~~CONTROLLED UNCLASSIFIED INFORMATION (CUI) // SPECIFIED SENSITIVE SECURITY INFORMATION (SP-SSI)~~

FAA

Redacted Report FI2026023
April 1, 2026

FAA Does Not Effectively Secure Its High-Impact Systems Supporting the National Airspace System

Highlights

Federal Aviation Administration (FAA)
FI2026023 | April 1, 2026

FAA Does Not Effectively Secure Its High-Impact Systems Supporting the National Airspace System

Self-Initiated

Our Objective(s)

To assess whether FAA (1) has selected and implemented the required high-impact baseline security controls for its high-impact systems and (2) is mitigating potential vulnerabilities for its high-impact systems.

Why This Audit?

FAA relies on critical information systems to meet its mission of safely and efficiently managing air travel in the United States. In August 2021, we reported that FAA had re-categorized 45 information systems as high-impact systems. Further, we found FAA was not holding its high-impact system owners responsible for remediating high-security baseline control weaknesses. Given our previous findings, and the potential risks to the National Airspace System (NAS) if high-impact baseline security controls are not fully implemented, we self-initiated this audit.

What We Found

FAA has begun selecting and implementing required security controls for its high-impact systems supporting the NAS, but gaps remain.

- FAA has made progress but has not selected all required high baseline security controls for its systems that support the NAS. We found 15 of the 45 high-impact systems we reviewed had security controls selected under the outdated NIST SP 800-53 Revision 4 (Rev 4) standards, rather than the current Revision 5 (Rev 5) standards.
- FAA has not fully implemented required security controls for systems that support the NAS. According to system documentation we reviewed, FAA had not fully implemented 1,836 (11.3 percent) of the 16,245 required controls for the 45 systems.
- Some high-impact systems continue to have missing baseline security controls, according to their system documentation.
- According to FAA, these gaps exist in part because of technical and other challenges with FAA's systems. Until these gaps are filled, these systems may be vulnerable to cyberattacks that could cause severe or catastrophic effects on the NAS.

FAA does not fully track and mitigate all potential vulnerabilities for its high-impact systems in DOT's system of record.

- FAA is not tracking and mitigating vulnerabilities within DOT's system of record, as required. As a result, FAA is not being fully transparent with the Department in identifying its vulnerabilities.
- FAA has not ensured its security system documentation is fully updated with the status of all vulnerabilities.

4 **Recommendations** to mitigate the risks associated with not selecting and implementing all required high-baseline security controls and/or not fully mitigating potential vulnerabilities for FAA's 45 high-impact systems supporting the NAS. *(p. 13)*

Contents

U.S. Department of Transportation
Office of Inspector General

Memorandum

Date: April 1, 2026

Subject: ACTION: FAA Does Not Effectively Secure Its High-Impact Systems Supporting the National Airspace System | Report No. FI2026023

From: Dormayne "Dory" Dillard-Christian
Assistant Inspector General for Financial, IT, and Procurement Audits

To: Federal Aviation Administrator

The Federal Aviation Administration (FAA) relies on critical information systems to meet its mission of safely and efficiently managing air travel in the United States. In August 2021,[1] we reported that FAA had recategorized 45 information systems from low-or moderate-impact to high-impact systems. High-impact systems are those where a loss is expected to have a severe or catastrophic effect on organizational operations, assets, or individuals. These high-impact systems provide safety-critical services, such as air traffic control and communications. Therefore, if any of these systems fail, it would adversely impact FAA's mission and the safety and efficiency of the National Airspace System (NAS). After being recategorized to high-impact, these systems became subject to more stringent security controls.[2]

Selecting and implementing[3] required high-security baseline controls[4] such as penetration testing, supply chain protection, and other access controls is vital to securing NAS systems and mitigating cybersecurity risks. For example, FAA may be at an increased risk of successful cyberattacks if the Agency does not perform

[1] *FAA Is Taking Steps to Properly Categorize High Impact Information Systems, but Security Risks Remain Until High Security Controls Are Implemented* (OIG Report No. IT2021033), August 2, 2021. OIG reports are available on our website at http://www.oig.dot.gov.
[2] Security controls are 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 and organizations.
[3] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 Rev 2. Prepare, categorize, select, implement, assess, authorize, and monitor are the seven steps of the Risk Management Framework process.
[4] Baseline controls are the set of controls that are applicable to information or an information system to meet legal, regulatory, or policy requirements, as well as address protection needs for the purpose of managing risk.

comprehensive testing of its systems' security defenses and check for flaws in the supply chain software of its high-impact systems.

