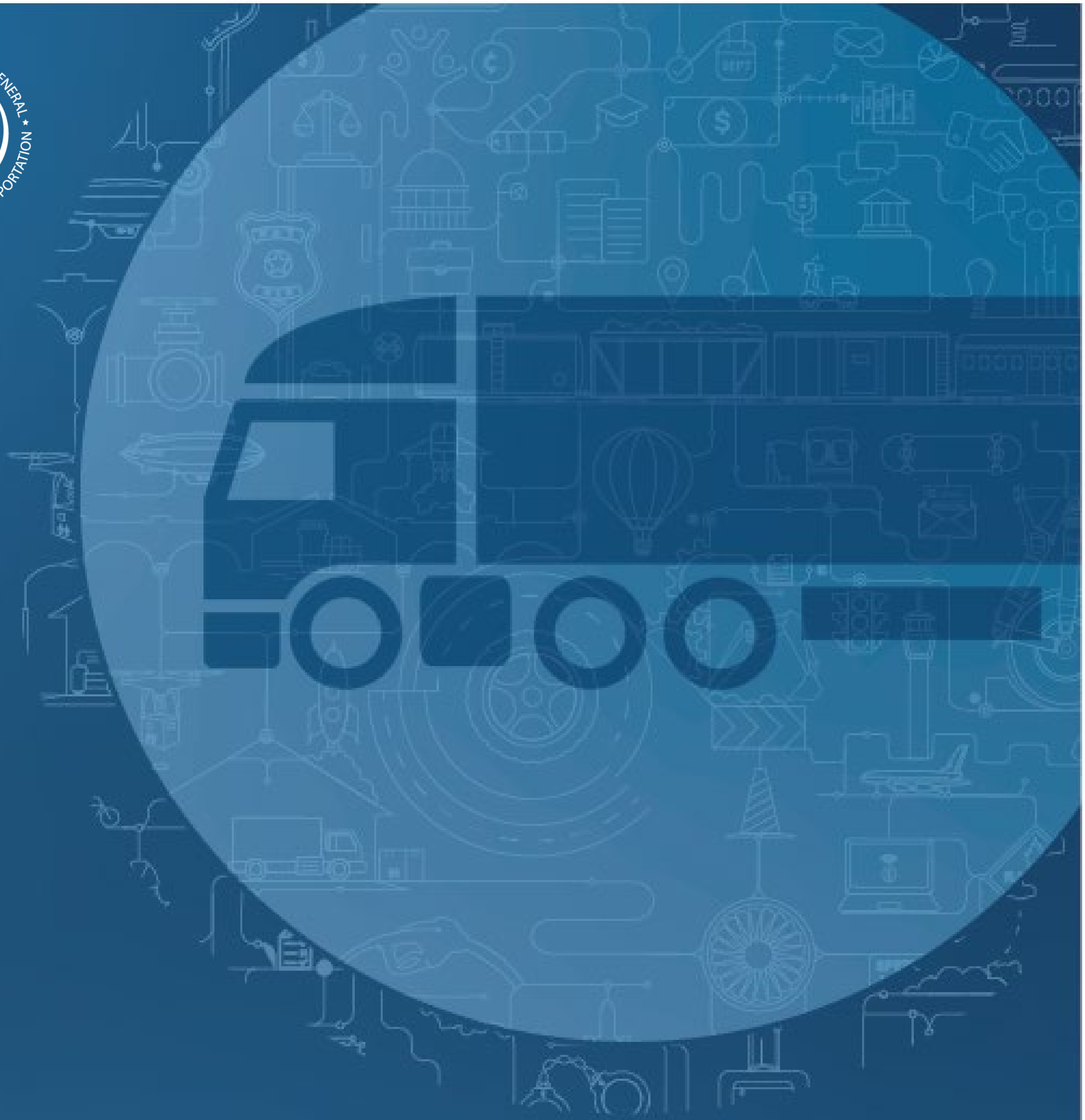
OFFICE OF INSPECTOR GENERAL
U.S. DEPARTMENT OF TRANSPORTATION



FMCSA

Report No. IT2022003
October 20, 2021

FMCSA's IT 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.

