Report No. DOWIG-2026-083

INSPECTOR GENERAL

U.S. Department of War

MAY 13, 2026

(U) Audit of Cyber Vulnerabilities Impacting Department of the Air Force Defense Critical Infrastructure

~~Classified By: Sean J. Keaney, Acting Assistant Inspector General for Audit, Cyberspace Operations~~
~~Derived From: Multiple Sources~~
~~Declassify On: 20510513~~

~~Controlled By: DoW OIG~~
~~Controlled By: Audit, Cyberspace Operations~~
~~CUI Category: DCRIT~~
~~Distribution/Dissemination Control: FEDCON~~
~~POC: [redacted]~~

~~This content is classified at the Secret//NOFORN level and may contain elements of controlled unclassified information (CUI), unclassified, or information classified at a lower level than the overall classification displayed. This content shall not be used as a source of derivative classification; refer instead to the applicable classification guides. It must be reviewed for both Classified National Security Information (CNSI) and CUI in accordance with DoWI 5230.09 prior to public release.~~

INDEPENDENCE ★ INTEGRITY ★ EXCELLENCE ★TRANSPARENCY

Pursuant to Executive Order 14347, "Restoring the United States Department of War," September 5, 2025, the Department of Defense Inspector General (DoD IG) and Office of Inspector General (DoD OIG) use the secondary titles of the Department of War Inspector General (DoW IG) and Office of Inspector General (DoW OIG), respectively. The use of these secondary titles does not in any way affect the primary statutory title or authorities of the DoD IG under The Inspector General Act of 1978, as amended (5 U.S.C. Chapter 4, Inspectors General), or the authorities or responsibilities of the DoD IG or DoD OIG pursuant to any laws, regulations, or policies.

Results in Brief

(U) Audit of Cyber Vulnerabilities Impacting Department of the Air Force Defense Critical Infrastructure

May 13, 2026

(U) Objective

(U) The objective of this audit was to assess the progress made by the Department of the Air Force (DAF) in mitigating the Defense Critical Infrastructure (DCI) cybersecurity vulnerabilities identified during DoD assessments conducted in response to Section 1650 of the National Defense Authorization Act for FY 2017.

(U) Background

(U) DCI is any DoW asset of such extraordinary importance to the DoW and Armed Forces that its incapacitation or destruction would have a debilitating effect on the DoW's ability to fulfill its mission.

(U) Finding

~~(CUI)~~ The DAF made progress in mitigating cybersecurity vulnerabilities identified during Section 1650 assessments at the five installations we visited but additional actions are needed. Of the [redacted] risk vulnerabilities in the sample we reviewed, DAF officials:

- ~~(CUI)~~ mitigated [redacted] risk) vulnerabilities;
- ~~(CUI)~~ partially mitigated [redacted] risk) vulnerabilities;
- ~~(CUI)~~ had plans in place to mitigate [redacted] risk) vulnerabilities; and
- ~~(CUI)~~ did not take action to mitigate [redacted] risk) vulnerabilities.

~~(CUI)~~ Although DAF officials prioritized the identified vulnerabilities, they did not take action to mitigate some vulnerabilities identified during Section 1650 assessments because all five installations lacked staff with cybersecurity expertise to mitigate the vulnerabilities.

Finding (cont'd)

~~(CUI)~~ In addition to the vulnerabilities in our sample, DAF officials stated that they did not take action for [redacted] risk vulnerabilities at other DAF installations. DAF officials did not take action for these vulnerabilities or ensure responsible officials were aware of the vulnerabilities because they misunderstood the scope of the assessments.

(U) These vulnerabilities, if left unmitigated, provide adversaries and malicious actors with opportunities to adversely affect critical missions or functions and the DAF's ability to deploy, support, and sustain military forces worldwide.

(U) Since June 2025, the Federal Bureau of Investigation, National Security Agency, and Cybersecurity and Infrastructure Security Agency have reported that Iranian-affiliated cyber actors and hacktivist groups are aggressively targeting U.S. critical infrastructure, which further emphasizes the DAF's need to take corrective actions to minimize the threat that adversaries and other malicious actors pose to DCI.

(U) Recommendations

(U) Among other recommendations, we recommended that the Director of Civil Engineers, in coordination with Air Force Civil Engineer Control Systems, Air Force Civil Engineer Center (AFCEC), Cyber Resiliency Office for Control Systems, and installation officials immediately notify non-AFCEC components of the vulnerabilities identified during Section 1650 assessments that affect their control systems and develop and implement a process to verify that corrective actions were taken to mitigate those cybersecurity vulnerabilities.

Results in Brief

(U) Audit of Cyber Vulnerabilities Impacting Department of the Air Force Defense Critical Infrastructure

(U) Management Comments and Our Response

(U) The Assistant Deputy Chief of Staff for Logistics, Engineering, and Force Protection, responding for the Director of Civil Engineers, agreed with and provided planned actions for all recommendations; therefore, they are resolved but open. We will close the recommendations once we verify that management has implemented the agreed-upon actions. Please see the Recommendations Table on the next page for the status of the recommendations.

(U) Recommendations Table

~~(S//NF)~~ Management	Recommendations Unresolved	Recommendations Resolved	Recommendations Closed
(U) Director of Civil Engineers	None	1 and 3	None
~~(S//NF)~~ Base Civil Engineer, [redacted]	None	2	None ~~(S//NF)~~

NOTE: The following categories are used to describe agency management's comments to individual recommendations.

- **Unresolved** – Management has not agreed to implement the recommendation or has not proposed actions that will address the recommendation.
- **Resolved** – Management agreed to implement the recommendation or has proposed actions that will address the underlying finding that generated the recommendation.
- **Closed** – The DoD OIG verified that the agreed upon corrective actions were implemented.

OFFICE OF INSPECTOR GENERAL
DEPARTMENT OF WAR
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

May 13, 2026

MEMORANDUM FOR AUDITOR GENERAL, DEPARTMENT OF THE AIR FORCE

SUBJECT: (U) Audit of Cyber Vulnerabilities Impacting Department of the Air Force Defense Critical Infrastructure (Report No. DOWIG-2026-083)

(U) This final report provides the results of the DoW Office of Inspector General's audit. We previously provided copies of the draft report and requested written comments on the recommendations. We considered management's comments on the draft report when preparing the final report. These comments are included in the report.

(U) The Assistant Deputy Chief of Staff for Logistics, Engineering, and Force Protection, responding for Director of Civil Engineers, agreed to address all the recommendations presented in the report; therefore, we consider the recommendations resolved and open. We will close them when you provide us documentation showing that all agreed upon actions are completed. Therefore, please provide us within 90 days your response concerning specific actions in process or completed on the recommendations. Send your response to either aud.cso@dodig.mil if unclassified or [redacted] if classified SECRET.

(U) If you have questions, please contact me at [redacted]. We appreciate the cooperation and assistance received during the audit.

Sean J. Keaney
Acting Assistant Inspector General for Audit
Cyberspace Operations

Contents

(U) Introduction

(U) Objective

(U) The objective of this audit was to assess the progress made by the Department of the Air Force (DAF) in mitigating the Defense Critical Infrastructure (DCI) cybersecurity vulnerabilities identified during DoD assessments conducted in response to Section 1650 of the National Defense Authorization Act (NDAA) for FY 2017.[1] This audit is the second in a series of audits related to the DoW's efforts to mitigate control system cybersecurity vulnerabilities impacting DCI.[2]

(U) Background

(U) The National Security Memorandum on Critical Infrastructure Security and Resilience provides U.S. policy for strengthening the security and resilience of critical infrastructure against both physical and cyber threats.[3] The Memorandum requires Federal agencies to identify, prioritize, assess, remediate, and secure critical infrastructure that supports mission-essential functions, which are functions that must continue regardless of any incident, event, or threat.

(U) DCI is any DoW asset of such extraordinary importance to the DoW and the operation of the Armed Forces that its incapacitation or destruction would have a debilitating effect on the DoW's ability to fulfill its mission. DCI includes any networked asset (physical or virtual) or facility essential to support and sustain military forces and operations worldwide. For example, dams, information technology, nuclear reactors, and water and wastewater systems and facilities are DCI when critical to the DoW's mission to deter war and ensure national security.

[1] (U) This report contains information that has been redacted because it was identified by the Department of War as Controlled Unclassified Information (CUI) that is not releasable to the public. CUI is Government-created or owned unclassified information that allows for, or requires, safeguarding and dissemination controls in accordance with laws, regulations, or Government-wide policies. Public Law 114-328, "National Defense Authorization Act for Fiscal Year 2017," section 1650, "Evaluation of Cyber Vulnerabilities of Department of Defense Critical Infrastructure," December 23, 2016. Section 1650 of the FY 2017 NDAA used the term "evaluations" to discuss the reviews required while the DoD called the reviews "assessments." We use the term "assessments," except when discussing the requirement in the NDAA.

[2] (U) Pursuant to Executive Order 14347, "Restoring the United States Department of War," September 5, 2025, the Department of War Inspector General and Office of Inspector General use the secondary titles of all Department of War Components. The use of these secondary titles does not in any way affect the primary statutory title or authorities of Department of War Components pursuant to any laws, regulations, or policies.

