~~SENSITIVE SECURITY INFORMATION~~

U.S. DEPARTMENT OF TRANSPORTATION

OFFICE OF INSPECTOR GENERAL

FAA Is Not Remediating STARS Security Weaknesses in a Timely Manner and Contingency Planning Is Insufficient

FAA

Report No. IT2020039

July 15, 2020

U.S. DEPARTMENT OF TRANSPORTATION
OFFICE OF INSPECTOR GENERAL

Highlights

FAA Is Not Remediating STARS Security Weaknesses in a Timely Manner and Contingency Planning Is Insufficient

Self-initiated

Federal Aviation Administration | IT2020039 | July 15, 2020

What We Looked At

The Federal Aviation Administration (FAA) operates up to 172 Terminal Radar Approach Control (TRACON) facilities, which provide air traffic control services to pilots in the airspace immediately surrounding major airports. Currently, air traffic controllers use the Standard Terminal Automation Replacement System (STARS) to provide critical air traffic services at the 11 largest TRACONs, which handle about 33 percent of all TRACON traffic in the United States. Effective security controls and contingency plans at these 11 facilities are critical to maintaining the safety and security of the National Airspace System. Accordingly, we initiated this audit to (1) assess FAA's identification and mitigation of security risks in STARS and (2) determine whether FAA's contingency planning limits the effects caused by the loss of STARS operations at large TRACON facilities during emergencies.

What We Found

FAA is identifying STARS' security risks but is not mitigating vulnerabilities in a timely manner. In March 2019, for example, FAA found vulnerabilities in 53 of 73 STARS security controls but did not meet its own schedule for remediating them. DOT policy requires timely remediation of network vulnerabilities to reduce the risk that an attacker could gain unauthorized access to mission-critical systems. In addition, the Agency's STARS incident response policy does not comply with Federal requirements, and we found security control weaknesses at the [redacted]. These weaknesses could make it harder for the Agency to ensure the confidentiality, integrity, and availability of STARS. Finally, FAA's contingency plans for three large TRACONS—[redacted]—are not sufficient to maintain continuity of air traffic operations during unplanned outages, as Agency policy requires.

Our Recommendations

We consider recommendations 1–9 and 11 resolved but open pending completion of FAA's planned actions. In accordance with DOT Order 8000.1C, we have asked the Agency to provide additional information on its planned actions for recommendation 10 within 30 days of the date of this report.

Contents

U.S. DEPARTMENT OF TRANSPORTATION
OFFICE OF INSPECTOR GENERAL

Memorandum

Date: July 15, 2020

Subject: ACTION: FAA Is Not Remediating STARS Security Weaknesses in a Timely Manner and Contingency Planning Is Insufficient | Report No. IT2020039

From: Kevin Dorsey
Assistant Inspector General for Information Technology Audits

To: Federal Aviation Administrator

The Federal Aviation Administration (FAA) operates up to 172 Terminal Radar Approach Control (TRACON) facilities, which provide air traffic control services to pilots in the airspace immediately surrounding major airports. Currently, air traffic controllers use the Standard Terminal Automation Replacement System (STARS) to provide these critical services, which include separation and sequencing of air traffic, conflict and terrain avoidance, and weather advisories for aircraft departing and arriving in the terminal airspace.

In February 2016,[1] we reported that FAA's legacy terminal automation system—Common Automated Radar Terminal System (CARTS)—had 407 significant vulnerabilities in key subsystems that could allow an attacker to establish connection with the network and possibly disrupt flight operations. At that time, FAA management stated that remediating these vulnerabilities would require substantial investment and could not be completed before CARTS was replaced by STARS. In April 2017, FAA replaced CARTS with STARS at the 11 largest TRACON facilities.

These 11 facilities handle about 33 percent of all TRACON traffic in the United States. As such, security vulnerabilities in any system serving these facilities could pose a risk to the entire National Airspace System (NAS). Effective security controls and contingency plans for systems at large TRACONs are critical to maintaining safety and security of the NAS; this is especially the case with STARS

[1] *FAA's Security Controls Are Insufficient for Large Terminal Radar Approach Control Facilities* (OIG Report No. FI2016019), February 4, 2016. OIG reports are available on our website: https://www.oig.dot.gov/.

due to the safety-critical information it manages. Accordingly, we initiated this audit to (1) assess FAA's identification and mitigation of security risks in STARS and (2) determine whether FAA's contingency planning limits the effects caused by the loss of STARS operations at large TRACON facilities during emergencies.