U.S. Department of Transportation
Office of Inspector General

Highlights

FMCSA's IT Infrastructure Is at Risk of Compromise

Self-Initiated

Federal Motor Carriers Safety Administration | IT2022003 | October 20, 2021

What We Looked At

The Federal Motor Carrier Safety Administration (FMCSA) regulates and oversees the safety of commercial motor vehicles. It partners with other agencies and the motor carrier industry to conduct this work. The Agency uses 13 web-based applications to aid vehicle registration, inspections, and other activities. Many of FMCSA's information systems contain sensitive data, including personally identifiable information (PII). Due to the importance of FMCSA's programs to the transportation system and sensitivity of some Agency information, we conducted this audit of FMCSA's information technology (IT) infrastructure. Our objective was to determine whether FMCSA's IT infrastructure contains security weaknesses that could compromise the Agency's systems and data.

What We Found

We found [redacted] several Agency web servers which allowed us to gain unauthorized access to FMCSA's network. FMCSA did not detect our access or placement of malware on the network in part because it did not use required automated detection tools and malicious code protections. [redacted] We also gained access to 13.6 million unencrypted PII records. Had malicious hackers obtained this PII, it could have cost FMCSA up to $570 million in credit monitoring fees. Furthermore, the Agency does not always remediate vulnerabilities as quickly as DOT policy requires. These weaknesses put FMCSA's network and data at risk for unauthorized access and compromise.

Our Recommendations

FMCSA concurred with our 13 recommendations. We consider all 13 recommendations resolved but open pending FMCSA's completion of planned actions.

All OIG audit reports are available on our website at www.oig.dot.gov.

For inquiries about this report, please contact our Office of Legal, Legislative, and External Affairs at (202) 366-8751.

Contents

U.S. Department of Transportation
Office of Inspector General

Memorandum

Date: October 20, 2021

Subject: INFORMATION: FMCSA's IT Infrastructure Is at Risk for Compromise | Report No. IT2022003

From: Kevin Dorsey
Assistant Inspector General for Information Technology Audits

To: Federal Motor Carrier Safety Administrator
DOT Chief Information Officer

The Federal Motor Carrier Safety Administration (FMCSA) is responsible for regulating and overseeing the safety of commercial motor vehicles. To conduct this work, FMCSA partners with other stakeholders, including Federal, State, and local law enforcement agencies, the motor carrier industry, safety groups, and organized labor. FMCSA's core information system applications—hosted in the cloud[1]—support the Agency's mission processes. The Agency uses 13 web-based applications,[2] [redacted], to aid vehicle registration, inspections, compliance monitoring, and enforcement. Many of FMCSA's information systems contain sensitive data, including personally identifiable information (PII).

Due to the importance of FMCSA's programs to the Nation's transportation system and the sensitivity of some of the Agency's information, we conducted this audit of FMCSA's information technology (IT) infrastructure. Our objective was to determine whether security weaknesses exist in FMCSA's IT infrastructure that could lead to the compromise of the Agency's systems and data. This audit is the third in a planned series of reviews the Office of the Inspector General (OIG) is conducting of the Department's Operating Administrations (OA) and components

[1] Cloud computing is the on-demand availability of computer systems resources without the user's direct active management.

[2] A web-based application is a type of software that allows users to interact with a remote server through a web browser interface.

IT infrastructure and cybersecurity posture[3] to determine if Department of Transportation (DOT) has the appropriate security controls[4] in place to protect its networks and information systems from unauthorized access.

We conducted this audit in accordance with generally accepted Government auditing standards. We reviewed FMCSA's network documentation and security policies and performed assessments of FMCSA's entire IT infrastructure, including penetration tests, vulnerability scans, and manual tests. We also interviewed FMCSA personnel. Exhibit A details our scope and methodology and exhibit B lists the entities we visited or contacted. Exhibit C presents a list of acronyms used in this report and exhibit D presents a glossary of terms.

We appreciate the courtesies and cooperation of DOT representatives during this audit. If you have any questions concerning this report, please call me at (202) 366-1518, or Leon Lucas, Program Director, at (202) 366-0377.

cc: The Secretary
FMCSA Audit Liaison, MC-PRS
DOT Audit Liaison, M-1

[3] *The Volpe Center's Information Technology Infrastructure Is at Risk for Compromise* (Report No. FI2016056), March 22, 2016; *The Maritime Administration's Information Technology Infrastructure Is at Risk for Compromise* (Report No. FI2019057), July 24, 2019.