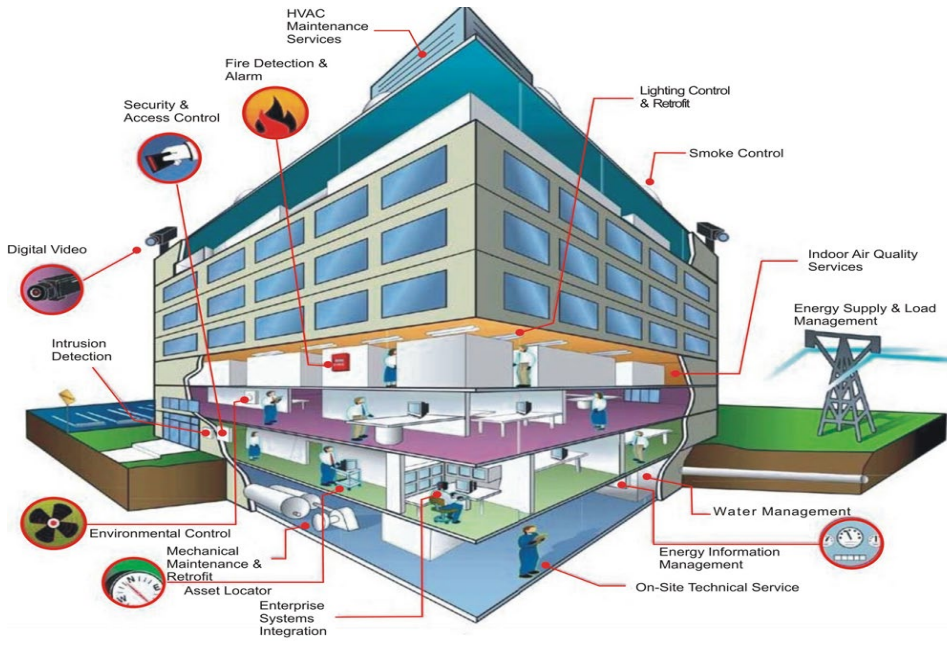
[3] (U) National Security Memorandum 22, "The National Security Memorandum on Critical Infrastructure Security and Resilience," April 30, 2024.

(U) The DoW's reliance on DCI presents opportunities for adversaries to exploit cybersecurity vulnerabilities to compromise, incapacitate, or degrade DoW missions and essential operations. Compromised DCI can severely impact the DoW's ability to deploy, support, and sustain critical missions and operations in the United States and abroad.

(U) Control systems are specialized systems and mechanisms that support infrastructure by ensuring infrastructure services are delivered to accomplish the mission.[4] Infrastructure services include electricity, fluids, gas, air movement, traffic control, and water distribution. Control systems can operate or monitor equipment and are essential to the function of weapon systems, utilities, facilities, medical systems, and other assets. Facility-related control systems are a subset of control systems designed to manage facility-specific systems, such as heating, ventilation, air conditioning, lighting, access control operations, automated building operations, security alarms, and energy efficiency. Figure 1 shows an example of how control systems are embedded into infrastructure.

(U) Figure 1. Example of Embedded Control Systems in Infrastructure

(U)



(U)

(U) Source: The DAF.

[4] (U) A control system is a system of digital controllers, communication architecture, and user interfaces that monitor, or monitor and control, infrastructure and equipment as defined by the United Facilities Criteria 4-010-06, "Cybersecurity of Facility-Related Control Systems," effective September 19, 2016.

(U) DoW Requirements and Responsibilities for Protecting Defense Critical Infrastructure

(U) DoD Directive 3020.40 requires DoW Components to implement Presidential Policy Directive-21 requirements for protecting DCI through existing mission assurance policy and activities.[5] DoD Directive 3020.40 focuses on mission assurance, which is the DoW's process for protecting or ensuring continuation and resiliency of DoW mission-essential functions, capabilities, and assets, such as DCI.

(U) DoD Instruction 3020.45 further defines processes for mission owners to follow for managing risk that consists of either accepting risk, building redundancy, or reducing risk through mitigation or remediation.[6] DoD Manual 8530.01 requires DoW Components to take corrective actions to mitigate vulnerabilities or threats to a Component's assets, which includes DCI and associated control systems.[7] In addition, the Manual requires DoW Components to track the status of vulnerability remediation in a corrective action plan for the asset or capability.

(U) DAF Guidance Memorandum 2024-32-01 establishes cybersecurity policy for Civil Engineer-owned control systems.[8] The Memorandum implements policy for securing and mitigating cybersecurity risk to control systems and outlines roles and responsibilities for managing risks. The Memorandum states that control systems support nearly all aspects of DAF core mission areas; by extension, if the control systems can be compromised, so can the missions they support.

(U) FY 2017 NDAA Section 1650 Requirements

(U) Section 1650 of the FY 2017 NDAA required the Secretary of Defense to:

- (U) submit to Congress a plan for evaluating the cyber vulnerabilities of the DoD's critical infrastructure,
- (U) prioritize the evaluation of military installations as determined by the Chairman of the Joint Chiefs of Staff,

[5] (U) DoD Directive 3020.40, "Mission Assurance," November 29, 2016 (Change 1 Effective September 11, 2018). Presidential Policy Directive 21 was effective when the DAF conducted its Section 1650 cybersecurity assessments but was superseded by National Security Memorandum 22 on April 30, 2024.

[6] (U) DoD Instruction 3020.45, "Mission Assurance Construct," August 14, 2018 (Change 1 Effective May 2, 2022). Mitigation is an action taken to lessen the effects on a given military operation or infrastructure. Remediation is an action to correct known deficiencies and avoid the effects an exploited vulnerability could cause.

[7] (U) DoD Manual 8530.01, "Cybersecurity Activities Support Procedures," May 31, 2023.

[8] (U) Department of the Air Force Guidance Memorandum 2024-32-01, "Civil Engineer Control Systems Cybersecurity," October 16, 2024.

- (U) identify cyber vulnerabilities affecting DCI, and
- (U) develop strategies to mitigate the risks of those vulnerabilities.

~~(CUI)~~ The Under Secretary of Defense for Acquisition and Sustainment, on behalf of the Secretary of Defense, provided Congress the DoD's [redacted] in May 2018.[9] The DoD response plan provided the framework that the DoD planned to use to accomplish the assessments, including identifying the installations the DoD planned to review and outlining the methodology for completing assessments to identify cybersecurity vulnerabilities.

~~(CUI)~~ The Secretary of Defense prioritized the evaluation of military installations based on the criticality of the infrastructure, mission of the Armed Forces stations at the installation, and installation threats as determined by the Chairman of Joint Chiefs of Staff. [redacted] The Joint Staff list identified 64 installations—24 Army, 12 Navy, and 28 Air Force with the highest priority critical infrastructure. See Appendix B for the list of the DAF installations where Section 1650 assessments were conducted and the date of the assessment report.

(U) Department of the Air Force Section 1650 Assessments

~~(S//NF)~~ DAF officials requested support from the National Security Agency to complete their Section 1650 assessments. The National Security Agency Platform Resiliency and Mission Assurance Team completed Section 1650 assessments at 29 installations between July 25, 2019, and September 27, 2021.[10] Officials from the Director of Civil Engineers and Air Force Civil Engineer Center (AFCEC) jointly developed the [redacted] Expectations and Mitigation Procedures," to establish roles and responsibilities for Air Force Civil Engineers Cyber Integration (A4CIC), AFCEC, and installation officials for updating plans of action and milestones and mitigating the vulnerabilities identified during Section 1650 assessments.[11] A4CIC officials assigned the responsibilities of leading the

[9] ~~(CUI)~~ Under Secretary of Defense for Acquisition and Sustainment, [redacted] May 31, 2018.

[10] ~~(S//NF)~~ Our review did not include the assessment of [redacted] because the Office of the Under Secretary for War for Acquisition and Sustainment considered it to be a Department of the Army installation.

[11] ~~(S//NF)~~ The Director of Civil Engineers and AFCEC, [redacted] Expectations & Mitigation Procedures," May 2022. On July 24,2024, A4CIC was renamed from the Air Force Civil Engineers Control Systems team when it was merged with the Air Force Civil Engineers Integration division.

~~(S//NF)~~ initiative for the DAF to AFCEC.[12] Table 1 outlines the roles and responsibilities for mitigating vulnerabilities identified in Section 1650 assessments.

(U) Table 1. DAF Roles and Responsibilities for Mitigating Vulnerabilities Identified During Section 1650 Assessments

~~(S//NF)~~ Organization	Roles and Responsibilities
(U) A4CIC	• (U) Provide guidance on the prioritization of vulnerabilities and potential mitigation actions • (U) Oversee vulnerability mitigation progress • ~~(S//NF)~~ Develop strategy, policy, and processes to address enterprise-wide gaps and vulnerabilities identified by [redacted]
(U) AFCEC	• (U) Perform the Authorizing Official function for the Air Force's Civil Engineer control systems • ~~(S//NF)~~ Track overall installation-level progress and timely completion of [redacted] mitigations • (U) Provide guidance to installation personnel about vulnerability mitigation strategies and facilitate knowledge-sharing across installations • (U) Develop standard operating procedures and guidance for addressing common control system vulnerabilities
(U) Installations	• ~~(S//NF)~~ Determine mitigation strategies for vulnerabilities identified in [redacted] reports • (U) Implement mitigations and determine potential mission impact of specific vulnerabilities if left unmitigated • (U) Report the installation's mitigation progress, status, and roadblocks • (U) Determine whether additional resources are required to mitigate vulnerabilities and build requirements into installation-level budgets • (U) Communicate vulnerability mitigation updates and obstacles to AFCEC and identify solutions to remediate challenges ~~(S//NF)~~

~~(S//NF)~~ Source: The Director of Civil Engineers and AFCEC, [redacted] Expectations and Mitigation Procedures," May 2022.

[12] ~~(S)~~ Department of the Air Force, [redacted] April 8, 2019.

~~(CUI)~~ The DAF Section 1650 assessment reports identified [redacted] cybersecurity vulnerabilities affecting DCI control systems, including [redacted] risk cybersecurity vulnerabilities.[13] See Appendix C for a list of the [redacted] risk cybersecurity vulnerabilities identified at each installation assessed.

(U) What We Reviewed

~~(CUI)~~ We focused on the [redacted] risk vulnerabilities identified during the Section 1650 assessments because of the impact that exploitation or compromise could have on the DAF's ability to conduct critical operations or mission-essential functions. We selected 5 installations that had high and significant risk vulnerabilities based on various factors, including average risk score for the cybersecurity vulnerabilities, proximity to other installations, and the DAF's reported mitigation status of the vulnerabilities.[14]

(U) We selected a statistical sample of cybersecurity vulnerabilities with a mitigation status reported as complete or in progress to review at each installation we visited. In addition, we selected a nonstatistical sample of cybersecurity vulnerabilities with a status reported as other and not started at each installation visited to determine whether the installations miscategorized the vulnerability status and the reason for not taking action to mitigate the vulnerabilities.