We conducted this audit in accordance with generally accepted Government auditing standards. To conduct our work, we interviewed officials at the Department of Transportation (DOT) and FAA Headquarters offices in Washington, DC, and FAA's William J. Hughes Technical Center (WJHTC) in Atlantic City, NJ. We visited the [redacted]. In addition, we issued data calls to FAA and reviewed the Agency's STARS-related documentation, including the security controls authorization package. We also reviewed contingency planning policy and procedures for STARS at WJHTC, and the [redacted] TRACONs.

We appreciate the courtesies and cooperation of Department of Transportation representatives during this audit. If you have any questions concerning this report, please call me at (202) 366-1518.

cc: The Secretary
DOT Audit Liaison, M-1
FAA Audit Liaison, AAE-100

Results in Brief

FAA is identifying STARS' security risks but is not mitigating vulnerabilities in a timely manner.

During a network vulnerability scan for STARS in March 2019, for example, FAA identified 1,270 vulnerabilities—109 with critical severity, 598 with high severity, and 563 with medium severity. Many of the critical and high vulnerabilities discovered during the scan testing were related to [redacted]. FAA also assessed 73 STARS security controls in March 2019 and found vulnerabilities in 53 of them; the Agency acknowledges that the scheduled completion dates for remediating those weaknesses has passed. Departmental policy states that DOT components (Operating Administrations) must remediate vulnerabilities with a critical severity within 7 days, high severity within 60 days, and medium severity within 90 days. If the vulnerabilities are not remediated within the thresholds defined above, FAA must prepare a Plan of Action and Milestones (POA&M) within 30 days to identify, prioritize, and track vulnerabilities and document the planned remediation actions. Continued operation without mitigating known system vulnerabilities increases the likelihood of an attacker gaining unauthorized access to STARS information. That in turn could have a debilitating impact on the Agency's mission because STARS is a mission-critical system that provides safety-critical services for the NAS. Furthermore, FAA's incident response policy for STARS lacks some of the policy elements required by the National Institute of Standards and Technology (NIST).[2] In December 2019, FAA officials informed OIG that an updated version of the policy would be available in about a year. However, policies and procedures that are neither formal nor consistent can increase the time needed to coordinate responses to incidents. Finally, we found security control weaknesses related to separation of duties at [redacted], where the system specialists told us they were unaware that DOT requires someone independent to review the system-generated reports about their work. We also noted that [redacted] does not comply with FAA's data storage or access control procedures, which could make it harder for the Agency to manage STARS and ensure the system's confidentiality, integrity, and availability.

[2] NIST, *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST Special Publication (SP) 800-53, revision 4 (April 2013).

FAA's contingency plans for three large TRACONs are not sufficient to maintain continuity of air traffic operations.

Agency policy requires TRACON facilities to establish operational plans that aim to continue services during unplanned outages and return the affected airspace to a 90-percent capacity within 96 hours. However, the plans used by the TRACONs at [redacted] lack DOT and FAA-required procedures for alternate processing site agreements and signature pages confirming that the plans were reviewed and approved. In addition, the [redacted] contingency plan does not discuss steps for returning the affected airspace to a 90-percent capacity within 96 hours. When we asked about the missing procedures, officials at the three TRACONs said—and we confirmed—that they were aware of what their actions should be if a STARS outage occurs. Still, the lack of formal contingency procedures means FAA cannot have assurance that TRACON officials will respond effectively to an unexpected outage or a disruption to air traffic operations.

We are making recommendations to help FAA mitigate the security risks to the integrity and availability of STARS.

Background

STARS is a joint FAA and Department of Defense (DoD) program that replaced Automated Radar Terminal Systems (ARTS) and other older, capacity-constrained technology systems at several TRACON facilities and associated towers—up to 172 at FAA and up to 199 at DoD.

STARS is a mission-critical NAS operational system used by controllers to provide air traffic control services to aircraft in terminal areas. Typical services include separating and sequencing air traffic, providing traffic alerts and weather advisories, and radar vectoring for departing and arriving traffic. In addition, the system accommodates air traffic growth and includes automation functions that improve the safety and efficiency of the NAS. It minimizes the chance of air traffic collisions by providing the automation that enables air traffic controllers to provide situational awareness advisories to pilots who work under visual flight rules.

STARS provides safety-critical services, and if it were not available and its functions could not be performed, that disruption would have a serious impact on FAA and its mission. It also would increase the risk of injuries and loss of life,

and keep the organization from performing its primary functions of aircraft separation and safety, which will result in flight delays and cancellations.

FAA Is Identifying STARS' Security Risks But Is Not Mitigating Vulnerabilities in a Timely Manner

STARS is currently at risk of compromise because FAA is not mitigating the system's critical, high, and medium security vulnerabilities in a timely manner, and the current incident response policy does not include some required elements. In addition, there are security control weaknesses at [redacted], where staff do not always adhere to departmental policies.