[4] Security controls are the safeguards or countermeasures prescribed for information systems or organizations designed to protect the confidentiality, integrity, and availability of information that is processed, stored or transmitted by the systems or organizations, and to manage information security risk.

Results in Brief

FMCSA's IT infrastructure and information is at an increased risk of compromise.

We found [redacted] several Agency web servers which allowed us to gain unauthorized access to FMCSA's network using a basic hacker technique. According to DOT policy, OAs are required to use strong passwords—ones that include, for example, a minimum number of characters and mixes of upper and lower case letters, numbers, and special characters. FMCSA did not detect our access or our placement of malware[6] on the network in part because it did not use automated detection tools and malicious code protections as DOT policy requires. [redacted] DOT policy requires OAs to implement boundary protection controls, deny network communications traffic by default, and allow network communications traffic by exception. Using another hacker technique, we discovered unsecured credentials to an FMCSA database and gained access to 13.6 million PII records that were not encrypted. DOT policy prohibits users from recording passwords in electronic form and requires them to use encryption to protect data. Had malicious hackers obtained this PII, it could have cost FMCSA up to $570 million in credit monitoring fees. We also found that FMCSA does not remediate system vulnerabilities according to DOT policy, which requires remediation of critical and high vulnerabilities within 30 days of detection. On the Agency's [redacted] devices, we identified [redacted] critical and [redacted] high vulnerabilities. FMCSA officials acknowledge these weaknesses and have informed us that the Agency is working to resolve many of them. The weaknesses—[redacted]

[redacted]

[6] Malware is software that performs an unauthorized process that will have adverse impact on the system's confidentiality, integrity, or availability.

[7] A mechanism for mapping addresses on one network to addresses on another network, typically private addresses to public addresses.

[8] Network boundary controls monitor and control communications between external and internal networks and connect only through managed interfaces made up of boundary protection devices arranged in accordance with an organizational security and privacy architecture.

[redacted] pose serious threats to the security to FMCSA's network and data.

We made recommendations to help FMCSA make its data and systems more secure. FMCSA has concurred with all 13 of our recommendations.

Background

FMCSA's employees and contractors operate and maintain the servers and databases for FMCSA's information systems. DOT's Cybersecurity Compendium and other departmental policy state standards, processes, and procedures for information system security. FMCSA's security policies and processes must adhere to these departmental policies as well as guidelines from the National Institute on Standards and Technology (NIST).[9] The Compendium requires departmental system users 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 any personal or departmental information solicited by e-mail, forward to the appropriate DOT security help desk any e-mail requesting such information or account or security settings verifications, and then delete the email.

DOT's Compendium also requires the use of strong passwords, encryption to prevent unauthorized disclosure of information during transmission, and

[9] NIST is a non-regulatory Federal agency within the U.S. Department of Commerce whose mission is to promote innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

automated incident detection and response tools. DOT information systems shall enforce least privilege[10] for all information system accounts.

DOT policy also requires technical, physical and administrative safeguards to protect the PII collected or maintained by the Department. This policy also calls for DOT to protect the records against reasonably anticipated threats and hazards that could result in harm, embarrassment, inconvenience, or unfairness to the individuals whose identities are revealed in the PII. At a minimum, all PII must be protected with controls that provide moderate confidentiality.[11]

FMCSA's IT Infrastructure and Information Is at an Increased Risk of Compromise

Using [redacted], we gained access to FMCSA's network. Weaknesses [redacted] helped us gain this access. FMCSA's lack of adherence to DOT policy exposes the PII it contains to compromise. Furthermore, FMCSA does not remediate vulnerabilities in a timely manner.

Using [redacted] We Gained Access to FMCSA's Network

Because FMCSA was not following DOT policy on password establishment, we gained unauthorized access to the Agency's network and systems. DOT policy requires OAs to use strong passwords—ones that include, for example, a minimum number of characters and mixes of upper and lower case letters, numbers, and special characters. The policy also prohibits the use of [redacted]. However, [redacted]

[10] A security principle that restricts the access privileges—such as program execution privileges and file modification privileges—of authorized personnel to the minimum necessary for the personnel to perform their jobs.