[13] ~~(CUI)~~ High-risk vulnerabilities, if exploited, would likely cause strategic mission failure or result in a marginal capability to execute assigned missions. Significant-risk vulnerabilities, if exploited, may significantly degrade strategic mission capability, leaving diminished ability to execute assigned missions. Only 14 DAF Section 1650 assessments included cybersecurity vulnerabilities with other than high or significant risk vulnerabilities. Those reports identified [redacted] that were considered moderate or low risk. Moderate-risk vulnerabilities, if exploited, may degrade mission capability but still allow mission execution. Low-risk vulnerabilities are not expected to impact mission execution.

[14] ~~(CUI)~~ The average risk score of a cybersecurity vulnerability is a calculation based on [redacted] Threat is an [redacted] Vulnerability is [redacted] Criticality is [redacted]

(U) Finding

(U) The Department of the Air Force Must Take Additional Actions to Mitigate Vulnerabilities Identified During Section 1650 Assessments

~~(CUI)~~ The DAF made progress in mitigating vulnerabilities identified during Section 1650 assessments at the five installations we visited, but additional actions are needed. Of the [redacted] risk vulnerabilities we reviewed, DAF officials:

- ~~(CUI)~~ mitigated [redacted] risk) vulnerabilities;
- ~~(CUI)~~ partially mitigated [redacted] risk) vulnerabilities;
- ~~(CUI)~~ had plans in place to mitigate [redacted] risk) vulnerabilities; and
- ~~(CUI)~~ did not take action to mitigate [redacted] risk) vulnerabilities.

(U) Although DAF officials prioritized the identified vulnerabilities, they did not take action to mitigate some vulnerabilities in our sample because all five installations lacked staff with cybersecurity expertise to mitigate the vulnerabilities.

~~(CUI)~~ In addition to the vulnerabilities in our sample, DAF officials stated that they did not take action for [redacted] risk vulnerabilities at other DAF installations. DAF officials did not take action for these vulnerabilities or ensure responsible officials were aware of all vulnerabilities because AFCEC and A4CIC officials misunderstood the scope of the DAF Section 1650 assessments.

(U) These vulnerabilities, if left unmitigated, provide adversaries and malicious actors with opportunities to adversely affect critical missions or functions and the DAF's ability to deploy, support, and sustain military forces worldwide. In addition, DAF officials did not notify most control system owners of identified vulnerabilities that could have been acted upon to reduce the known risks to DCI. Since June 2025, the Federal Bureau of Investigation, National Security Agency, and Cybersecurity and Infrastructure Security Agency have reported that Iranian-affiliated cyber actors and hacktivist groups are aggressively targeting U.S. critical infrastructure, which further emphasizes the DAF's need to take corrective actions to minimize the threat that adversaries and other malicious actors pose to DCI.[15]

[15] (U) Federal Bureau of Investigation, National Security Agency, and Cybersecurity and Infrastructure Security Agency, Joint Statement, "Iranian Cyber Actors May Target Vulnerable US Networks and Entities of Interest," June 30, 2025.

(U) The DAF Made Progress, but Additional Actions Are Needed to Mitigate Cybersecurity Vulnerabilities Impacting DCI

(U) The DAF made progress in mitigating vulnerabilities identified during Section 1650 assessments at the five installations we visited, but additional actions are needed. DoD Manual 8530.01 requires DoW Components to take corrective actions to mitigate vulnerabilities or threats to Component assets, including DCI and their associated control systems. The Manual also requires DoW Components to prioritize actions taken, validate the effectiveness of corrective actions, and track the status of actions to mitigate vulnerabilities in a plan of action and milestones for the asset or capability.[16]

(U) The DAF Supported Actions Taken and Plans to Mitigate Cybersecurity Vulnerabilities

~~(CUI)~~ The DAF supported actions taken or planned to mitigate [redacted] risk vulnerabilities we reviewed at five installations. High-risk vulnerabilities, if exploited, would likely cause strategic mission failure or result in a marginal capability to execute assigned missions. Significant-risk vulnerabilities, if exploited, may significantly degrade strategic mission capability, leaving diminished ability to execute assigned missions. See Appendix D for a summary, by installation visited, of the status of mitigation actions for the [redacted] risk vulnerabilities. Specifically, DAF officials:

- ~~(CUI)~~ mitigated [redacted] risk) vulnerabilities,
- ~~(CUI)~~ partially mitigated [redacted] vulnerabilities, and
- ~~(CUI)~~ had plans in place to mitigate [redacted] vulnerabilities.

~~(S//NF)~~ For example, [redacted] In July 2025, [redacted]

~~(S//NF)~~ In another instance, [redacted] In August 2025, [redacted]

[16] (U) Department of the Air Force Guidance Memorandum 2024-32-01, "Civil Engineer Control Systems Cybersecurity," October 16, 2024. A plan of action and milestones is a document that identifies tasks, resources required to accomplish the elements of the plan, and milestones for meeting the tasks.

~~(S//NF)~~ [redacted]

~~(S//NF)~~ [redacted] We observed that the software was still outdated so the vulnerability was not mitigated; however, [redacted] officials stated that they had a plan in place to address the vulnerability. Specifically, [redacted] officials provided a contract that included services for updating software on the computer attached to the [redacted]

(U) The DAF Did Not Take Action to Mitigate Some Cybersecurity Vulnerabilities

~~(S//NF)~~ Although DAF officials prioritized the vulnerabilities identified during Section 1650 assessments, the DAF did not take action to mitigate [redacted] risk) of the [redacted] risk vulnerabilities we assessed at the five installations visited. For example, at [redacted] In May 2025, we observed that [redacted] [17] Network flow diagrams identify and support troubleshooting network issues, including monitoring communication protocols used by controllers and field devices connected to all control systems. Not knowing all communication protocols used increases the installation's risk of a malicious actor exploiting an unsecure protocol and introducing malware into the network or gaining unauthorized access to the network.

~~(S//NF)~~ In another instance, the [redacted] AFCEC officials categorized this vulnerability as "other" because they stated that the base security forces squadron was responsible for airfield security at the installation. However, AFCEC officials could not demonstrate that they followed up with the security forces squadron about their actions to mitigate the vulnerability. In August 2025, we observed that this vulnerability remained unmitigated. [redacted]

[17] (U) A stand-alone system is a system not connected to any other network and does not transmit, receive, route, or exchange information outside of the system's authorization boundary.

~~(S//NF)~~ Of the [redacted] vulnerabilities, DAF officials categorized [redacted] of them as "other," stating that these vulnerabilities were out of the scope of their responsibilities and assumed the non-AFCEC control systems were reviewed in error. For example, the October 2019 assessment at [redacted] AFCEC officials categorized this vulnerability as "other" because the [redacted] This vulnerability, if exploited, [redacted]

~~(S//NF)~~ In addition to these [redacted] vulnerabilities included in our sample, we learned that the DAF officials also categorized [redacted] more vulnerabilities in a similar manner at other DAF installations where Section 1650 assessments occurred. For example, [redacted] AFCEC officials categorized this vulnerability as "other" [redacted]

(U) Additional Actions Must be Taken to Mitigate All Vulnerabilities Identified During Section 1650 Assessments

(U) The DAF must take additional actions to mitigate all vulnerabilities identified during Section 1650 assessments. DAF officials partially mitigated or did not mitigate vulnerabilities identified during Section 1650 assessments because they lacked staff with cybersecurity expertise or demonstrate that the non-AFCEC organizations were aware of vulnerabilities that affected their assets when AFCEC officials determined that AFCEC did not have responsibility for corrective actions.

(U) The DAF Lacked Staff with Cybersecurity Expertise

~~(S//NF)~~ DAF officials at the five installations visited stated that they did not take action to mitigate some vulnerabilities identified during Section 1650 assessments because they lacked cybersecurity expertise for a variety of reasons, including turnover,

~~(S//NF)~~ vacancies, or inexperienced or unqualified staff at their installations. We identified that all DAF installations visited relied on contractors to mitigate cybersecurity vulnerabilities to cover the needed but missing expertise. The contractors provided engineering and cybersecurity expertise to support AFCEC in managing cyber risk for AFCEC-owned control systems. For example, the [redacted] Civil Engineering Squadron experienced key cybersecurity position on turnover for the Information System Security Manager (ISSM) and Deputy Base Civil Engineer positions. As of July 2025, [redacted] officials appointed a temporary Deputy Base Civil Engineer. However, vacancies and temporary appointments of key cybersecurity officials at [redacted] limited the base's ability to mitigate all control system vulnerabilities in a timely manner. Therefore, the Director of Civil Engineers, in coordination with the Commanders of Air Force Major Commands, should identify solutions to address vacant positions or lacking expertise to mitigate cybersecurity risks and maintain the cybersecurity of control systems for Defense Critical Infrastructure.

~~(S//NF)~~ At [redacted], the Section 1650 assessments identified [redacted] risk vulnerabilities. The ISSM reported that the installation mitigated [redacted] vulnerabilities in our sample, but we verified that the installation mitigated only [redacted] vulnerabilities. The ISSM reported that [redacted] additional vulnerabilities not in our sample from the [redacted] risk vulnerabilities identified during that Section 1650 assessment were also mitigated. [redacted] and we verified that [redacted] vulnerabilities in our sample had not been mitigated despite being reported as such, we question whether all vulnerabilities that the former ISSM was responsible for were effectively mitigated. Therefore, the Base Civil Engineer at [redacted] should validate whether corrective actions taken by the former ISSM for all vulnerabilities identified during Section 1650 assessments were effectively mitigated and take appropriate actions to address any vulnerabilities not mitigated.