In 2021, we found FAA was taking steps to implement its high-security baseline controls for its recategorized high-impact systems but had not yet implemented mitigations for identified vulnerabilities. Given our previous findings, and the potential risks to the NAS if high-impact baseline security controls are not fully implemented, we self-initiated this audit. Our audit objectives were to assess whether FAA (1) has selected and implemented the required high-impact baseline security controls for its high-impact systems and (2) is mitigating potential vulnerabilities for its high-impact systems.

We conducted our work in accordance with generally accepted Government auditing standards. Exhibit A details our scope and methodology. Exhibit B lists the organizations we visited or contacted, and exhibit G lists the acronyms used in this report.

We appreciate the courtesies and cooperation of Department of Transportation (DOT) representatives during this audit. If you have any questions concerning this report, please contact me or Shirell Butcher, Program Director.

cc: The Secretary
DOT Audit Liaison, M-1
FAA Audit Liaison, AAE-001

Background

As FAA's operational arm, the Air Traffic Organization (ATO) is responsible for providing safe and efficient air navigation services in U.S.-controlled airspace. ATO also provides air navigation services in over 17 percent of the world's airspace, including large portions of international airspace over the Atlantic and Pacific Oceans and the Gulf of Mexico.

In response to prior Office of Inspector General (OIG) and Government Accountability Office (GAO)[5] audits, which documented that FAA had not rated any NAS critical infrastructure systems as high-impact, ATO started revalidating NAS systems to ensure appropriate security categorizations were applied. In 2021, we reported that FAA had recategorized 45 systems as high-impact (see exhibit C).[6]

The ATO Cybersecurity Group secures FAA's information technology (IT) systems and services against existing and evolving cybersecurity threats. Other functions include ensuring compliance with the Federal Information Security Modernization Act of 2014[7] (FISMA); conducting risk management activities; supporting NAS cyber operations; and establishing enterprise security strategies, services, partnerships, and guidance.

FAA's selection and implementation of high-impact security controls as well as mitigating potential vulnerabilities are based on standards in Federal Information Processing Standards (FIPS) 200[8] and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, as amended.[9] In accordance with NIST SP 800-37 Revision 2 (Rev 2), the system owner is responsible for the Selection step, which includes selecting, tailoring, and documenting the controls necessary for the protection of the information system and the agency's operations. Additionally, the system owner is responsible for the Implementation step, which includes the implementation and documentation of specific details of the control implementation in the system's security and privacy plans. These standards are mandatory for all Federal information systems and organizations. The table below displays Federal standards applicable to Federal information systems.

---

[5] GAO, *FAA Actions Are Urgently Needed to Modernize Aging Systems* (GAO Report No. GAO-24-17001), September 2024.

[6] For this report, our review focused on the 45 high-impact systems identified in our 2021 report.

[7] Public Law Number (Pub. L. No.) 113-283 (2014).

[8] NIST, *Minimum Security Requirements for Federal Information and Information Systems (FIPS 200),* March 2006.

[9] NIST, *Security and Privacy Controls for Federal Information Systems and Organizations* (NIST SP 800-53), September 2020 (Revision 5) and April 2013 (Revision 4).