FAA Is Not Mitigating STARS' Critical, High, and Medium Vulnerabilities in a Timely Manner

DOT's *Cybersecurity Compendium* requires the Department's components to remediate vulnerabilities with critical severity within 7 days, high severity within 60 days, and medium severity within 90 days. If critical, high, and medium vulnerabilities are not remediated within the thresholds defined above, FAA must prepare a POA&M within 30 days to identify, prioritize, and track vulnerabilities and document the planned remediation actions. Based on our review, FAA is not effectively tracking or mitigating vulnerabilities in a timely manner. For example, FAA has yet to address a critical vulnerability to remediate STARS [redacted], as well as other security control weaknesses, as listed below.

Remediating STARS [redacted]

During a network vulnerability scan for STARS in March 2019, FAA identified 1,270 vulnerabilities—109 with critical severity, 598 with high severity, and 563 with medium severity. [redacted]

[redacted] FAA created a POA&M to mitigate these vulnerabilities in November 2014 but did not meet the scheduled completion date of September 2016. The new planned completion date is December 2021.

Remediating STARS Security Control Weaknesses

In March 2019, FAA's assessment team also evaluated 73 STARS security control requirements and found that 53 (75 percent) of them had vulnerabilities (including the [redacted] discussed above). DOT's *Cybersecurity Compendium* states that critical vulnerabilities have the highest priority and must be remediated first. Listed below are examples of the vulnerabilities to key security controls that FAA designated as having a very high, high, or moderate risk and requiring remediation. Also included are the Agency's planned completion dates for remediation, as stated in the relevant POA&Ms:

Protecting network boundaries

- [redacted] POA&M creation date: October 2015, scheduled completion date: September 2016, current planned completion date: November 2019.
- [redacted] POA&M creation date: October 2015, scheduled completion date: September 2016, current planned completion date: November 2019.

Implementing software updates and use of antivirus software

- Security-relevant software updates for critical, high, and medium vulnerabilities in STARS were not implemented in accordance with requirements. FAA had not created a POA&M at the time of our review.
- [redacted] OA&M creation date: April 2017, actual start date: May 2017, scheduled completion date: December 2017, current planned completion date December 2021.

Remediating configuration weaknesses

- [redacted] POA&M creation date: November 2014, scheduled completion date: September 2016, current planned completion date: December 2021.
- [redacted] POA&M creation date: November 2014, actual start date: March 2016, scheduled completion date: September 2016, current planned completion date: December 2021.

Limiting unsuccessful login attempts

- [redacted] POA&M creation date: November 2014, planned start date: October 2013, scheduled completion date: September 2015, current planned completion date: December 2021.

Updating Plans of Action and Milestones

- FAA is not updating STARS POA&Ms at least quarterly, as DOT's *Cybersecurity Compendium* requires. The STARS system owner needs to update POA&Ms for 27 security control weaknesses, including the ones listed above (see exhibit D). FAA reported that these are open POA&Ms that have passed their scheduled completion dates, but their status has not been updated. However, the lack of a documented process to monitor remediation progress and track overdue mitigation of vulnerabilities puts STARS at risk of disruption or compromise. FAA also needs to report its POA&Ms in the Department's Cybersecurity Assessment and Management monitoring system, which facilitates DOT's ability to identify common threats and vulnerabilities and provides comprehensive reporting on IT weaknesses.

Our 2016 audit found that FAA had identified hundreds of security vulnerabilities in CARTS, nine of which were "critical." However, FAA accepted the risk, concluding that remediation would require a substantial investment and could not be completed before the Agency was to replace CARTS with STARS in April 2017. As we noted in the 2016 report, that would allow "the vulnerabilities to remain exploitable for at least 2 years [posing] a threat to the entire system's

security." Although FAA replaced CARTS, its March 2018 and March 2019 vulnerability assessments show that STARS has numerous critical vulnerabilities (see table 1).

Table 1. Results From FAA's 2018 and 2019 Vulnerability Assessments on STARS

Vulnerability levels of severity	Scan date March 22, 2018	Scan date March 13–14, 2019
Critical*	97	109
High**	310	598
Medium***	506	563
Total number of vulnerabilities found	**913**	**1,270**
Total assets (IP addresses) scanned	119	147

Note: **Critical:* system is exposed to a threat with some exceptions; prioritize fixing these risks first. ***High:* in most cases, system is exposed to a potential threat ; fix these risks immediately. ****Medium:* can mean system is exposed to a potential threat; fix critical and high risks first.