(U) DAF Officials Did Not Ensure All Non-AFCEC Asset Owners Were Aware of Vulnerabilities Identified During Section 1650 Assessments

~~(CUI)~~ DAF officials did not mitigate vulnerabilities identified during Section 1650 assessments or coordinate all known vulnerabilities with non-AFCEC asset owners,

~~(CUI)~~ such as the Defense Logistics Agency, Defense Information Systems Agency, and Security Forces Squadron. AFCEC and A4CIC officials misunderstood the scope of the Section 1650 assessments, stating that they assumed the control systems not owned by AFCEC were reviewed in error and should not have been included in the scope of the Section 1650 assessments. When the assessments were completed, DAF officials provided the assessments and plans of action and milestones to the installations. However, AFCEC officials only began notifying most non-AFCEC asset owners of vulnerabilities identified during Section 1650 assessments after we brought the issue to their attention. AFCEC officials provided documentation during the audit supporting that they notified non-AFCEC asset owners about [redacted] vulnerabilities but could not provide support for the remaining [redacted]

(U) Regardless of whether DAF officials considered the vulnerabilities outside the scope of the Section 1650 assessments, DoD Manual 8530.01 requires DoW Components to mitigate identified vulnerabilities. DAF officials were aware that these vulnerabilities existed and did nothing to ensure corrective actions were taken. Therefore, the Director of Civil Engineers, in coordination with A4CIC, AFCEC, Cyber Resiliency Office for Control Systems, DoW Components, and installation officials, should immediately notify non-AFCEC components of the remaining vulnerabilities identified during Section 1650 assessments that affect control systems not under the responsibility of AFCEC. In addition, the Director of Civil Engineers, in coordination with A4CIC, AFCEC, Cyber Resiliency Office for Control Systems, DoW Components, and installation officials, should develop and implement a process to notify and verify that corrective actions were taken to mitigate cybersecurity vulnerabilities affecting assets not owned by AFCEC but that directly impact AFCEC missions and operations.

(U) The Department of the Air Force Took Some Action to Manage Risk Associated with Vulnerabilities Identified During Section 1650 Assessments

(U) In October 2024, the DAF began forming the Cyber Resiliency Office for Control Systems, which is part of A4CIC, with responsibility for technical oversight of control systems cybersecurity and critical infrastructure resiliency.[18] Establishing this office creates a centralized group to support cybersecurity posture improvements by making recommendations to control system plans, policies, processes, and programs and to facilitate information sharing across the Air Force.

~~(CUI)~~ In addition, AFCEC officials also began notifying most non-AFCEC asset owners of vulnerabilities identified during Section 1650 assessments after we brought the issue to

[18] (U) MeriTalk, "Air Force Moving Forward With New Office for Operational Technology Cyber Resiliency," December 3, 2024.

~~(CUI)~~ their attention. AFCEC officials provided documentation supporting that it notified non-AFCEC asset owners about [redacted] vulnerabilities. The newly formed Cyber Resiliency Office for Control Systems would be responsible for verifying that corrective actions were taken to mitigate these vulnerabilities.

(U) Unmitigated Vulnerabilities Identified During Section 1650 Assessments Unnecessarily Increase Risk to Critical Missions or Mission-Essential Functions

~~(CUI)~~ By not mitigating the known cybersecurity vulnerabilities affecting DCI, the DAF unnecessarily increased the risk that its DCI could be degraded, incapacitated, or exploited, resulting in the failure of critical missions or mission-essential functions. Although the DAF completed Section 1650 assessments between July 2019 and September 2021, as of December 2025, the DAF supported that it had taken or was taking corrective actions for [redacted] risk vulnerabilities impacting DCI that we reviewed at the five installations.

~~(S//NF)~~ These vulnerabilities, if left unmitigated, provide adversaries and malicious actors with opportunities to adversely affect critical missions or functions and the DAF's ability to deploy, support, and sustain military forces worldwide. For example, the assessment at [redacted] Outdated operating systems are more susceptible to exploitation by malicious actors who could establish unauthorized access to mission-essential control systems. [redacted]

(U) In a joint statement, the Federal Bureau of Investigation, National Security Agency, and Cybersecurity and Infrastructure Security Agency reported that since June 2025, Iranian-affiliated cyber actors and hacktivist groups have been aggressively targeting U.S. critical infrastructure, which further emphasizes the DAF's need to take corrective actions to minimize the threat that adversaries and other malicious actors pose to DCI. For example, Iranian-affiliated cyber actors target the use of unpatched or outdated software within critical infrastructure components with known common vulnerability exposure.

(U) Management Comments on the Finding and Our Response

(U) The Assistant Deputy Chief of Staff for Logistics, Engineering, and Force Protection, responding for the Director of Civil Engineers, provided comments on the finding

(U) related to communications with non-AFCEC asset owners, the number of Section 1650 assessments conducted, AFCEC and Air Force Major Command responsibilities, and security portion markings.

(U) Our Response

(U) Comments from the Assistant Deputy Chief of Staff on the report were similar to those we already considered when preparing the draft of this report. However, we reviewed information previously received in relation to the comments and updated the report where appropriate. Specifically, we updated the report to show that the DAF conducted 29 Section 1650 assessments and communicated with some non-AFCEC asset owners. We also updated the report to include the Commanders of Air Force Major Commands in one of the recommendations. See the following section for further discussion on the revised recommendation. However, we did not update portion markings in the report because a separate security review of the report by the DAF identified that we had appropriately portioned marked CUI and classified information throughout the report.

(U) Recommendations, Management Comments, and Our Response

(U) Revised Recommendation

(U) As a result of management comments, we included the Commanders of Air Force Major Commands in Recommendation 1 because of their responsibility for manpower-related actions to implement the recommendation.

(U) Recommendation 1

(U) We recommend that the Director of Civil Engineers, in coordination with the Commanders of Air Force Major Commands, identify solutions to address vacant positions or lacking expertise to mitigate cybersecurity risks and maintain the cybersecurity of control systems for Defense Critical Infrastructure.

(U) Director of Civil Engineers Comments

(U) The Assistant Deputy Chief of Staff for Logistics, Engineering, and Force Protection, responding for the Director of Civil Engineers, agreed with the intent of the recommendation, stating that they would recommend that ownership be assigned to each applicable installation and corresponding Air Force Major Command. The Assistant Deputy Chief of Staff stated that the Major Commands, not AFCEC, were responsible for funding or filling vacant positions at installations. The Assistant Deputy Chief of Staff also stated that once the Major Commands filled positions, those personnel would be trained. The Assistant Deputy Chief of Staff stated that the actions would be completed by November 30, 2026.

(U) Our Response

(U) Comments from the Assistant Deputy Chief of Staff addressed all specifics of the recommendation; therefore, it is resolved but will remain open. Based on the Assistant Deputy Chief of Staff's comments, we revised the recommendation to include the Commanders of Air Force Major Commands in the process. We will close the recommendation once the Director of Civil Engineers provides documentation validating that the Major Commands addressed their staffing and training needs.

(U) Recommendation 2

~~(S//NF)~~ We recommend that the Base Civil Engineer at [redacted] validate whether corrective actions taken by the former Information System Security Manager for all vulnerabilities identified during Section 1650 assessments were effectively mitigated and take appropriate actions to address any vulnerabilities not mitigated.

(U) Director of Civil Engineers Comments

~~(S//NF)~~ The Assistant Deputy Chief of Staff for Logistics, Engineering, and Force Protection, responding for the Director of Civil Engineers, agreed with the recommendation, stating that A4CIC, in coordination with AFCEC, would work with [redacted] to validate the effectiveness of corrective actions taken by the former ISSM for vulnerabilities identified during the assessment. The Assistant Deputy Chief of Staff stated that the actions would be completed by September 30, 2026.

(U) Our Response

(U) Comments from the Assistant Deputy Chief of Staff addressed the specifics of the recommendations; therefore, it is resolved but will remain open. We will close the recommendation once the Director of Civil Engineers provides documentation showing it completed its review, and based on its review, took action or documented actions to be taken to mitigate any unmitigated vulnerabilities.

(U) Recommendation 3

(U) We recommend that the Director of Civil Engineers, in coordination with Air Force Civil Engineers Cyber Integration, Air Force Civil Engineer Center, Cyber Resiliency Office for Control Systems, DoW Components, and installation officials as appropriate:

a. **(U) Immediately notify non-AFCEC components of the remaining vulnerabilities identified during Section 1650 assessments that affect control systems not under the responsibility of AFCEC.**

(U) Director of Civil Engineers Comments

(U) The Assistant Deputy Chief of Staff for Logistics, Engineering, and Force Protection, responding for the Director of Civil Engineers, agreed with the recommendation, stating that A4CIC was working with AFCEC and installation officials to develop a process to notify non-AFCEC components of vulnerabilities under their purview. The Assistant Deputy Chief of Staff stated that the actions would be completed by December 31, 2026.

(U) Our Response

(U) Comments from the Assistant Deputy Chief of Staff addressed all specifics of the recommendation; therefore, it is resolved but will remain open. We will close the recommendation once the Director of Civil Engineers provides the approved process for notifying non-AFCEC owners of assets with vulnerabilities and documentation that it notified those asset owners.

b. (U) Develop and implement a process to notify and verify that corrective actions were taken to mitigate cybersecurity vulnerabilities affecting assets not owned by the Air Force Civil Engineer Center but that directly impact its missions and operations.

(U) Director of Civil Engineers Comments

(U) The Assistant Deputy Chief of Staff for Logistics, Engineering, and Force Protection, responding for the Director of Civil Engineers, agreed with the recommendation, stating that A4CIC would develop a process to verify that DAF operational technology not owned by AFCEC but that directly impacted AFCEC missions and operations were mitigated. The Assistant Deputy Chief of Staff stated that actions would be completed by December 31, 2026.

(U) Our Response

(U) Comments from the Assistant Deputy Chief of Staff addressed all specifics of the recommendation; therefore, it is resolved but will remain open. We will close the recommendation once the Director of Civil Engineers provides the approved process and verifies that corrective actions were implemented to mitigate the vulnerabilities affecting assets not owned by AFCEC.

(U) Appendix A

(U) Scope and Methodology

(U) We conducted this performance audit from February 2025 through January 2026 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.

(U) This report was reviewed by the DoW Components associated with this oversight project to identify whether any of their reported information, including legacy FOUO information, should be safeguarded and marked in accordance with the DoW CUI Program. In preparing and marking this report, we considered any comments submitted by the DoW Components about the CUI treatment of their information. If the DoW Components failed to provide any or sufficient comments about the CUI treatment of their information, we marked the report based on our assessment of the available information.

~~(CUI)~~ We analyzed 28 of the 29 DAF Section 1650 assessment reports and associated recommendations for corrective actions to identify the types of cybersecurity vulnerabilities identified during the assessments. The reports included [redacted] cybersecurity vulnerabilities affecting DCI control systems; [redacted] risk vulnerabilities that, if exploited or compromised, could adversely impact the DAF's ability to conduct mission critical operations or perform mission-essential functions.