Table. Federal Standards Applicable to Federal Information Systems

Criteria	Description
Federal Information Processing Standards (FIPS) 200	• A standard which specifies the minimum-security requirements for Federal information and information systems. • Federal agencies must meet the minimum-security requirements as defined herein using security controls in accordance with NIST SP 800-53.
NIST SP 800-37 Revision 2 (Rev 2)	• Provides guidelines on managing security and privacy risks, and six steps for conducting a gap analysis and applying the Risk Management Framework to information systems and organizations.
NIST SP 800-53 Revision 5 (Rev 5)	• Provides a comprehensive and flexible catalog of security and privacy controls to meet current and future protection needs based on changing threats, vulnerabilities, requirements, and technologies.

Source: OIG analysis of Federal standards.

FAA's air traffic control information systems we reviewed were organized into four major operational capabilities:[10]

- **Automation:** Operational facility types and services used to provide automated processing of data elements used in the NAS.
- **Communication:** Operational facility types and services used to transmit or receive voice or data.
- **Navigation and Weather:** Operational facility types and services used to provide navigational data and landing guidance information for pilots; and operational facility types and services used to provide meteorological data and guidance information.
- **Surveillance:** Operational facility types and services used for real-time detection and/or display of airborne or ground positional information for air traffic control.

[10] FAA Order 6000.5F, Facility, Service, and Equipment Profile (FSEP), June 29, 2022.

FAA Has Begun Selecting and Implementing Required Security Controls for Its High-Impact Systems Supporting the NAS, but Gaps Remain

FAA has begun to select and implement the required high security control baseline[11] for its 45 high-impact systems that support four major NAS operational capabilities: automation, communication, navigation and weather, and surveillance. However, FAA has not completed the selection of all required high baseline controls for its systems. In addition, FAA has not fully implemented the required high baseline security controls for its systems protecting the NAS, and some of the high-impact systems continue to have outdated system documentation. According to FAA, these gaps exist in part because of technical and other challenges with FAA's systems.

FAA Has Made Progress but Has Not Selected All Required High Baseline Security Controls for Its Systems

FAA has made progress selecting NIST SP 800-53 Revision 5 (Rev 5) high baseline security controls for its 45 recategorized high-impact systems. We performed a comprehensive risk assessment[12] by collecting and analyzing system security plans (SSPs) for the 45 systems. The SSP provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements. The SSP also documents the status of the selection of the high baseline security controls for the system.

In accordance with NIST SP 800-37 Rev 2 standards, FAA is required to select an initial set of controls for the system. Based on our review of the systems' SSPs, we found that FAA system owners selected NIST SP 800-53 high baseline security controls. However, several of the system owners[13] did not select all the required baseline security controls. We found 30 of the 45 systems had selected high baseline controls under NIST SP 800-53 Rev 5—NIST's most recent applicable

[11] The control baseline is the set of controls that are applicable to information or an information system to meet legal, regulatory, or policy requirements, as well as address protection needs for the purpose of managing risk.
[12] Risk assessment is a systematic process that identifies, analyzes, and evaluates potential risks to an organization, activity, or project, with the goal of minimizing their impact and ensuring informed decision-making.
[13] NIST SP 800-37 Rev 2. A system owner is an organizational official responsible for the development and maintenance of the security plans and ensures that the system is operated in accordance with the selected and implemented controls.

standards—which requires the selection of 370 high security controls. However, 15 systems had security controls selected under the outdated NIST SP 800-53 Rev 4, which required 343 high baseline security controls. As a result, these systems continue to be vulnerable because they are not meeting current Federal requirements under NIST SP 800-53 Rev 5 and NIST SP 800-37 Rev 2.

FAA Has Not Fully Implemented Required Security Controls for Systems That Support the NAS