[11] Moderate confidentiality complies with Federal Information Processing Standard (FIPS) 199, The Standard defines it as a vulnerability whose successful exploitation is likely to have a serious adverse effect on the organization or individuals associated with the organization.

[redacted] and we used them to gain administrative access[12] to [redacted] web servers[13] hosted on FMCSA's cloud environment.

FMCSA officials acknowledged that the passwords we identified and used to gain access to Agency systems were not set up according to DOT's policy requirements. FMCSA officials also stated that they will review the usernames and passwords of all servers in the Agency's environment and ensure that they adhere to DOT policy standards.

FMCSA's lack of strong passwords increases the risk of compromise. Attackers can access sensitive and critical information by exploiting weak passwords [redacted].

FMCSA's Protections Against Malicious Software Code Are Not Adequate and Lacks Effective Detection Controls

Using the previously discovered [redacted], we gained administrative access to [redacted] web servers hosted on FMCSA's cloud environment. We created and uploaded malicious software (malware) [redacted] to one of these servers that allowed us to gain [redacted] access to the host machine through a web browser. Additional malware that we created and uploaded to [redacted] other servers forced the host machines to connect back to our testing machine and gave us a backdoor[16] connection to each affected host machine. Through this backdoor, we gained [redacted] to [redacted] host machine and [redacted] to [redacted]. This access allowed us to establish a foothold in FMCSA's internal network that we used for further penetration and exploitation. A month after we gained access to the network, FMCSA detected some but not all of our access.

[12] Access that allows system administrators to view system information and perform maintenance tasks such as upgrades.

[13] A computer, including hardware, an operating system, web server software, and web site content, that provides services on the internet or intranet.

[redacted]

[15] A privileged user that is authorized, and therefore, trusted, to perform security-relevant functions that ordinary users are not authorized to perform.

[16] Malware that negates normal authentication procedures to access a system. Remote access is granted to resources within an application, such as databases and file servers, giving perpetrators the ability to remotely issue system commands and update malware.

FMCSA has not established adequate protections against malicious code and does not have effective detection controls in place to alert its administrators when malicious code is detected. DOT policy requires OAs to configure malicious code protection mechanisms that perform periodic scans of information systems and real-time scans of files from external sources as they are downloaded, opened, or executed. These protection mechanisms block and quarantine malicious code and alert administrators that such code has been detected. The policy and guidelines recommend that OAs use automated incident detection and response tools for these protections.

FMCSA officials acknowledged that the malicious code protection and detection controls were not configured per DOT's policy requirements. FMCSA officials agreed to

- develop and implement strong malicious code protections and detection controls,
- review the real time security monitoring tools and alerts that the Agency is using in its environments, and
- restrict access to administrator login pages to verified administrators and computers.

FMCSA's weaknesses in malicious code protections can allow attackers to gain access to the network and potentially compromise sensitive systems and data. We intentionally did not cover our tracks to determine whether FMCSA could detect our access. If we had covered our tracks, the Agency most likely would not have detected our unauthorized access.

Weaknesses in FMCSA's Network [redacted] Helped Us Gain Unauthorized Access

Weaknesses in FMCSA's network [redacted] [redacted] contributed to our unauthorized access to FMCSA's network. Using a device such as a router or firewall, an organization can create boundaries to separate local area networks into segments called network boundaries. The organization can use these boundaries to restrict traffic to individual boundary segments and unauthorized access by shutting down segments during intrusions. DOT policy requires OAs to implement boundary protection controls, deny network communication traffic by default, and allow network communication traffic by exception. Exceptions to this traffic flow policy should be reviewed and removed if not supported by a mission or business need.

FMCSA has established boundary protection controls, but has also [redacted]

[redacted] thus making the Agency's [redacted] ineffective. As a result, FMCSA has exposed its cloud environment to [redacted] [redacted] and created a risk of unauthorized access. FMCSA officials have acknowledged that Agency's use of the [redacted] [redacted] exposes the network to risk. The officials stated further that rather than disabling [redacted], the Agency will coordinate with the Department to implement least privilege controls for [redacted]. These controls will give only authorized DOT users access to FMCSA resources.

FMCSA was not able to prevent our unauthorized access from the [redacted] or the FMCSA cloud environment. [redacted].