~~(CUI)~~ We selected five Air Force installations to review the DAF's actions taken in mitigating a statistical sample of [redacted] risk cybersecurity vulnerabilities identified during Section 1650 assessments. In addition, we selected a nonstatistical sample of [redacted] at the five sites visited that were reported as "other" and "not started" or where the DAF reported that mitigation actions had not been taken. The installations selected were based on various factors, including average risk score for the cybersecurity vulnerabilities, proximity to other installations, reported mitigation status of the vulnerabilities, and the types of services at the base. We excluded installations where the Air Force Audit Agency conducted audits related to vulnerabilities affecting civil engineering control systems.

(U) To determine responsibilities for mitigating control system cybersecurity vulnerabilities, we interviewed personnel from offices that provided oversight, policies, and subject matter experts from the:

- (U) DAF Principal Cyber Adviser;
- (U) Defense Logistics Agency;
- (U) AFCEC;
- (U) A4CIC;
- (U) Cyber Resiliency Office for Control Systems; and
- (U) Office of the Under Secretary of War for Acquisition and Sustainment.

~~(S//NF)~~ We conducted site visits at [redacted] We met with and obtained information from ISSMs, Civil Engineers, Field Service Representatives, and other officials responsible for the facilities, assets that the control systems operated or monitored, and cybersecurity to determine actions taken or planned to mitigate the vulnerabilities. We validated DAF reported actions for the [redacted] risk vulnerabilities we reviewed based on interviews we held, documentation we reviewed, walkthroughs we conducted, and observations we made.

(U) We reviewed the following Federal, DoW, and Air Force criteria.

- (U) Public Law 114-328, NDAA for FY 2017, December 23, 2016
- (U) National Security Memorandum 22, "The National Security Memorandum on Critical Infrastructure Security and Resilience," April 30, 2024
- (U) DoD Directive 3020.40, "Mission Assurance," November 29, 2016 (Incorporating Change 1, September 11, 2018)
- (U) DoD Instruction 3020.45, "Mission Assurance Construct," August 14, 2018 (Incorporating Change 1, May 2, 2022)
- (U) DoD Instruction 8531.01, "Vulnerability Management," September 15, 2020
- (U) Department of the Air Force Guidance Memorandum, "Civil Engineer Control Systems Cybersecurity," October 16, 2024

(U) Internal Control Assessment and Compliance

(U) We assessed internal controls and compliance with laws and regulations necessary to satisfy the audit objective. In particular, we assessed the internal control components and underlying principles for mitigating the cybersecurity vulnerabilities identified in the Section 1650 assessments. However, because our review was limited to these internal control components and underlying principles, it may not have disclosed all internal control deficiencies that may have existed at the time of this audit.

(U) Use of Computer-Processed Data

(U) We obtained and analyzed computer-processed data from scanning tools and task management systems used by the DAF. Specifically, we were provided Assured Compliance Assessment Solution scan results in Microsoft Excel for the cybersecurity vulnerabilities identified during the Section 1650 assessments.[19] To determine the reliability of the data, we interviewed the DAF officials responsible for the scans, discussed the results during meetings and walkthroughs, and reviewed standard operating procedures for using the tools. Based on our reviews of the results and verification of the tools used by the DAF, we considered the information to be sufficiently reliable for the purpose of our audit.

(U) Use of Technical Assistance

~~(CUI)~~ The DoW Office of Inspector General (DoW OIG) Data Services Directorate provided assistance in developing a stratified attribute simple random sample design to obtain a sample size of [redacted] risk vulnerabilities to review. We selected a nonstatistical sample for [redacted] additional vulnerabilities from the vulnerabilities that were reported as "other" or for which installations reported that mitigation actions had not been taken.

(U) Prior Coverage

(U) During the last 5 years, the DoW OIG, Government Accountability Office (GAO), Army Audit Agency, Naval Audit Service, and Air Force Audit Agency issued six reports discussing cybersecurity vulnerabilities impacting DCI.

[19] (U) Assured Compliance Assessment Solution is a program that the Defense Information System Agency uses to assess DoW networks and information technology systems.

(U) Unrestricted DoW OIG reports can be accessed at https://www.dodig.mil. Unrestricted GAO reports can be accessed at http://www.gao.gov. Army Audit Agency, Naval Audit Service, and Air Force Audit Agency reports are not available over the Internet.

(U) DoW OIG

(U) Report No. DODIG-2025-071, "Audit of Cyber Vulnerabilities Impacting Defense Critical Infrastructure," February 21, 2025

~~(CUI)~~ The DoD OIG determined that the Department of the Navy made minimal progress in mitigating the [redacted] identified during its Section 1650 assessments. Specifically, the Department of the Navy mitigated only [redacted] Department of the Navy officials:

- ~~(CUI)~~ could not provide documentation to support actions that they stated they took to [redacted];
- ~~(CUI)~~ could not produce documentation, such as implementation plans or requests for funding, to support plans they stated were developed [redacted]; and
- ~~(CUI)~~ did not know the status of [redacted].

(U) The DoD OIG recommended that the Department of the Navy develop and implement processes that establish asset and control system ownership, define responsibilities for managing cybersecurity risks, establish expectations for mitigating the unmitigated cybersecurity vulnerabilities identified during the Section 1650 assessments, and hold Navy officials and system owners accountable for not taking corrective action.

(U) GAO

(U) Report No. GAO-23-105468, "Critical Infrastructure Protection: National Cybersecurity Strategy Needs to Address Information Sharing Performance Measures and Methods," September 2023

(U) The GAO determined that 14 assessed sector risk management agencies reported relying on 11 methods to facilitate sharing of cyber threat information with critical infrastructure owners and operators. The GAO found six challenges to effectively sharing cyber threat information. Thirteen of the 14 Federal agencies reported that they took initial actions to address these threats. The GAO determined the weaknesses in identifying outcome-oriented performance measures and assessing whether existing processes are optimal for addressing

(U) challenges. The GAO made two recommendations to the Office of the National Cyber Director and the Cybersecurity and Infrastructure Security Agency. The Office of the National Cyber Director disagreed with the recommendation whereas the Department of Homeland Security agreed with it.

(U) Report No. GAO-22-105103, "Critical Infrastructure Protection: Agencies Need to Assess Adoption of Cybersecurity Guidance," February 2022

(U) The GAO determined that sector risk management agencies for 3 of the 16 critical infrastructure sectors decided to use the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity. Federal agencies with a lead role in protecting one or more of the 16 critical infrastructure sectors are referred to as sector risk management agencies. For the remaining 13 sectors, the GAO determined that lead agencies for 4 of the sectors had taken initial steps to adopt the framework while lead agencies for 9 of the sectors had not. The GAO recommended that the nine sector risk management agency leads develop methods for determining the level and type of framework adoption by entities across their respective sectors and collect and report sector-wide improvements. Five of the risk management agency sector leads agreed with the recommendations while four neither agreed nor disagreed with the recommendations.

(U) Army

(U) Report No. A-2025-0012-FMZ, "Audit of Cyber Vulnerabilities and Resilience of Infrastructure," December 18, 2024

~~(S//NF)~~ [redacted] The Army Audit Agency made four recommendations, including establishing an enduring cyber vulnerability assessment program to identify and mitigate cyber vulnerabilities, developing and implementing a prioritized plan to mitigate open cyber vulnerabilities, and establishing a comprehensive, centralized system to track the remediation status of vulnerabilities.

(U) Navy

(U) Report No. N2023-009, "Naval Facilities Engineering Systems Command's Facility Related Control Systems for Defense Critical Infrastructure," March 20, 2023

~~(CUI)~~ [redacted]

~~(CUI)~~ [redacted]

(U) Air Force

(U) Report No. F2023-0007-O1000, "Audit of Civil Engineer Control Systems Cyber Hygiene," February 1, 2023

(U) The Air Force Audit Agency determined that DAF officials did not maintain physical and logical access to control systems components; properly secure master versions of control systems resources; utilize the most current version of vulnerability scanning tools; prepare and test required response, recover, and contingency plans; perform operating system updates necessary to mitigate vulnerabilities; and update the Enterprise Mission Assurance Support Service with required system documentation. Although the audit did not identify any instances of adversarial access, diversion, intercept of sensitive information, or denial of service attacks, effective cyber hygiene practice helps to protect control systems against unauthorized access that could potentially damage critical DAF systems.

(U) The Air Force Audit Agency made four recommendations to improve civil engineer control systems cyber hygiene, including establishing and implementing a process to monitor civil engineer control systems cybersecurity training requirements; establishing and implementing a method to notify users when updated scan tools are available; and establishing and implementing a process to periodically monitor a sample of the cyber hygiene documentation uploaded for accuracy and completeness.

(U) Appendix B

(U) Conducted Section 1650 Assessments at Department of the Air Force Installations

~~(S//NF)~~ As identified in the DoD response plan and associated Joint Staff prioritized list of critical infrastructure, the DAF conducted assessments at those 28 installations and [redacted] bringing the number of assessments to 29. Table 2 lists the installations where the DAF conducted Section 1650 assessments and the date of the assessment report.

(U) Table 2. Installations Where DAF Conducted Section 1650 Assessments

~~(S//NF)~~ Installation	Report Date
[redacted]	January 28, 2020
[redacted]	December 13, 2019
[redacted]	May 31, 2021
[redacted]*	October 09, 2019
[redacted]	February 4, 2020
[redacted]	July 24, 2020
[redacted]	September 19, 2019
[redacted]	October 22, 2019
[redacted]	June 30, 2020
[redacted]	March 13, 2020
[redacted]	September 19, 2019
[redacted]	February 28, 2020
[redacted]	August 12, 2019
[redacted]	January 10, 2020
[redacted]	January 24, 2020 ~~(S//NF)~~

(U) Table 2. Installations Where DAF Conducted Section 1650 Assessments (cont'd)

~~(S//NF)~~ Installation	Report Date
[redacted]	March 13, 2020
[redacted]	July 6, 2020
[redacted]	March 13, 2020
[redacted]	August 14, 2020
[redacted]	January 24, 2020
[redacted]	November 11, 2019
[redacted]	May 28, 2020
[redacted]	July 25, 2019
[redacted]	March 13, 2020
[redacted]	August 15, 2019
[redacted]	March 13, 2020
[redacted]	March 13, 2020
[redacted]	March 6, 2020
[redacted]	June 10, 2020 ~~(S//NF)~~

* (U) On September 27, 2021, the DAF conducted a second assessment at this location.