While FAA officials have made progress on selection, those responsible for securing the 45 high-impact systems that support the NAS have not yet ensured the implementation of all required high baseline security controls. In accordance with NIST SP 800-37 Rev 2 standards, FAA is required to implement the controls, including describing how the controls are employed within a system and its environment of operation. According to the required system documentation we reviewed, FAA had not fully implemented 1,836 selected controls (11.3 percent) of the 16,245 required controls for the 45 systems, including 717 that were documented as *not implemented* and 1,119 that were documented as *planned*. "Not implemented" denotes that the specified security control is entirely absent, has not been tested, or only exists in a form that fails to satisfy the required control objectives.[14] "Planned" signifies that the weakness has been formally identified and a plan has been established to implement the control in order to mitigate accepted risk. FAA officials stated some system owners use the terms "not implemented" and "planned" interchangeably when documenting the control implementation statuses, which is not in accordance with DOT's guidance. Without properly implementing all required high-impact security controls, FAA cannot ensure required safeguards are in place to protect the systems from being compromised, which may cause a severe impact on the NAS and the flying public. Specifically, figure 1 (and exhibit D) shows the security control implementation status for the high-impact systems that provide NAS operational capabilities at FAA facilities.

[14] DOT Security Weakness Management Guide, version 4.0, January 2020.

Figure 1. Number of High Baseline Controls Planned and Not Yet Implemented for High-Impact Systems

Totals by Capability	Automation	Communication	Navigation	Surveillance
Rev 5				
Not Implemented	75	75	37	104
Planned	239	221	3	412
Rev 4				
Not Implemented	196	113	1	116
Planned	133	43	0	68

Source: OIG analysis of FAA data.

Some High-Impact Systems Continue To Have Missing Baseline Security Controls According to Their System Documentation

Although FAA has made progress selecting controls for its high-impact systems, our review found that FAA's documentation did not accurately reflect the current security postures[15] for many of its systems. NIST 800-37 Rev 2 states system owners are required to update and document control implementation details and the impact of the changes on the security posture of each system. Therefore, as controls are implemented, the security plans are required to be updated. However, for 38 of the 45 (84 percent) high-impact systems, FAA did not update documentation for the required high baseline security controls. Instead, FAA documented some of the controls in the SSPs as planned or not implemented, or the controls were just not accounted for or missing. In many cases, even though FAA had selected NIST SP 800-53 Rev 5 controls for its systems, the systems were still documented under Rev 4 requirements. During our audit, FAA officials acknowledged that the system documentation had not been updated to present an accurate security posture for some systems that were using NIST SP 800-53 Rev 5 security controls. As a result, it is not clear whether these systems have the required up-to-date controls necessary to protect them.

[15] A security posture is the security status of an enterprise's networks, information, and systems based on information assurance resources (e.g., people, hardware, software, policies) and capabilities in place to manage the defense of the enterprise and to react as the situation changes.

Figure 2 below shows the number of systems we identified with non-compliant SSP documentation, and the operational capabilities of those systems.

Figure 2. Number of High-Impact Systems With NIST SP 800-53 Rev 4 Documentation Instead of the Required NIST SP 800-53 Rev 5 SSP Documentation

Operational Capability	Number of SSPs documented Rev 4	Number of SSPs documented Rev 5	Total Systems
Automation	13	1	14
Communication	9	2	11
Navigation and Weather	2	1	3
Surveillance	14	3	17
Total	**38**	**7**	**45**

Source: OIG analysis of FAA data.

Technical and Other Challenges Limit FAA's Ability To Select, Implement, and Document Required Controls

According to FAA, the gaps in FAA's selection, implementation, and documentation of all required controls are due to several factors. Specifically, FAA stated that system owners face critical challenges with funding limitations, technical constraints, and operational complexities. Additionally, FAA noted that many of its existing systems are not easily upgradeable, requiring either significant technical modifications or entirely new procurements. Integrating these controls into legacy systems often necessitates extensive retrofitting, which can significantly increase costs and delay implementation timelines.

Nevertheless, not addressing the need for selecting, implementing, and sufficiently documenting all required high baseline security controls for these high-impact systems may affect FAA's ability to maintain and protect these critical systems. As a result, these systems may be vulnerable to cyberattacks that could cause severe or catastrophic effects on the NAS.

FAA Does Not Fully Track and Mitigate All Potential Vulnerabilities for Its High-Impact Systems

FAA is not tracking and mitigating all vulnerabilities within DOT's system of record, as required. As a result, FAA is not being fully transparent with the Department in identifying its vulnerabilities. In addition, FAA has not ensured its system security documentation is sufficiently updated with the status of all vulnerabilities.