FMCSA's Inconsistent Adherence to DOT Policy Increases Risk of PII to Compromise

Because FMCSA does not adhere to DOT's cybersecurity policy, the PII on the Agency's systems is also at risk for compromise. Using our [redacted] connection that we previously established, we discovered [redacted] containing [redacted], for access to FMCSA's [redacted] database. Using these [redacted], we gained access to [redacted] preproduction databases containing over 13.6 million unencrypted records with PII, including contact information and medical examination information for commercial motor vehicle drivers, and license and contact information for certified medical examiners. We found that the databases contained production data rather than test or dummy data. FMCSA did not detect our unauthorized access to these databases.

DOT policy prohibits users from recording passwords in electronic form. The policy also requires technical, physical, and administrative safeguards to protect PII. DOT policy requires OAs to monitor information systems to detect unauthorized local, network, and remote connections and use automated tools to support near real-time analysis of events. NIST recommends agencies use test or dummy data in preproduction environments to minimize security risks.

[redacted] [redacted].

FMCSA officials acknowledged that the Agency was not properly adhering to DOT policy on security safeguards for PII protection and that controls and alerts for monitoring were not configured to distinguish database administrator account logins from unauthorized internet protocol addresses. The officials agreed to [redacted] and anonymize the production data used in preproduction environments.

FMCSA's lack of adherence to DOT policy on password and PII protection, information system monitoring, and use of live data in preproduction environments creates a risk for unauthorized access to FMCSA sensitive information. If our attacks had been malicious, the damage could potentially result in credit monitoring for affected individuals, costing the Agency an average of $41.73 per person[18] and up to $570,367,559. Citizens' identities whose PII is at risk could suffer substantial harm, inconvenience, and financial disruption, up to and including identity theft. Furthermore, the disclosure of this information, could cause serious public embarrassment to the Agency.

FMCSA Does Not Remediate Vulnerabilities in a Timely Manner

FMCSA does not remediate vulnerabilities, including critical[19] ones, as quickly as DOT policy requires. The policy requires remediation or mitigation of critical and high vulnerabilities[20] within 30 days of detection and medium vulnerabilities[21] within 60 days. On the [redacted] devices that FMCSA manages in its cloud environment, we identified [redacted] critical vulnerabilities, such as [redacted], which could allow a malicious actor to execute commands on a server or application to gain unauthorized access to the network or system. In addition, we identified [redacted] high vulnerabilities, such as [redacted], which could allow a hacker to access a system's resources and sensitive data, but unlike a critical vulnerability the malicious actor will not be capable of executing system commands. Finally, we identified [redacted] medium vulnerabilities, such as errors and deficiencies in application configurations. Ninety-six percent of the critical

[18] This is the average of the 2019 annual costs per person for credit monitoring from three vendors—ID Experts, Identity Force, and Ladlas. For more information, go to Identity Protection Services on the General Services Administration's Blanket Purchase Agreement.

[19] Critical vulnerabilities require immediate attention because they are relatively easy to exploit and may provide full control of affected systems.

[20] High vulnerabilities are more difficult to exploit but exploitation can result in significant data loss or downtime.

[21] Medium vulnerabilities generally require user privileges and may result in access to sensitive data but the impact is relatively limited.

vulnerabilities, 36 percent of high, and 73 percent of medium were over 1 year old.

FMCSA officials indicated that the Agency has developed a plan to remediate the critical and high vulnerabilities in its production environment. These officials also indicated that the Agency will develop a plan to remediate the medium vulnerabilities in its production environment and the critical, high and medium vulnerabilities in its Continuous Integration and Beta environments. However, the officials did not mention plans for the vulnerabilities in its three other environments—Operations & Maintenance, Security, and Development that we also compromised during our testing.

FMCSA has not remediated its vulnerabilities in the timeframes that DOT policy requires. FMCSA's lack of adherence to DOT policy on security vulnerability mitigation puts servers and workstations, information systems, and sensitive information at risk for compromise.

