediation of weaknesses and vulnerabilities. The DOT Office of the Chief Information Officer (OCIO) and the Maritime Administration (MARAD) have already addressed and mitigated several risks through enterprise commodity Information Technology (IT) realignment and migration to enterprise shared service solutions.

Based on our review of the draft report, we concur with the 19 recommendations, as written, and plan to implement the recommendations by the following dates:

Recommendation Number	Target Action Completion Date
1, 2, 3, 10, 11 and 12	July 15, 2019
16, 17 and 18	August 15, 2019
7	September 30, 2019
9 and 6	October 31, 2019
8	December 31, 2019
4, 5, 13, 14, 15 and 19	September 30, 2020

We appreciate the opportunity to review the OIG draft report. Please contact Andrew R. Orndorff, Associate CIO/Chief Information Security Officer, at 202-366-7111 with any questions.

U.S. DOT OIG Fraud & Safety Hotline

hotline@oig.dot.gov | (800) 424-9071

https://www.oig.dot.gov/hotline

Our Mission

OIG conducts audits and investigations on behalf of the American public to improve the performance and integrity of DOT's programs to ensure a safe, efficient, and effective national transportation system.

OFFICE OF INSPECTOR GENERAL
U.S. Department of Transportation
1200 New Jersey Ave SE
Washington, DC 20590

www.oig.dot.gov