FAA Has a Process for Tracking Potential Vulnerabilities, but Its Primary Method Is Not DOT's Official System of Record

While FAA tracks potential vulnerabilities and weaknesses for high-impact systems within its internal tracking system, FAA does not use DOT's system of record—Cyber Security Assessment & Management (CSAM)[16]—as its primary source for tracking and mitigating as required. According to DOT[17] and FAA[18] policy, FAA is required to create a Plan of Action & Milestone (POA&M) for tracking all vulnerabilities discovered during the security control assessment process. Additionally, FAA must enter all POA&Ms related to NIST SP 800-53 into CSAM.

FAA has conducted assessments and documented identified vulnerabilities; however, these vulnerabilities were not reported, tracked, and mitigated within CSAM. Instead, FAA officials use an internal tracking system, Security Management & Assessment Reporting Tool (SMART), as the primary source for documenting, tracking, and mitigating potential vulnerabilities for FAA systems. According to FAA, the Agency's deficiencies of tracking and documenting vulnerabilities within CSAM are due to lack of funding, technical issues with upgrading legacy systems, and limited operational resources. FAA officials further acknowledged that their use of SMART has caused a significant delay in the reporting of vulnerabilities within CSAM due to having to input vulnerabilities within CSAM manually. In May 2025, FAA officials stated that they are working

[16] CSAM is a comprehensive FISMA monitoring system created by the Department of Justice. CSAM is the DOT-wide weakness management system and is the official repository for all Programs and Systems across the Department.
[17] DOT Security Weakness Management Guide, version 4.0, January 2020.
[18] Fiscal Year 2024 FAA Security Authorization Handbook, October 2023.

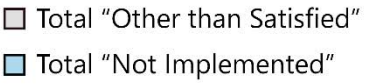
with the Department to automate a process for transferring vulnerabilities from SMART to CSAM.

We identified potential high-impact baseline security control assessment vulnerabilities that were not being tracked in CSAM. For example, we found that all systems supporting Automation, Communication, and Navigation and Weather capabilities had vulnerabilities that were not reported, tracked, and mitigated. For the Surveillance capability, 14 of the 17 systems had vulnerabilities that were not reported, tracked, and mitigated.

Figure 3 below lists the total number of vulnerabilities that were not tracked in CSAM for each group of systems providing operational capabilities to the NAS (also see exhibit E).

Figure 3. Overall Security Control Assessment Vulnerabilities Not Tracked in CSAM

Rev 4			Rev 5		
Automation	114	114	Automation	158	52
Communication	14	25	Communication	351	24
Navigation/ Weather	9	0	Navigation/ Weather	58	7
Surveillance/ Flight Services	109	4	Surveillance/ Flight Services	249	32



Source: OIG analysis of FAA data.

Although FAA tracks these vulnerabilities internally in SMART, without properly documenting, tracking, and mitigating potential vulnerabilities as required within CSAM, FAA is not providing transparency to the rest of DOT. Lack of transparency increases the risk that FAA and the Department may not be able to identify common threats and vulnerabilities or provide comprehensive IT weakness tracking and reporting.

FAA Has Not Ensured Its System Security Plans Are Fully Updated With the Status of All Vulnerabilities

While FAA has made progress identifying vulnerabilities within its high-impact systems, FAA's SSP security control documentation does not accurately reflect the current security control implementation statuses for its baseline security controls for its high-impact systems. DOT's Security Authorization and Continuous Monitoring Guide[19] states that system owners are responsible for documenting security control implementation with enough detail to enable a compliant implementation of the control. Yet, many high-impact system SSPs inaccurately reflect the implementation status of controls as "implemented" even though the controls were assessed as "other than satisfied"[20] within the Security Assessment Results (SAR) (see figure 4 and exhibit F).

Figure 4. Number of High-Impact Controls Inaccurately Documented for High-Impact Systems

Total Controls Inaccurately Documented in SSP							
Rev 4				Rev 5			
Automation	Communication	Navigation/ Weather	Surveillance/ Flight Services	Automation	Communication	Navigation/ Weather	Surveillance/ Flight Services
170	35	8	38	281	257	70	298

Source: OIG analysis of FAA data.