Source: STARS Security Assessment Report, May 2019

We asked FAA officials why they had not yet remediated the critical vulnerabilities; a supervisory aviation technical systems specialist responded that the Agency has been "deficient in remediating risks/vulnerabilities in a timely manner in some areas." This official added that remediation is in process, but the documentation of the Agency's remediation efforts is not yet complete. For example, the risk pertaining to the continued use of outdated software has been partially remediated, and remediation will be complete in [redacted]. However, the official did not provide evidence to support these statements or explain why this critical security weakness will not be remediated until [redacted]—FAA's current completion date. IT security control weaknesses that remain unaddressed for extended periods can create unnecessary system exposures that may be exploited by an attacker; disrupt flight operations; or compromise the confidentiality, integrity, and availability of systems and data.

FAA's Incident Response Policy for STARS Is Incomplete

The Agency's incident response policy for STARS—which is included in the broader *FAA Information Security and Privacy Program and Policy*[3]—describes the actions management and staff should take following a security breach or similar event. However, the policy is missing some elements that are required by NIST.

According to NIST Special Publication (SP) 800-53, revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, an incident response policy should address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. NIST also requires Federal agencies to establish procedures for implementing the policy and associated internal controls.

FAA Information Security and Privacy Program and Policy has specific policy elements regarding the purpose and the scope of the Agency's response to potential STARS-related incidents. However, it does not have similar policy elements for roles, responsibilities, management commitment, coordination among organizational entities, or compliance (see table 2). According to a cybersecurity official from FAA's Air Traffic Organization (ATO), coordination among organizational entities was included in a previous policy that has now expired.[4] In December 2019, the ATO official told us that the Agency is working on a permanent incident response policy that will be final within a year.

Without the NIST-required elements in its incident reporting policy, FAA's senior leaders may not understand the impact of information security incidents arising from the operation and use of information systems. Furthermore, organizational entities may not be aware of their responsibilities in responding to cybersecurity incidents.

[3] FAA Order 1370.121, *FAA Information Security and Privacy Program and Policy*, appendix 9 (December 23, 2016).
[4] FAA Order JO 1370.50, *NAS Information Security Detection, Reporting and Response Policy* (March 6, 2018–March 6, 2019).

Table 2. Inclusion of NIST-Required Elements in FAA's STARS-Related Policies

NIST-Required Elements	FAA Incident Response Policy	STARS System Administration Security Handbook
Purpose	Yes	No
Scope	Yes	No
Roles	No	No
Responsibilities	No	No
Management Commitment	No	No
Coordination Among Organizational Entities	No	No
Compliance	No	No
Procedures	No	Yes

Sources: NIST SP 800-53, rev. 4; FAA Order 1370.121, appendix 9; STARS Order JO 6191.2.

FAA's [redacted] Facility Has Security Control Weaknesses

During our visit to [redacted], we found three types of security control weaknesses related to separation of duties, backup tape storage, and access account management.

- **Separation of duties.** NIST defines separation of duties as a security principle that divides critical functions among different staff members in an attempt to ensure that no one individual has enough information or access privilege to perpetrate damaging fraud. According to the *Departmental Cybersecurity Compendium*,[5] DOT Operating Administrations should define system access authorizations in a way that

[5] DOT, Office of the Chief Information Officer, *Departmental Cybersecurity Compendium, Supplement to DOT Order 1351.37, Departmental Cybersecurity Policy*, version 4.2, DOT-AC-5 (March 2018).

supports separation of duties and independent reviews. FAA's *STARS System Security Plan* has the same requirements, which apply to all TRACONs with STARS.

At [redacted], however, the same system specialists who operate STARS also review those operations. This may be because system administration support for STARS at [redacted] is limited to a small, three-person office. However, the [redacted] system specialists acknowledged that they were unaware that someone independent—that is, other than the individual who performed the work—should review the system-generated reports about that work.

- **Storage of backup tapes.** During our walkthrough of the [redacted] equipment room, we noticed backup tapes on top of the system specialists' desks. The tapes were neither placed in a designated safe and secure location, out of the view of unauthorized personnel, nor marked as sensitive security information (SSI), as the Agency requires in FAA Order JO 6191.2.[6] When we asked the system specialists why they did not follow the Agency's policies for SSI, they told us the Order did not require them to do so. A management official concurred with the comment from the system specialists. However, the FAA Order clearly states that the proper management of sensitive STARS data is of paramount importance to overall system protection, and SSI is a specific category of sensitive information.

- **Access control management.** [redacted] system specialists do not consistently use the designated forms for requesting changes in access to STARS, as required by FAA Order JO 6191.2.[7] We reviewed the access authorization forms for 61 unique user IDs; the forms for 3 users were missing, and 1 lacked a manager's signature. When we asked the system specialists at [redacted] about this situation, they seemed to be unaware that the forms were either missing or unsigned.