(U) Source: The DoW OIG.

(U) Appendix C

(U) High and Significant Risk Cybersecurity Vulnerabilities at Department of the Air Force Installations

~~(CUI)~~ The DAF Section 1650 assessment reports identified [redacted] cybersecurity vulnerabilities on DCI controls systems at the 28 installations assessed. Table 3 identifies the number of high and significant risk cybersecurity vulnerabilities, by installation, identified in DAF Section 1650 assessment reports.

(U) Table 3. High and Significant Risk Cybersecurity Vulnerabilities by Installation

~~(S//NF)~~ Installation	Number of High-Risk Vulnerabilities Identified During Section 1650 Assessments	Number of Significant-Risk Vulnerabilities Identified During Section 1650 Assessments
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted] ~~(S//NF)~~

(U) Table 3. High and Significant Risk Cybersecurity Vulnerabilities by Installation (cont'd)

~~(S//NF)~~ Installation	Number of High-Risk Vulnerabilities Identified During Section 1650 Assessments	Number of Significant-Risk Vulnerabilities Identified During Section 1650 Assessments
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
Total	[redacted]	[redacted] ~~(S//NF)~~

* ~~(S//NF)~~ We did not include [redacted] in our assessment; therefore, the vulnerabilities from that assessment are not included in our totals.

(U) Source: The DoW OIG.

(U) Appendix D

(U) Mitigation Status of High and Significant Risk Sampled Vulnerabilities

~~(CUI)~~ We reviewed [redacted] risk vulnerabilities of the [redacted] identified in Section 1650 assessments at the five installations visited. Table 4 identifies the status of the [redacted] risk vulnerabilities, by installation, based on our analysis of documentation reviewed and our observations.

(U) Table 4. Mitigation Status of Sampled High and Significant Risk Vulnerabilities by Installation

~~(S//NF)~~ Installation	Mitigated	Partially Mitigated	Unmitigated	Planned
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Total	[redacted]	[redacted]	[redacted]	[redacted] ~~(S//NF)~~

* ~~(S//NF)~~ Of the [redacted] vulnerabilities unmitigated at the time of our audit, DAF officials explained that [redacted] vulnerabilities were not AFCEC responsibilities.

(U) Source: The DoW OIG.

(U) Appendix E

(U) Sources of Classified Information

(U) Source 1: ~~**(S//NF)**~~ [redacted] (SECRET//NOFORN)
Declassification Date: October 22, 2044
Date of Source: October 22, 2019

(U) Source 2: ~~**(S//NF)**~~ [redacted] (SECRET//NOFORN)
Declassification Date: July 2, 2045
Date of Source: June 30, 2020

(U) Source 3: ~~**(S//NF)**~~ [redacted] (SECRET//NOFORN)
Declassification Date: July 1, 2044
Date of Source: March 13, 2020

(U) Source 4: ~~**(S//NF)**~~ [redacted] (SECRET//NOFORN)
Declassification Date: March 1, 2045
Date of Source: September 19, 2019

(U) Source 5: ~~**(S//NF)**~~ [redacted] (SECRET//NOFORN)
Declassification Date: August 1, 2045
Date of Source: February 28, 2020

(U) Source 6: ~~**(S//NF)**~~ [redacted]
(SECRET//NOFORN)
Declassification Date: July 1, 2044
Date of Source: August 12, 2019

(U) Source 7: ~~**(S//NF)**~~ [redacted] (SECRET//NOFORN)
Declassification Date: January 1, 2045
Date of Source: January 10, 2020

(U) Source 8: **~~(S//NF)~~** [redacted] (SECRET//NOFORN)
Declassification Date: October 1, 2044
Date of Source: January 24, 2020

(U) Source 9: **~~(S//NF)~~** [redacted] (SECRET//NOFORN)
Declassification Date: July 1, 2044
Date of Source: March 13, 2020

(U) Source 10: **~~(S//NF)~~** [redacted] (SECRET//NOFORN)
Declassification Date: July 2, 2045
Date of Source: July 6, 2020

(U) Source 11: **~~(S//NF)~~** [redacted]
(SECRET//NOFORN)
Declassification Date: September 1, 2045
Date of Source: January 28, 2020

(U) Source 12: **~~(S//NF)~~** [redacted] (SECRET//NOFORN)
Declassification Date: September 1, 2045
Date of Source: March 13, 2020

(U) Source 13: **~~(S//NF)~~** [redacted] (SECRET//NOFORN)
Declassification Date: March 1, 2045
Date of Source: December 13, 2019

(U) Source 14: **~~(S//NF)~~** [redacted] (SECRET//NOFORN)
Declassification Date: January 24, 2045
Date of Source: January 24, 2020

(U) Source 15: **~~(S//NF)~~** [redacted] (SECRET//NOFORN)
Declassification Date: March 1, 2045
Date of Source: November 11, 2019

(U) Source 16: **~~(S//NF)~~** [redacted] (SECRET//NOFORN)
Declassification Date: June 15, 2045
Date of Source: May 28, 2020

(U) Source 17: **~~(S//NF)~~** [redacted] (SECRET//NOFORN)
Declassification Date: May 31, 2046
Date of Source: May 31, 2021

(U) Source 18: **~~(S//NF)~~** [redacted] (SECRET//NOFORN)
Declassification Date: October 1, 2044
Date of Source: October 9, 2019

(U) Source 19: **~~(S//NF)~~** [redacted] (SECRET//NOFORN)
Declassification Date: August 1, 2046
Date of Source: September 27, 2021

(U) Source 20: **~~(S//NF)~~** [redacted] (SECRET//NOFORN)
Declassification Date: February 1, 2045
Date of Source: April 25, 2019

(U) Source 21: **~~(S//NF)~~** [redacted] (SECRET//NOFORN)
Declassification Date: February 1, 2045
Date of Source: February 4, 2020

(U) Source 22: **~~(S//NF)~~** [redacted] (SECRET//NOFORN)
Declassification Date: March 1, 2045
Date of Source: August 15, 2019

(U) Source 23: **~~(S//NF)~~** [redacted] (SECRET//NOFORN)
Declassification Date: March 1, 2045
Date of Source: March 13, 2020

(U) Source 24: ~~**(S//NF)**~~ [redacted] (SECRET//NOFORN)
Declassification Date: March 13, 2045
Date of Source: March 13, 2020

(U) Source 25: ~~**(S//NF)**~~ [redacted] (SECRET//NOFORN)
Declassification Date: May 1, 2045
Date of Source: June 24, 2020

(U) Source 26: ~~**(S//NF)**~~ [redacted] (SECRET//NOFORN)
Declassification Date: January 1, 2045
Date of Source: September 19, 2019

(U) Source 27: ~~**(S//NF)**~~ [redacted] (SECRET//NOFORN)
Declassification Date: July 1, 2044
Date of Source: March 13, 2020

(U) Source 28: ~~**(S//NF)**~~ [redacted] (SECRET//NOFORN)
Declassification Date: September 1, 2045
Date of Source: March 6, 2020

(U) Source 29: ~~**(S//NF)**~~ [redacted] (SECRET//NOFORN)
Declassification Date: June 1, 2045
Date of Source: June 10, 2020

(U) Source 30: ~~**(S//NF)**~~ [redacted] (SECRET//NOFORN)
Declassification Date: February 7, 2050
Date of Source: February 7, 2025

(U) Source 31: ~~**(S//NF)**~~ [redacted] (SECRET)
Declassification Date: July 2044
Date of Source: July 2019

(U) Management Comments

(U) Air Force, Director of Civil Engineers

~~SECRET//NOFORN~~

DEPARTMENT OF THE AIR FORCE
HEADQUARTERS UNITED STATES AIR FORCE
WASHINGTON, D.C.

13 Apr 2026

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL

FROM: HQ USAF/A4
1120 Air Force Pentagon Suite 4E154
Washington, DC 20330

SUBJECT: Department of the Air Force Response to DoD Office of Inspector General Draft Report, "Audit of Cyber Vulnerabilities Impacting Department of the Air Force Defense Critical Infrastructure" (D2025-D000CS-0081.000).

1. This is the Department of the Air Force response to the DoDIG Draft Report, "Audit of Cyber Vulnerabilities Impacting Department of the Air Force Defense Critical Infrastructure" (Project No. D2025-D000CS-0081.000). The DAF agrees with the intent of the report as written and welcomes the opportunity to review and provide feedback.

2. AF/A4, in coordination Air Force Civil Engineer Center (AFCEC) and MAJCOMs, will correct issues identified in the report and develop, and implement, a corrective action plan outlined in the following recommendations:

(U) RECOMMENDATION 1: The DODIG recommends the Air Force Civil Engineer Center (AFCEC) Director identify solutions to address vacant positions or lacking expertise to mitigate cybersecurity risks and maintain the cybersecurity of control systems for Defense Critical Infrastructure.

(U) DAF RESPONSE: The DAF agrees with the intent of the recommendation and will recommend ownership be placed with each installation and corresponding MAJCOM respectively. AFCEC is not responsible for funding or filling vacant positions within each squadron at the installation level. MAJCOMs are responsible for manpower determinations and funding vacant positions. Once positions are filled, appropriate training will be provided to ensure the appropriate level of expertise.

(U) Estimated Completion Date: 30 Nov 2026

~~(S_NF)~~ RECOMMENDATION 2: The DODIG recommends the Base Civil Engineer (BCE) at [redacted] validate whether corrective actions taken by the former Information System Security Manager (ISSM) for all vulnerabilities identified during Section 1650 assessments were effectively mitigated and appropriate actions were taken to address any vulnerabilities not mitigated.