[redacted]

[19] DOT Security Authorization & Continuous Monitoring Performance Guide, September 2019. The System Owner is responsible for documenting security control implementation with enough detail to enable a compliant implementation of the control. Security control documentation describes how system-specific, hybrid, and common controls are implemented.

[20] NIST SP 800-53A Rev 5. A finding of "other than satisfied" may also indicate that the assessor was unable to obtain sufficient information to make the determination called for in the determination statement for reasons specified in the assessment report.

According to FAA, these gaps in tracking and documenting vulnerabilities are due in part to funding limitations, technical constraints, and operational complexities, as previously noted above. As a result, FAA authorizing officials lack accurate information on whether the required high baseline controls are implemented correctly and working as intended.

Conclusion

FAA's high-impact systems play a critical role in the safety and efficiency of operations within the NAS. Although FAA recategorized 45 of these systems as high-impact and began selecting and implementing high baseline security controls several years ago, FAA has not completed implementing controls for automation, communication, navigation and weather, and surveillance systems. Because FAA has not ensured that all required high baseline security controls have been selected, properly implemented, documented, and tracked, or that risks have been otherwise mitigated where controls cannot be implemented, many of FAA's high-impact systems remain vulnerable to cyberattacks. Consequently, FAA cannot have assurance that critical NAS systems are protected from cybersecurity threats that could severely disrupt air traffic operations.

Recommendations

To mitigate the risks associated with not selecting and implementing all required high-baseline security controls and/or not fully mitigating potential vulnerabilities for the 45 high-impact systems supporting the National Airspace System, we recommend that the Federal Aviation Administrator:

1. Identify all required National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev 5 high baseline security controls that have not yet been selected and implemented, conduct a security impact analysis to document potential security ramifications from not implementing the identified controls, and develop plans of action and milestones.

2. Identify and update system documentation that has outdated NIST SP 800-53 security controls documented within the System Security Plan (SSP) and update all SSP documentation and appendices to reflect the current selection and implementation status of security controls.

3. Develop and implement a process to ensure that system vulnerabilities currently being tracked only in FAA's Security Management & Assessment

Reporting Tool (SMART) system are fully tracked within Cyber Security Assessment & Management (CSAM), the Departmental system of record.

4. Update and track mitigation efforts for all identified NIST SP 800-53 Rev 5 high baseline security controls that were assessed as either "other than satisfied" or with an implementation status as "not implemented;" and accurately document the controls implementation status within the SSP.

Agency Comments and OIG Response

We provided FAA with our draft report on January 26, 2026. On March 9, 2026, we received FAA's response, which is included as an appendix to this report. FAA concurred with all four of our recommendations and proposed appropriate actions and completion dates. Accordingly, we consider all recommendations resolved but open pending completion of the planned actions.

Actions Required

We consider recommendations 1 through 4 resolved but open pending completion of planned actions.

Exhibit A. Scope and Methodology

This performance audit was conducted between October 2024 and January 2026. 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 audit objectives for this self-initiated audit were to assess whether FAA (1) has selected and implemented the required high-impact baseline security controls for its high-impact systems and (2) is mitigating potential vulnerabilities for its high-impact systems.

To address our objectives, we reviewed relevant Federal, DOT, and FAA information security laws, regulations, policies, procedures, and plans for selecting, implementing, and assessing high baseline security controls. We relied on the high-impact security baseline controls as required by NIST.

To determine whether FAA had selected and implemented the required high security baseline controls for its 45 high-impact systems, we assessed whether FAA has properly (1) selected, implemented, and assessed the required security controls and (2) developed and implemented any mitigation strategies to address potential vulnerabilities.

We also interviewed FAA cybersecurity officials and reviewed Federal, departmental, and FAA policies and procedures to determine whether FAA has maintained proper oversight to provide the required cybersecurity protection for its high-impact systems.