The lack of adherence to policies and procedures for separation of duties, secure storage of data, and access control can make it harder for FAA to manage STARS.

---

[6] FAA Order JO 6191.2, CHG1, *Standard Terminal Automation Replacement System (STARS) System Administration Security Handbook* (June 13, 2013). This report refers to this policy as FAA Order JO 6191.2.

[7] FAA Order JO 6191.2, chapter 2, Security Policies: Requests for all accounts with system access must be submitted to the System Support Center Manager on Form 6191-2, User Account Access Request Form. The request must include the access privileges required and the justification for why [access] is needed.

Furthermore, there is an increased risk that the confidentiality, integrity, and availability of STARS data could be intentionally or unintentionally compromised.

FAA's Contingency Plans for Three Large TRACON Facilities Are Insufficient

The Agency's contingency plans at three large TRACONs are not sufficient to maintain continuity of air traffic operations after a loss or disruption. FAA's policy, *Air Traffic Control Operational Contingency Plans*,[8] requires TRACON facilities to establish operational plans that provide for continuity of services during unplanned outages and aim to return the affected airspace to a 90-percent capacity within 96 hours. However, the contingency plans[9] we reviewed for three TRACONs—[redacted]—are missing the following DOT- and FAA-required documents:

- Formal and complete alternate processing site agreement, which permits the transfer of STARS operations to another site; and
- Signature page to confirm that an authorized official has reviewed and approved the plan.

In addition, the [redacted] contingency plan does not include language for returning the affected airspace to a 90-percent capacity within 96 hours.

We asked FAA officials why the [redacted] contingency plans did not include the required documents and language. A representative from the office of the ATO Chief of Staff explained that the TRACON officials were aware of what their actions should be if a STARS outage occurs. During our review, we did confirm[10] that officials at [redacted] know what to do in the event of an emergency, although their contingency plan is missing some required documents and language. Still, the lack of formal contingency procedures puts the TRACONs at

[8] FAA Order JO 1900.47E April 20, 2016.

[9] FAA Order JO 1900.47E, *STARS NAS Information Contingency Plan*, ATO Order JO 6030.31G.

[10] [redacted] systems specialists told us that they conduct annual contingency plan testing, such as table-top exercises that incorporate discussions about roles and responsibilities during emergencies. They also showed us checklists and after-action reports documenting these activities.

risk; specifically, FAA cannot have assurance that TRACON officials will respond effectively to an unexpected outage or a disruption to air traffic operations.

Without formal and complete alternate processing site agreements, TRACON officials may perform STARS operational activities in an ad hoc manner. Similarly, the lack of a signature and date stamp could indicate the document has not been reviewed, approved, or finalized. As a result, TRACONs may not be able to minimize the effects of potential disasters or recover STARS timely after an outage or loss.

Conclusion

STARS is a mission-critical system that provides safety-critical services to FAA. The Agency's primary mission is to ensure the safety and efficiency of the NAS. Longstanding weaknesses in STARS' security controls—such as untimely remediation of security vulnerabilities and insufficient contingency plans—pose significant risks to the operations of the NAS. FAA must take immediate steps to prevent STARS from being compromised and enhance its ability to respond to an unexpected disruption of services at TRACON facilities. Thus, it is critical that FAA remediate vulnerabilities in STARS or develop a risk-acceptance strategy with detailed plans for mitigating those vulnerabilities until remediated. At the same time, FAA must update its STARS-related security policies and procedures and effectively communicate its requirements to Agency personnel. Until then, these unmitigated vulnerabilities will continue to increase the risk of a NAS cybersecurity compromise that could result in lengthy and costly disruptions and impact the safety of both the Nation and its public.

Recommendations

To mitigate the risks that might impact the integrity and availability of the Standard Terminal Automation Replacement System (STARS), we recommend that the Federal Aviation Administrator:

1. Develop and implement a plan with a timeline that identifies when critical, high, and medium vulnerabilities in STARS will be mitigated and implemented at the 11 largest TRACON facilities and includes a:

a. Patch management program to ensure that the security patches for all operating systems, software, and applications are up to date; and

b. Timeline when FAA will implement security-relevant software updates for critical, high, and medium vulnerabilities, in accordance with requirements.

2. Develop and implement a plan with a timeline that identifies a date when FAA will implement [redacted] protection [redacted] in the system and other assets at the 11 largest TRACON facilities.

3. Develop and implement a plan that defines how FAA will remediate weaknesses [redacted], and provide a timeline for the completion of corrective actions.