~~(S_NF)~~ DAF RESPONSE: The DAF agrees with the recommendation. AF/A4, in coordination with AFCEC, will work with [redacted] to validate whether corrective

~~SECRET//NOFORN~~

(U) Air Force, Director of Civil Engineers (cont'd)

~~SECRET//NOFORN~~

2

actions taken by the former ISSM for vulnerabilities identified during the assessment effectively mitigated those vulnerabilities and if any additional actions were required as a result.

(U) Estimated completion date: 30 Sept 2026

(U) RECOMMENDATION 3: The DODIG recommends the Director of Civil Engineers, in coordination with Air Force Civil Engineers Cyber Integration, AFCEC, DAF CROCS, DoD Components, and installation officials as appropriate:

a. (U) Immediately notify non-AFCEC components of remaining vulnerabilities identified during Section 1650 assessments that affect control systems not under the responsibility of AFCEC.

b. (U) Develop and implement a process to notify and verify corrective actions were taken to mitigate cybersecurity vulnerabilities affecting assets not owned by AFCEC but directly impact its missions and operations

(U) DAF RESPONSE: The DAF agrees with the recommendation.

a. (U) AF/A4, in coordination with AFCEC and installation officials, are developing a process to notify non-AFCEC components of vulnerabilities within their respective boundaries.

b. (U) AF/A4 will develop a process to verify completion of identified vulnerabilities outside of AFCEC's boundary related to DAF operational technology (OT).

(U) Estimated Completion Date: 31 Dec 2026

3. The AF/A4 point of contact is [redacted] AF/A4 CROCS, [redacted] or via email at [redacted]

BAITY.ANTHONY.RAY.[redacted]

ANTHONY R. BAITY, SES, DAF
Asst DCS/Logistics, Engineering & Force Protection

~~SECRET//NOFORN~~

(U) Air Force, Director of Civil Engineers (cont'd)

Final Report Reference

Revised- Page 7

~~SECRET//NOFORN~~

CONSOLIDATED DoD ISSUANCE COMMENT MATRIX

Issuance Type and Number, "Title"

CLASS	#	PAGE	PARA	BASIS FOR NON-CONCUR?	COMMENTS, JUSTIFICATION, AND ORIGINATOR JUSTIFICATION FOR RESOLUTION	COMPONENT AND POC NAME, PHONE, AND E-MAIL
~~CUI~~	1	7	2	☐	**Coordinator Comment and Justification**: This statement is misleading because it leads the reader to believe that no actions have been taken to mitigate the risk of these vulnerabilities and that a lack of cyber expertise was the only rationale. There's a variety of reasons vulnerabilities may not have been mitigated including technical feasibility issues, costly mitigations, involve systems outside CE's authority to address, etc. that would limit the type of actions taken to mitigate the vulnerabilities. Where possible, additional controls were put in place to lower the risk for instances where mitigation actions could not be taken within CE's control. **Coordinator Recommended Change**: Change: "Although DAF officials prioritized the identified vulnerabilities, they did not take action to mitigate vulnerabilities in our sample because all five installations lacked staff with cybersecurity expertise to mitigate the vulnerabilities. " To: "Although DAF officials prioritized the identified vulnerabilities, they did not take action to mitigate some vulnerabilities in our sample. Reasons to include: installations lacked funding, staff with cybersecurity expertise, and/or incurred technological issues, and certain systems were outside CE's authority. Where possible, compensating control were added to bring down the risk of unmitigated vulnerabilities." **Originator Response**: Choose an item. **Originator Reasoning**:	[redacted]
~~CUI~~	2	7	3	☐	**Coordinator Comment and Justification**: AFCEC did send notifications to entities outside CE's boundary to pass along vulnerabilities. Not all transfers of vulnerabilities had available documentation at the time of the audit.	[redacted]

DD FORM 818-1, AUG 2016 **SELECT A CLASSIFICATION** 1

(U) Air Force, Director of Civil Engineers (cont'd)

~~SECRET//NOFORN~~

CONSOLIDATED DoD ISSUANCE COMMENT MATRIX

Issuance Type and Number, "Title"

CLASS	#	PAGE	PARA	BASIS FOR NON-CONCUR?	COMMENTS, JUSTIFICATION, AND ORIGINATOR JUSTIFICATION FOR RESOLUTION	COMPONENT AND POC NAME, PHONE, AND E-MAIL
					A4C also presented email evidence showing entities outside CE's boundary did receive the S. 1650 reports at the time they were completed. The distro list for these reports included Wing Commanders, Base Civil Engineers (BCEs), Mission Assurance Group Commanders, etc. who received the reports and associated POA&Ms. **Coordinator Recommended Change**: Change: DAF officials did not take action for these vulnerabilities or ensure responsible officials were aware of the vulnerabilities because they misunderstood the scope of the DAF Section 1650 assess To: DAF officials took some actions to address these vulnerabilities by establishing a process for AFCEC to inform DAF officials outside of CE's boundary of their vulnerabilities. Documentation for this was not always available. AF/A4C sent initial reports and POA&Ms at the time of completion to Wing Commanders, Mission Support Group Commanders, and the Base Civil Engineer (BCE) at each installation. **Originator Response**: Choose an item. **Originator Reasoning**:	
~~CUI~~	3	9	3	☐	**Coordinator Comment and Justification**: It would be helpful to see the [redacted] POA&M IDs that align to the vulnerabilities the audit deemed unmitigated. It would also be helpful to see a breakout of those POA&Ms that are inside CE's boundary vs outside. The way it is being reported may misrepresent the work CE has completed.	[redacted]

DD FORM 818-1, AUG 2016 SELECT A CLASSIFICATION 2

(U) Air Force, Director of Civil Engineers (cont'd)

~~SECRET//NOFORN~~

CONSOLIDATED DoD ISSUANCE COMMENT MATRIX

Issuance Type and Number, "Title"

CLASS	#	PAGE	PARA	BASIS FOR NON-CONCUR?	COMMENTS, JUSTIFICATION, AND ORIGINATOR JUSTIFICATION FOR RESOLUTION	COMPONENT AND POC NAME, PHONE, AND E-MAIL
					Coordinator Recommended Change: Provide documentation showing which POA&Ms were still unmitigated at the time of the audit that make up the [redacted] listed in this paragraph, as well as on page 7, para 1. **Originator Response**: Choose an item. **Originator Reasoning**:	
~~CUI~~	4	7 & 12	3 & 1	☐	**Coordinator Comment and Justification**: DAF did not think non-AFCEC control systems were reviewed in error, the assessments were initially handed to A4C, after coming down from Congress, which only had the authority to assess CE control systems (not Security Forces, DLA, private companies, etc.) **Coordinator Recommended Change**: Change: "DAF officials misunderstood the scope of the DAF Section 1650 assessments, stating that they assumed the control systems not owned by AFCEC were reviewed in error and should not have been included in the scope of the Section 1650 assessments." To: "DAF officials did not cover all DAF operational technology (OT). AF/A4C lead the assessment effort. AF/A4C only has authority over Civil Engineer-owned systems." **Originator Response**: Choose an item. **Originator Reasoning**:	[redacted]
~~CUI~~	5	Pg. 11	Para. 1	☐	**Coordinator Comment and Justification**: CE personnel are inherently engineers first. They are not intended to be cybersecurity SMEs. However, CE partners with cyber entities such as 16th AF, Cybersecurity Service Providers (CSSPs), CROCS, AFCEC and contractors to gain necessary cyber expertise	[redacted]

DD FORM 818-1, AUG 2016 SELECT A CLASSIFICATION 3

Final Report Reference

Revised- Page 11

(U) Air Force, Director of Civil Engineers (cont'd)

Final Report Reference

~~SECRET//NOFORN~~

CONSOLIDATED DoD ISSUANCE COMMENT MATRIX

Issuance Type and Number, "Title"

CLASS	#	PAGE	PARA	BASIS FOR NON-CONCUR?	COMMENTS, JUSTIFICATION, AND ORIGINATOR JUSTIFICATION FOR RESOLUTION	COMPONENT AND POC NAME, PHONE, AND E-MAIL
					where applicable. Additionally, each installation has an ISSM and cyber contractors to assist in cyber related matters. However, it is the MAJCOM's responsibilities to fill vacant positions within the CE Squadron. AFCEC's only oversight is of their [redacted] which provide boots on the ground SMEs at each installation. **Coordinator Recommended Change**: Change: Therefore, the AFCEC Director should identify solutions to address vacant positions or lacking expertise to mitigate cybersecurity risks and maintain the cybersecurity of control systems for Defense Critical Infrastructure. (Recommendation 1) To: Therefore, installations, and ultimately the MAJCOMs should identify solutions to address vacant positions or lacking expertise to mitigate cybersecurity risks and maintain the cybersecurity of control systems for Defense Critical Infrastructure. The AFCEC Commander should ensure any contractual support under their cyber contract is staffed appropriately. (Recommendation 1) **Originator Response**: Choose an item. **Originator Reasoning**:	
~~CUI~~	6	Multiple		☐	**Coordinator Comment and Justification**: The CROCS is incorrectly titled the "Cyber **Resilience** Office **of** Control Systems" at least five times in the report. **Coordinator Recommended Change**: Change all references to be the correct name of, "Cyber **Resiliency** Office **for** Control Systems." **Originator Response**: Choose an item. **Originator Reasoning**:	[redacted]

DD FORM 818-1, AUG 2016 **SELECT A CLASSIFICATION** 4

Revised Pages 12, 13, 15, and 18

(U) Air Force, Director of Civil Engineers (cont'd)

Final Report Reference

~~SECRET//NOFORN~~

CONSOLIDATED DoD ISSUANCE COMMENT MATRIX

Issuance Type and Number, "Title"