We collected and reviewed Authorization to Operate/Decision Letters within the high-impact system security documentation to verify the official management decision by a senior FAA official to authorize operation of its high-impact information systems and whether the official had explicitly accepted the risk to agency operations based on the implementation statuses of specific high baseline security and privacy controls.

We collected and reviewed system categorization documentation to determine whether FAA categorized the system and the information processed, stored, and transmitted based on an analysis of the impact of loss to determine their criticality to FAA's NAS operational capabilities (e.g., automation, communication, navigation and weather, and surveillance), and the potential impact on FAA's facilities/services and mission if the high-impact systems were compromised.

We conducted interviews with FAA security officials responsible for the high-impact systems in FAA Headquarters, including contract employees and ATO NAS management, to get an understanding of the process for selection, implementation, and assessment of high baseline security controls and how vulnerabilities are being mitigated and tracked.

We assessed whether FAA applied NIST Risk Management Framework steps for selecting and implementing security controls for its high-impact systems, which provides a disciplined, structured, and flexible process for managing security and privacy risk.

We collected and reviewed SSPs and associated workbooks to determine the selection of high baseline security controls for the system as needed to reduce risk to an acceptable level based on an assessment of risk. We also used this review to determine the implementation statuses of security controls and how the controls are employed within the system and its environment of operation. We then performed a comprehensive risk assessment by analyzing SSPs for the 45 systems to determine whether patterns existed between the security controls documented as not implemented, planned, or missing.

We collected and reviewed SAR documentation to determine whether the controls were implemented correctly, operating as intended, and producing the desired outcomes with respect to satisfying the security and privacy requirements. We conducted analysis on the SAR for each system to determine whether FAA is effectively mitigating vulnerabilities for the high baseline security controls implemented that did not satisfy testing and determined whether FAA created POA&Ms that documented its planned remedial actions to correct and track.

Lastly, we collected and reviewed POA&Ms for the high-impact systems to identify whether FAA planned remedial actions to correct weaknesses or deficiencies as documented in the SAR based on the assessment of the baseline security controls, which allowed us to determine whether FAA is mitigating and tracking all potential vulnerabilities for the 45 high-impact systems.

Exhibit B. Organizations Visited or Contacted

FAA

Federal Aviation Administration Headquarters, Washington, DC

DOT

Office of the Secretary of Transportation, Washington, DC

Office of the Chief Information Officer, Washington, DC

Exhibit C. FAA's 45 Recategorized High-Impact Systems

Exhibit D. Number of Rev 5 High Baseline Controls Not Yet Implemented for High-Impact Systems

[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
	[redacted]		[redacted]	[redacted]
	[redacted]		[redacted]	[redacted]
	[redacted]		[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]	[redacted]
	[redacted]		[redacted]	[redacted]
	[redacted]		[redacted]	[redacted]
	[redacted]		[redacted]	[redacted]
	[redacted]		[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]	[redacted]
	[redacted]		[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]	[redacted]
	[redacted]		[redacted]	[redacted]
	[redacted]		[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
	[redacted]		[redacted]	[redacted]
	[redacted]		[redacted]	[redacted]
	[redacted]		[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]	[redacted]
	[redacted]		[redacted]	[redacted]
	[redacted]		[redacted]	[redacted]
	[redacted]		[redacted]	[redacted]
	[redacted]		[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]	[redacted]
	[redacted]		[redacted]	[redacted]
	[redacted]		[redacted]	[redacted]
	[redacted]		[redacted]	[redacted]

[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]	[redacted]
	[redacted]		[redacted]	[redacted]
	[redacted]		[redacted]	[redacted]
	[redacted]		[redacted]	[redacted]
	[redacted]		[redacted]	[redacted]
	[redacted]		[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]	[redacted]
	[redacted]		[redacted]	[redacted]
	[redacted]		[redacted]	[redacted]
	[redacted]		[redacted]	[redacted]
[redacted]	[redacted]		[redacted]	[redacted]
	[redacted]		[redacted]	[redacted]
	[redacted]		[redacted]	[redacted]
	[redacted]		[redacted]	[redacted]
	[redacted]		[redacted]	[redacted]
	[redacted]		[redacted]	[redacted]
	[redacted]		[redacted]	[redacted]
	[redacted]		[redacted]	[redacted]
	[redacted]		[redacted]	[redacted]
	[redacted]		[redacted]	[redacted]
	[redacted]		[redacted]	[redacted]
	[redacted]		[redacted]	[redacted]