4. Implement the current plan with a timeline that defines when [redacted] as defined in the System Security Plan.

5. Develop and implement a plan and timeline identifying when [redacted].

6. Direct STARS officials to prioritize mitigation efforts to resolve the security weaknesses for the 27 security controls identified in this report; develop a Plan of Action and Milestones that realistically reflects resources and timeframes for the completion of these actions; and report on these actions in the Department's Cybersecurity Assessment and Management monitoring system.

7. Update the STARS incident response policy to include the missing elements from the National Institute of Standards and Technology.

8. Provide training on FAA's policies and procedures regarding separation of duties and the proper management of sensitive data and markings to system specialists and other appropriate security officials at [redacted] on a periodic basis.

9. Develop and implement an internal control that ensures that Agency staff follow requirements for access control in accordance with the *STARS Security Handbook*.

10. Update the contingency plans for the [redacted] TRACONs to include a formal and complete alternate processing site agreement and a signature page to confirm the plans have been reviewed and approved by an authorized official.

11. Update the [redacted] contingency plan to describe the process for returning the affected airspace to a 90-percent capacity within 96 hours of an incident.

Agency Comments and OIG Response

We provided FAA with our draft report on May 21, 2020, and received its formal response on June 19, 2020, which is included as an appendix to this report. FAA concurred with 5 of our 11 recommendations, partially concurred with the remaining 6, and proposed appropriate actions and completion dates for all except recommendation 10.

We consider recommendations 3, 7, 8, 9, and 11 resolved but open pending completion of planned actions.

While FAA partially concurred with recommendations 1, 2, 4, 5, and 6, its planned actions to implement them by delivering POA&Ms by March 31, 2021, meet the intent of our recommendations. FAA stated that the vulnerability remediation timeframe requirements in the DOT Compendium—which we cite in this report—do not align with the requirements for STARS and the NAS. However, FAA's planned actions are consistent with the Compendium, which explains that if DOT components do not remediate vulnerabilities within established thresholds or timeframes, they must prepare POA&Ms to identify, prioritize, and track vulnerabilities and document planned remediation actions. FAA also stated that it will make NAS operational system changes via System Support Modifications, which can take up to a year to implement safely. Additionally, FAA plans to implement OIG's recommendations in accordance with the International Civil Aviation Organization Safety Management Manual, NIST SP 800-82[11] and NAS

[11] NIST Special Publication 800-82: Guide to Industrial Control Systems Security.

Configuration Management policies rather than the DOT Compendium. However we are not sure why FAA referred to NAS operational changes or cited other policies because we did not raise these issues. As we reported, our concern is that FAA is not effectively tracking and mitigating POA&Ms to remediate STARS vulnerabilities in a timely manner. For example, FAA has not remediated some vulnerabilities in 7 years, although FAA stated remediation could take up to a year.

FAA partially concurred with recommendation 10, stating that it is not required to establish the alternate processing site agreements that we cited. We are requesting that FAA provide us with the basis for this response. As we reported, the DOT Compendium requires organizations to develop alternate processing site agreements for systems categorized at moderate impact level, which is where STARS was at the time of our review. Moreover, in 2016, OIG recommended that FAA conduct annual contingency plan exercises for large TRACONs using an alternate processing site. The goal was to familiarize TRACON personnel with the alternate facility's resources and equipment and evaluate the site's ability to support contingency operations using explicit test objectives and success criteria. While FAA concurred with this recommendation, and provided a planned completion date of December 31, 2016, it has yet to be resolved. FAA also proposed updating the contingency plans for the three TRACONs identified in this report by adding formal procedures for transferring published air traffic services to other sites. FAA stated that it will complete documentation and confirm that the plans have been reviewed and approved by an authorized official by June 30, 2022. While we believe FAA's alternative actions may address the intent of our recommendation, we are concerned about the Agency's planned completion date, as it has yet to remediate our prior recommendation from 2016.

In its response, FAA disagreed with some of our report conclusions. For example, the Agency stated that the number of security scan vulnerabilities we discuss represent raw data findings that have not been assessed against any actual threat or system exposure level. FAA said that these raw numbers mischaracterize STARS security posture, because the report does not provide any context to relate them to actual security risks. We disagree; as we reported, many of the critical and high vulnerabilities discovered during the scan testing were related to [redacted] The scan results provide clear context for the actual security risks to STARS. Furthermore, according to FAA, our report is misleading because it refers to vulnerability scan raw findings rather than POA&M items. We disagree; as we reported on the status of FAA's POA&M to

remediate vulnerabilities associated with STARS [redacted]; which currently has a schedule completion date of [redacted] after its creation date.

Finally, FAA disputes OIG's statement that [redacted] According to FAA officials, they provided an updated POA&M [redacted]. However, FAA did not send the updated POA&M to us.