Conclusion

To complete its mission, FMCSA’s network processes, stores, and transmits a substantial amount of sensitive information that is connected to DOT’s network. In our testing, we demonstrated that the network has serious vulnerabilities that increase the likelihood that hacking attempts will succeed. As a result, these vulnerabilities make FMCSA’s information technology infrastructure and the sensitive information stored on it more vulnerable to unauthorized access and security compromises. Many of the weaknesses we found at FMCSA also tie into the same persistent enterprise-level security risks we found during our audits of the Maritime Administration’s and the Volpe National Transportation Systems Center’s IT networks and systems. Until the Department implements appropriate safeguards and countermeasures to protect its networks, the Department and its OAs will continue to be at risk for a potential enterprise-wide cybersecurity attack that could have a major impact on its mission.

Recommendations

To improve the security of FMCSA’s IT infrastructure, we recommend the Federal Motor Carrier Safety Administrator:

1. Change the passwords for the compromised web servers to strong passwords that meet DOT's Cybersecurity Compendium requirements.

2. Restrict access to administrator login pages to only verified administrators and computers.

3. Identify and remove all malware that was uploaded to FMCSA's web servers

4. Develop and implement stronger malicious code protection and detection controls.

5. Disable FMCSA [redacted] or implement least privilege controls for access to FMCSA resources by DOT personnel who have a need to know.

6. Remove [redacted] from noted [redacted] files.

7. Change the passwords for FMCSA's compromised databases.

8. Remove or anonymize all production data from the preproduction versions of the [redacted] database.

9. Validate whether production data is being used on other preproduction databases that FMCSA hosts.

10. Establish and implement security safeguards for the protection of PII in accordance with DOT policy. Implementing this recommendation could put up to $570,367,559 of funds to better use by avoiding the cost of credit monitoring for affected individuals.

11. Implement monitoring controls and alerts to identify when database admin accounts log in from non-authorized IP addresses.

12. Implement real time security monitoring tools and alert features to monitor FMCSA web servers and databases for access from unauthorized IP addresses.

13. Develop and implement a plan to remediate all identified critical, high, and medium vulnerabilities on FMCSA devices older than October 8, 2019.

Agency Comments and OIG Response

We provided FMCSA with our draft report on August 10, 2021, and received its formal response on September 23, 2021. FMCSA's response is included in its entirety as an appendix to this report. FMCSA concurred with all 13 recommendations and provided appropriate actions and completion dates for recommendations 2, 3, 4, 5, 11, 12, and 13.

FMCSA reported it has implemented recommendations 1, 6, 7, 8, 9, and 10 on September 16, 2021, provided supporting documentation for our review and requested that OIG close the recommendation within 30 days after issuing the final report.

Actions Required

We consider recommendations 1, 6, 7, 8, 9, and 10 resolved but open pending our evaluation of FMCSA documentation provided to close the recommendations, and will provide our response to FMCSA within 30 days after issuing our final report. We consider the other 7 recommendations resolved but open pending completion of the planned actions.

Exhibit A. Scope and Methodology

We performed our network security assessment between October 2020 and August 2021. 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 FMCSA'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 FMCSA's workstations, servers, infrastructure devices, and websites. Per the Rules of Engagement (ROE), we limited our tests to the agreed upon target devices and websites. FMCSA provided us with a list of [redacted] devices. However, when conducting scans of the subnets listed on ROE, we found [redacted] devices.

We used NIST Special Publication 800-115, *Technical Guide to Information Security Testing and Assessment*, to perform a penetration test and vulnerability assessment of FMCSA's 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 FMCSA's network and behind FMCSA's firewall with full knowledge of FMCSA's IT infrastructure as agreed to in the ROE. We used OIG-owned and licensed hardware and software, including Tenable Nessus and Netsparker for vulnerability scanning. We also used open source software including Kali Linux. During our tests, we notified FMCSA information security staff of issues we discovered and believed were indicative of serious problems that would require immediate attention.

We performed external vulnerability assessments of FMCSA's websites using OIG hardware and software and information available to the general public.

Upon completion of our tests, we provided FMCSA's IT audit liaison with the reports generated by our automated assessment tools so that the Agency could take 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 FMCSA management on our activities and the access we had gained, including our analysis of the issues reported by the tools we used.