[redacted]

Exhibit E. Overall Security Control Assessment Vulnerabilities Not Tracked in CSAM

[redacted]	[redacted]	[redacted]
[redacted]		
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]		
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]		
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]		
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

[redacted]

Exhibit F. Number of High-Impact Controls Inaccurately Documented for High-Impact Systems

[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]

[redacted]

Exhibit G. List of Acronyms

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
ATO	Air Traffic Organization
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
CSAM	Cyber Security Assessment and Management
CUI	Controlled Unclassified Information
[redacted]	[redacted]
[redacted]	[redacted]
DOD	Department of Defense
DOT	Department of Transportation
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
FAA	Federal Aviation Administration
[redacted]	[redacted]

[redacted]	[redacted]
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
[redacted]	[redacted]
IT	Information Technology
[redacted]	[redacted]
NAS	National Airspace System
[redacted]	[redacted]
NIST	National Institute of Standards and Technology
[redacted]	[redacted]
OIG	Office of Inspector General
POA&M	Plan of Action & Milestones
[redacted]	[redacted]
REV	Revision
[redacted]	[redacted]
SAR	Security Assessment Report
[redacted]	[redacted]
SP	Special Publication

SSP	System Security Plan
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
	[redacted]
[redacted]	[redacted]

Exhibit H. Major Contributors to This Report

SHIRELL **BUTCHER**	PROGRAM DIRECTOR
LEON **LUCAS**	PROGRAM DIRECTOR
STACY **JORDAN**	PROJECT MANAGER
JO'SHENA **JAMISON**	SENIOR IT SPECIALIST
JASON **MOTT**	SENIOR IT SPECIALIST
THADDEUS **PATRICE, JR**	SENIOR IT SPECIALIST
AUDRE **AZUOLAS**	CHIEF COMMUNICATIONS OFFICER
CELESTE **VERCHOTA**	SENIOR COUNSEL

Appendix. Agency Comments

SENSITIVE SECURITY INFORMATION

Federal Aviation Administration

Memorandum

Date: March 9, 2026

To: Dormayne "Dory" Dillard-Christian, Assistant Inspector General for Financial, IT, and Procurement Audits

BARBARA LOURDES BARNET Digitally signed by BARBARA LOURDES BARNET Date: 2026.03.09 09:58:44 -04'00'

From: Barbara Barnet, Deputy Director, Office of Audit and Evaluation, AAE-2

Subject: Management Response to Office of Inspector General (OIG) Draft Report on FAA Does Not Effectively Secure Its High-Impact Systems Supporting the National Airspace System | Project No. 24T3004T000

The Federal Aviation Administration (FAA) is committed to selecting and implementing required high-security baseline controls, such as penetration testing, supply chain protection, and other access controls that are vital to securing our National Airspace System (NAS) and mitigating cybersecurity risks. FAA is actively taking measures to enhance further the implementation of all National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev 5 high-baseline security controls of the 45 NAS High-Impact systems. Additional efforts include enhancing the integration of system and risk data from the Security Management and Assessment Reporting Tool (SMART) to the Department's system of record Cyber Security Assessment & Management (CSAM) platform.

Based on our review of the draft report, we concur with the four recommendations as written and plan to implement them fully by December 31, 2026.

We appreciate this opportunity to respond to the OIG draft report. Please contact Barbara Barnet at Barbara.Barnet@faa.gov, if you have any questions or require additional information about these comments.

~~CUI//SP-SSI~~

U.S. Department of Transportation
Office of Inspector General

Fraud, Waste, & Abuse Hotline

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

OUR MISSION

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

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