Actions Required

We consider recommendations 1–9 and 11 resolved but open pending completion of FAA planned actions. In accordance with DOT Order 8000.1C, we request that FAA provide our office with additional information for recommendation 10 within 30 days of the date of this report.

Exhibit A. Scope and Methodology

We conducted this performance audit between March 2019 and May 2020 in accordance with generally accepted Government auditing standards as prescribed by the Comptroller General of the United States. 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 audit covered FAA's security controls selection, implementation, assessment, system authorization, and continuous monitoring for STARS. Audit criteria included DOT information technology policies and procedural guidance, FAA information technology procedural guidance, NIST, and Office of Management and Budget requirements and guidance. Stakeholders included FAA's Chief Information Officer and Chief Information Security Officer, information system security managers, and system and program owners. Our audit objectives were to (1) assess FAA's identification and mitigation of security risks in STARS and (2) determine whether FAA's contingency planning limits the effects caused by the loss of STARS operations at large TRACON facilities during emergencies.

To conduct our work, we reviewed STARS Security Assessment Reports, System Security Plan, System Characterization Document, Information System Contingency Plan and Test Results, and POA&Ms, which contain the security architecture, risk assessment, security plan, and test result. We also assessed how FAA identifies and mitigates security issues at the large TRACONs and interviewed FAA management and subject matter experts. We visited and interviewed STARS security personnel, including contract employees, and management at FAA Headquarters in Washington, DC, WJHTC in Atlantic City, NJ, and the [redacted]. We also reviewed the contingency plans of the [redacted] TRACONs. These three TRACONs were selected because [redacted].

We also assessed some of STARS facility security controls, including access control management and backup and storage at [redacted]. We performed walkthroughs at the [redacted] facility for user access management, backup and storage, physical and environmental security, and separation of duties.

To determine whether FAA's contingency planning limits the effects caused by the loss of STARS operations at large TRACON facilities during emergencies, we reviewed the TRACON contingency plans and test results and assessed the plan's

ability to maintain TRACON operations during emergency situations. We interviewed FAA management and subject matter experts to learn about any additional details or issues that could prevent air traffic resumption after a loss of services.

Exhibit B. Organizations Visited or Contacted

Federal Aviation Administration

FAA Headquarters, Washington, DC

William J. Hughes Technical Center, Atlantic City, NJ

[redacted]

Exhibit C. List of Acronyms

ARTS	Automated Radar Terminal Systems
ATO	Air Traffic Organization
CARTS	Common Automation Radar Terminal System
DoD	Department of Defense
DOT	Department of Transportation
FAA	Federal Aviation Administration
FY	fiscal year
NAS	National Airspace System
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
POA&M	Plan of Action and Milestones
SSI	sensitive security information
STARS	Standard Terminal Automation Replacement System
TRACON	Terminal Radar Approach Control
WJHTC	William J. Hughes Technical Center

Exhibit D. STARS Security Controls Requiring Updated POA&Ms

POA&M Number	Security Control	Weakness	Risk Level
1	CA-05.b	Update POA&MS listed below.	Low
2	[redacted]	[redacted].	High
3	[redacted]	[redacted]	High
4	[redacted]	[redacted]	High
5	[redacted]	STARS maintenance laptop does not [redacted].	Low
6	[redacted]	[redacted]	Very High
7	[redacted]	[redacted]	High
8	CM-02.1	The System Characterization Document (SCD) does not document all STARS assets.	Low
9	CM-02EN01	The FY19 STARS SCD does not describe the current baseline configuration.	Low
10	[redacted]	[redacted]	High
11	[redacted]	[redacted]	High
12	CM-07EN01	Develop and implement procedures to ensure scan results are analyzed and non-secure functions, (e.g., ports, and protocols) reported are remediated.	Low
13	[redacted]	[redacted]	High
14	[redacted]	[redacted]	High
15	IA-05.e	Scan testing discovered that some servers have easily guessed community string names.	Low

POA&M Number	Security Control	Weakness	Risk Level
16	[redacted]	[redacted]	High
17	[redacted]	[redacted]	High
18	[redacted]	[redacted]	High
19	[redacted]	[redacted]	High
20	[redacted]	[redacted]	High
21	[redacted]	[redacted]	Very High
22	[redacted]	[redacted]	Very High
23	[redacted]	[redacted]	High
24	[redacted]	[redacted]	High
25	[redacted]	[redacted]	High
26	SI-03EN01	System Security Plan (SSP) states that this control is planned and describes high-level procedures that will be implemented.	Low
27	SI-03EN02	SSP states that this control is planned and describes high-level procedures that will be implemented.	Low