Exhibit B. Organizations Visited or Contacted

Federal Motor Carrier Safety Administration

Office of Chief Technology Officer

Office of Policy and Program Development

Office of Policy, Strategic Planning and Regulations

Office of Cybersecurity and Privacy

Department of Transportation Office of the Secretary

Office of the Chief Information Officer

Office of Audit Relations and Program Improvement

Information Technology Shared Services

Budget and Financial Management

General Counsel

Office of the Undersecretary for Policy

Exhibit C. List of Acronyms

CIO	Chief Information Officer
COE	common operating environment
DOT	Department of Transportation
IT	information technology
NIST	National Institute of Standards and Technology
OA	Operating Administration
OIG	Office of Inspector General
PII	personally identifiable information
ROE	Rules of Engagement

Exhibit D. Glossary of Terms

administrative access. Access that allows system administrators to view system information and perform maintenance tasks such as upgrades.

automated detection tool. A software application implemented on a host operating system or network device to monitor activity associated with intrusions and insider misuse.

beta environment. An environment used to test software in an actual production environment versus a lab or stage setting. This ensures the software can perform under real workloads and that speed, storage, and scalability all work as expected.

backdoor. Malware that negates normal authentication procedures to access a system. Remote access is granted to resources within an application, such as databases and file servers, giving perpetrators the ability to remotely issue system commands and update malware.

continuous integration environment. An environment where developers integrate new code they've written more frequently throughout the development cycle, adding it to the code base at least once a day. Automated testing is done against each iteration of the build to identify integration issues earlier, when they are easier to fix , which also helps avoid problems at the final merge for the release.

cloud computing. The on-demand availability of computer systems resources without the user's direct active management.

common operating environment. An opt-in environment that for a fee delivers common IT services to an organization's components.

configuration file. A file used to establish parameters and initial settings for some computer programs.

critical vulnerability. A vulnerability that requires immediate attention because it is relatively easy to exploit and may provide full control of affected systems.

[redacted]

exploit. Code that takes advantage of a software vulnerability or security flaw.

high vulnerability. A vulnerability that is difficult to exploit but whose exploitation can result in catastrophic adverse effects to the organization including significant data loss or downtime.

host machine. A hardware device with the capability of permitting access to a network through a user interface, specialized software, network address, protocol stack, or other means.

insider threat. A threat by an entity with authorized access that could harm an information system or enterprise through destruction, disclosure, modification of data, or denial of service.

[redacted]

least privilege. A security principle that restricts the access privileges—such as program execution privileges and file modification privileges—of authorized personnel to the minimum necessary for the personnel to perform their jobs.

malicious code protection. A protection used to detect and eradicate malicious code, such as viruses, worms, Trojan horses, spyware, that can be transported by email and email attachments, internet accesses, removable media, such as USB devices, diskettes and compact disks, and other common means, or by exploitation of information system vulnerabilities.

malware. Software that performs an unauthorized process that will have adverse impact on the system's confidentiality, integrity, or availability; a virus, worm, Trojan horse, or other code-based entity that infects a host; spyware and some forms of adware.

manual testing. Examination techniques conducted manually to evaluate systems, applications, networks, policies, and procedures to discover vulnerabilities.

medium vulnerability. A vulnerability whose successful exploitation is likely to have a serious adverse effect on the organization or individuals associated with the organization.

[redacted]

penetration testing. A method of testing where testers target individual binary components or the application as a whole to determine whether intra or inter-component vulnerabilities can be exploited to compromise the application, its data, or its environment resources.

preproduction environment. An environment where applications are built before going into production.

production data. A subset of information in an electronic format that allows it to be retrieved or transmitted within the production environment.

production environment. An environment where functionality and availability must be ensured for the completion of day-to-day activities.

root user. A privileged user that is authorized, and therefore, trusted, to perform security-relevant functions that ordinary users are not authorized to perform.

security controls are the safeguards or countermeasures prescribed for information systems or organizations designed to protect the confidentiality, integrity, and availability of information that is processed, stored or transmitted by the systems or organizations, and to manage information security risk.

test (or dummy) data. Artificial datasets used in a test environment.

virtual private network. A virtual network built on top of existing networks that provides secure communication for data and internet protocol information transmitted between networks.

vulnerability assessment. A systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, identify data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

web-based application. Software that allows users to interact with a remote server through a web browser interface.

web server. A computer, including hardware, an operating system, web server software, and web site content, that provides services on the internet or intranet.

[redacted]

Exhibit E. Major Contributors to This Report

LEON LUCAS	PROGRAM DIRECTOR
DANIEL JOPLIN	PROJECT MANAGER
ZACHARY LEWKOWICZ	IT SPECIALIST
RIFAT MAJUMDAR	IT SPECIALIST
STEPHANIE HIGHTOWER	IT SPECIALIST
SUSAN NEILL	WRITER-EDITOR
SEETHA SRINIVASAN	ASSOCIATE COUNSEL

Appendix. Agency Comments

U.S. Department
Of Transportation

Federal Motor
Carrier Safety
Administration

Memorandum

Subject: **INFORMATION:** Management Response – Office of Inspector General (OIG) Draft Report on FMCSA IT Infrastructure Project No. 19F3015F000

Date: 9 23 2021

From: Meera Joshi
Deputy Administrator

To: Kevin Dorsey
Assistant Inspector General for Information Technology Audits

The Information Technology (IT) applications and systems of the Federal Motor Carrier Safety Administration (FMCSA) play a critical role in supporting the Agency's mission to reduce crashes, injuries, and fatalities involving large trucks and buses. FMCSA is committed to ensuring the security of its systems, maintaining the accuracy of data that the Agency is mandated to collect, and protecting collected information from unauthorized access. FMCSA notes that there have been no major incidents attributed to FMCSA systems. As part of FMCSA's IT Modernization Plan, the Agency has developed a comprehensive approach to IT infrastructure that will significantly improve its cybersecurity posture. This approach includes the appointment of an FMCSA senior executive Chief Technology Officer (CTO) within the last 12 months to lead the effort. The Agency has taken steps to centralize all IT-related projects under the Office of the CTO, which has provided the necessary visibility and systematic structure to address cybersecurity through the life cycle of each application and system.

FMCSA has also taken the following actions to improve the cybersecurity of its applications and systems:

- Removed all PII from pre-Production environment by either removing data from pre-Production environment or by scrambling (anonymizing) data using a randomizing algorithm. Such measures mitigate risk of unauthorized access to PII by malicious entities, both internal and external.

- Migrated the responsibility for its IT infrastructure to the Departmental Office of the Chief Information Officer (OCIO) shared services organization within the Office of the Secretary of Transportation to ensure that new- and previously-identified infrastructure vulnerabilities at the are tracked and remediated within DOT timelines.
- Performed a comprehensive review of the login credentials associated with servers and applications residing within the FMCSA boundary to identify gaps and implement actions that meet DOT requirements, including but not limited to changing passwords on servers and databases to comply with DOT's Cybersecurity Compendium requirements.
- Developed a plan and started remediating identified critical, high, and medium vulnerabilities.
- Implemented a process to certify that all assets within the FMCSA inventory are reported to the DOT OCIO to ensure continuous monitoring for malicious activity.

Based on FMCSA's review of the draft report, we concur with OIG's thirteen recommendationsas written. **We implemented recommendations 1, 6, 7, 8, 9 and 10[1]; on September 16, 2021,we provided supporting documentation to OIG and requested closure of the recommendations within 30 days after OIG issues the final report.** In addition to several steps we have already taken based on the OIG recommendations, we plan to address the recommendations as follows:

Target Closure Date	Recommendation #
November 1, 2021	3, 12
January 31, 2022	2, 5
March 30, 2022	4, 13
September 14, 2022	11

We recognize the importance of completing recommendations and addressing vulnerabilities in a timely fashion and will endeavor to meet or exceed these deadlines. We appreciate the opportunity to review the OIG draft report. Please contact Pavan Pidugu, FMCSA CTO, at Pavan.Pidugu@dot.gov or 202-366-4313, with any questions.

[1] FMCSA agrees that preventing breach of its IT systems will allow it to avoid the cost of credit monitoring.

FOR OFFICIAL USE ONLY
Public availability to be determined under the Freedom of Information Act, 5 U.S.C. § 552.

U.S. Department of Transportation
Office of Inspector General

Fraud & Safety
Hotline

https://www.oig.dot.gov/hotline
hotline@oig.dot.gov
(800) 424-9071

OUR MISSION

OIG enhances DOT's programs and operations by conducting objective investigations and audits on behalf of the American public.

OFFICE OF INSPECTOR GENERAL • U.S. DEPARTMENT OF TRANSPORTATION •

1200 New Jersey Ave SE
Washington, DC 20590
www.oig.dot.gov