Source: STARS FY 2019 Security Assessment Report

Exhibit E. Major Contributors to This Report

ABDIL **SALAH**	PROGRAM DIRECTOR
SEVERIN **PEFOUBOU**	PROJECT MANAGER
SHAVON **MOORE**	INFORMATION TECHONOLOGY SPECIALIST
ANTIONE **SEARCY**	INFORMATION TECHONOLOGY SPECIALIST
JAMILA **WILLIAMS-MOORE**	INFORMATION TECHONOLOGY SPECIALIST
RIFAT **MAJUMDAR**	INFORMATION TECHONOLOGY SPECIALIST
JANE **LUSAKA**	WRITER-EDITOR
GEORGE **ZIPF**	SENIOR STATISTICIAN
AMY **BERKS**	DEPUTY CHIEF COUNSEL

Appendix. Agency Comments

Federal Aviation Administration

Memorandum

Date: June 19, 2020

To: Kevin Dorsey, Acting Assistant Inspector General for Information Technology Audits

From: H. Clayton Foushee, Director, Office of Audit and Evaluation, AAE-1

Subject: Federal Aviation Administration's (FAA) Response to Office of Inspector General (OIG) Draft Report: FAA Is Not Remediating STARS Security Weaknesses in a Timely Manner and Contingency Planning Is Insufficient

The Federal Aviation Administration (FAA) has successfully transitioned from the Common Automated Radar Terminal System (CARTS) to the Standard Terminal Automation Replacement System (STARS) in support of National Airspace System (NAS) modernization. STARS implementation at the 11 Large Terminal Radar Approach Control Facilities (TRACONs) was completed in 2017, which included transition of all non-FAA connections, such as Noise Abatement, to System Wide Information Management (SWIM). STARS has proven to be a highly reliable and secure system that has met or exceeded system requirements for availability.

The FAA believes that the OIG has mischaracterized the security posture of STARS and how the Department of Transportation (DOT) security requirements should be applied to safety-critical systems, most notably:

- The vulnerability remediation timeframe requirements documented in the DOT Compendium and included in the OIG's Draft Report do not align with the requirements of STARS and of the NAS. NAS operational system changes are implemented via System Support Modifications that can take up to a year to safely implement. As stated in the International Civil Aviation Organization (ICAO) Safety Management Manual (SMM), "effective security measures may have negative impacts on safety." National Institute of Standards and Technology (NIST) 800-82 identifies "Air Traffic Control" as an example of an Industrial Control System (ICS) and states, "personnel responsible for operating, securing, and maintaining ICS must understand the important link between safety and security. Any security measure that impairs safety is unacceptable." The DOT Compendium does not provide any policy or guidance concerning security control tailoring for ICS assets; hence it is not a

comprehensive policy source document to support NAS/ICS based safety requirements and the possible unacceptable safety impacts.

- The draft report presents security scan vulnerability numbers, which represent raw data findings that have not been assessed against any actual threat or system exposure level. Presenting these raw data numbers mischaracterizes the STARS security posture, because it does not provide any context to relate them to actual security risk. FAA has performed the risk analysis associated with the raw data and has generated Plans of Action and Milestones (POAMs) items that define the assessed risk. Referencing the vulnerability scan raw finding counts versus POAMs items when defining STARS risk in the draft report is misleading.
- We dispute the OIG's assertion that [redacted] have been transitioned to SWIM, which uses the NAS Enterprise Security Gateway for distribution to non-NAS systems.

Upon review of the draft report, the FAA concurs with recommendations 3, 7, 8, 9 and 11. We plan to implement recommendations 3 and 7 by December 31, 2020; recommendations 8 and 9 by June 30, 2021; and recommendation 11 by June 30, 2022.

The FAA partially concurs with recommendations 1, 2, 4, 5, 6, and 10. For recommendations 1, 2, 4, 5 and 6, we plan to implement the recommendations in accordance with ICAO SMM, NIST 800-82, and NAS Configuration Management policies versus the DOT Compendium timeframe requirements. The FAA will implement these recommendations via delivery of POAMs by March 31, 2021.

For recommendation 10, the FAA is not required to establish alternate processing site agreements as recommended by the OIG. However, the FAA will update the contingency plans for the TRACONs identified to include formal procedures that ensure the transfer of published air traffic services to other sites. The FAA will complete documentation and confirm that the plans have been reviewed and approved by an authorized official by June 30, 2022.

We appreciate this opportunity to offer additional perspective on the OIG draft report. Please contact H. Clayton Foushee at (202) 267-9000 if you have any questions or require additional information about these comments.

~~SENSITIVE SECURITY INFORMATION~~

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