CLASS	#	PAGE	PARA	BASIS FOR NON-CONCUR?	COMMENTS, JUSTIFICATION, AND ORIGINATOR JUSTIFICATION FOR RESOLUTION	COMPONENT AND POC NAME, PHONE, AND E-MAIL
~~SAP~~	7	4, 6, 15, 21, 23		☐	**Coordinator Comment and Justification**: The sentence, "The National Security Agency Platform Resiliency and Mission Assurance Team completed Section 1650 assessments at **28** installations…" is incorrect, as is footnote 9: "Our review did not include the assessment of [redacted] because it is a Department of the Army installation." **Coordinator Recommended Change**: Change the first sentence to read "… Section 1650 assessments at **29** installations…" and **remove footnote 9**. [redacted] with the lead Service being Dept of Air Force, not Army. Similarly on page 6: change, "We selected 5 of **28**…" to "We selected 5 of **29**…" And the same for the references on pages 15, 21, and 23. The very first reference, "The Joint Staff list identified 64 installations… 28 Air Force…" is valid and can remain 28. As we explained in person, the DAF choose to assess an additional 29th installation above and beyond the 28 identified by Joint Staff. **Originator Response**: Choose an item. **Originator Reasoning**:	[redacted]
~~SAP~~	8	Multi ple		☐	**Coordinator Comment and Justification**: The terms [redacted] and [redacted] are not classified by themselves, as is indicated throughout the report, such as the three areas in Table 1 and the Acronyms and Abbreviations section. As documented on the S.1650 SharePoint site, "For the purposes of facilitating interaction with the bases at an unclassified level, the Air Force has [redacted]	[redacted]

DD FORM 818-1, AUG 2016 SELECT A CLASSIFICATION 5

Revised Pages 4, 14, 17, 23

(U) Air Force, Director of Civil Engineers (cont'd)

Final Report Reference

~~SECRET//NOFORN~~

CONSOLIDATED DoD ISSUANCE COMMENT MATRIX

Issuance Type and Number, "Title"

CLASS	#	PAGE	PARA	BASIS FOR NON-CONCUR?	COMMENTS, JUSTIFICATION, AND ORIGINATOR JUSTIFICATION FOR RESOLUTION	COMPONENT AND POC NAME, PHONE, AND E-MAIL
					Coordinator Recommended Change: You can technically drop the classified portion markings for the [redacted] sentences in Table 1 and the Acronyms and Abbreviations section, provided that somewhere else in the report you note that it's the association of [redacted] that is classified. **Originator Response**: Choose an item. **Originator Reasoning**:	
~~CUI~~	9	9		☐	**Coordinator Comment and Justification**: The statement, "However, AFCEC officials could not demonstrate that they notified the security force about the vulnerability." is not completely accurate. During the DoD IG's visit to A4C, we provided the audit team with the 10 Feb 2021 communication from AF/A4C-2 to the [redacted] Wing Commander, [redacted] Mission Support Group Commander (who oversees Security Forces), and the PACAF A-staff, among others of the final S.1650 report, findings, and POA&M. **Coordinator Recommended Change**: It is potentially true that neither AFCEC nor DAF officials specifically followed-up with [redacted] Security Forces to ensure that all physical security findings from the report were addressed (nor should that necessarily be a Civil Engineer responsibility). But it is disingenuous to say that CE could not demonstrate that people in the Security Forces chain of command were not notified. **Originator Response**: Choose an item. **Originator Reasoning**:	[redacted]
~~CUI~~	10	Multiple		☐	**Coordinator Comment and Justification**: The terms "non-AFCEC control systems," "non-AFCEC asset owners," "not owned by AFCEC" (or similar) throughout the report are inaccurate and confusing.	[redacted]

DD FORM 818-1, AUG 2016 SELECT A CLASSIFICATION 6

Revised Pages 9

(U) Air Force, Director of Civil Engineers (cont'd)

~~SECRET//NOFORN~~

CONSOLIDATED DoD ISSUANCE COMMENT MATRIX

Issuance Type and Number, "Title"

CLASS	#	PAGE	PARA	BASIS FOR NON-CONCUR?	COMMENTS, JUSTIFICATION, AND ORIGINATOR JUSTIFICATION FOR RESOLUTION	COMPONENT AND POC NAME, PHONE, AND E-MAIL
					Coordinator Recommended Change: The Air Force Civil Engineer Center does not own any assets or missions in the context of the S.1650 assessments. The control systems and critical infrastructure are owned by the individual installations under the auspices of the Civil Engineers and the CE Squadron commander, specifically. AFCEC serves as subject matter experts and technical support capability to the DAF Civil Engineer community. Recommend changing all instances of "non-AFCEC asset owners," etc. to "non-Civil Engineer" or "not owned by the Civil Engineer community" when the intention is to draw a line around those DCI systems owned/operated supported by CE or the inverse. E.g. Recommendation 3b should read: "Develop and implement a process to notify and verify that corrective actions were taken to mitigate cybersecurity vulnerabilities affecting assets not owned by the Air Force Civil Engineers but that directly impact Department of Air force missions and operations." **Originator Response**: Choose an item. **Originator Reasoning**:	
~~S/NF~~	11			☐	**Coordinator Comment and Justification**: Table 2 is missing [redacted] as an identified DAF-owned S.1650 installation from Joint Staff that was assessed as part of the DAF's 1650 program. **Coordinator Recommended Change**: Add [redacted] **Originator Response**: Choose an item. **Originator Reasoning**:	[redacted]
~~CUI~~	12	14	1	☐	**Coordinator Comment and Justification**: This finding refers to the cyber positions within Civil Engineer squadrons. The Air Force Civil Engineer Center (AFCEC) is not responsible for funding or filling vacant positions within	[redacted]

DD FORM 818-1, AUG 2016 SELECT A CLASSIFICATION 7

Final Report Reference

Revised- Page 24

Revised- Page 11

(U) Air Force, Director of Civil Engineers (cont'd)

Final Report Reference

Revised- Page 11

~~SECRET//NOFORN~~

CONSOLIDATED DoD ISSUANCE COMMENT MATRIX

Issuance Type and Number, "Title"

CLASS	#	PAGE	PARA	BASIS FOR NON-CONCUR?	COMMENTS, JUSTIFICATION, AND ORIGINATOR JUSTIFICATION FOR RESOLUTION	COMPONENT AND POC NAME, PHONE, AND E-MAIL
					squadrons. Manpower determinations and the funding of vacant positions is a responsibility that resides with the respective Major Command (MAJCOM). AFCEC provides contractor assistance to installations that lack expertise to mitigate cybersecurity risks and help maintain the cybersecurity of control systems. Additionally, AFCEC has funded a team to focus on Defense Critical Infrastructure mitigations and assist installation in identifying and planning Section 1650 assessment projects. AFCEC does provide, in conjunction with Headquarters Air Force, advice and assistance to squadrons on cyber position classification. **Coordinator Recommended Change**: **Originator Response**: Choose an item. **Originator Reasoning**:	[redacted]
~~CUI~~	13	14	2	☐	**Coordinator Comment and Justification**: AFCEC is working with [redacted] using the Defense Critical Infrastructure mitigation contractor to validate whether corrective actions taken by the former Information System Security Manager for all vulnerabilities identified during Section 1650 assessments were effectively mitigated and to take appropriate actions. **Coordinator Recommended Change**: **Originator Response**: Choose an item. **Originator Reasoning**:	[redacted]
~~CUI~~	14	14	3	☐	**Coordinator Comment and Justification**: AFCEC has developed a process that is in coordination for approval by the Authorizing Official in the office of the	[redacted]

DD FORM 818-1, AUG 2016 SELECT A CLASSIFICATION 8

(U) Air Force, Director of Civil Engineers (cont'd)

~~SECRET//NOFORN~~

CONSOLIDATED DoD ISSUANCE COMMENT MATRIX

Issuance Type and Number, "Title"

CLASS	#	PAGE	PARA	BASIS FOR NON-CONCUR?	COMMENTS, JUSTIFICATION, AND ORIGINATOR JUSTIFICATION FOR RESOLUTION	COMPONENT AND POC NAME, PHONE, AND E-MAIL
					Director of Civil Engineers (AF/A4C). The process includes coordination with DoW Components and installation officials to notify and verify that corrective actions were taken to mitigate cybersecurity vulnerabilities affecting assets not owned by the Air Force Civil Engineer Center but that directly impact its missions and operations. The process was shared during the DoDIG Audit visit. **Coordinator Recommended Change**: **Originator Response**: Choose an item. **Originator Reasoning**:	[redacted]

DD FORM 818-1, AUG 2016 SELECT A CLASSIFICATION 9

(U) Air Force, Director of Civil Engineers (cont'd)

~~SECRET//NOFORN~~

CONSOLIDATED DoD ISSUANCE COMMENT MATRIX

Issuance Type and Number, "Title"

HOW TO FILL OUT THE DD 818-1 MATRIX

GENERAL GUIDANCE:

- **To sort table** by page/paragraph number, hover your mouse over the top of the first cell in the "page" column until a downward arrow appears; click and drag to the right to select both page and para columns. Under Paragraph on the Home ribbon, select A-Z button, set to sort by Column 3 and then Column 4, and select "OK." **To add new rows,** copy and paste a blank row to keep consistent formatting. **To add automatic numbering to column 2**, select entire column and click on the Numbering button under Paragraph on the Home ribbon.

OSD COMPONENT (OFFICE OF PRIMARY RESPONSIBILITY):

- Do **not** use the DD Form 818.
- Consolidate comments from all coordinators and adjudicate them. When **pasting** coordinator's comments from the coordinating Components' DD Form 818s into your consolidated DD Form 818-1, use "Insert New Row" paste option. You do not need to include administrative comments (spelling, paragraph numbering, etc.), in the consolidated DD Form 818-1. Leave columns 3 and 4 blank for general comments that apply to the whole document.
- **Sort comments** by the pages/paragraphs to which they apply using the **General Guidance** sort feature (e.g., all comments from all coordinators that apply to Page 3, Paragraph 1.1.a., should be together; all comments that apply to Page 3, Paragraph 1.1.b., should be next). Set classification header, footer, Column 2, and complete the last two entries in Column 6:

COLUMN 6	If you rejected or partially accepted a comment, enter your rationale in the originator reasoning area. If any material is **classified** or **controlled unclassified information**, follow DoDM 5200.01 or DoDI 5200.48 guidance for marking the document. Leave originator reasoning area blank if you accepted it. Include any related communications with the coordinating Component. You **must** provide convincing support for rejecting nonconcurrence comments.

DD FORM 818-1, AUG 2016 **SELECT A CLASSIFICATION** 10

(U) Acronyms and Abbreviations

(U) A4CIC	Air Force Civil Engineers Cyber Integration
(U) AFCEC	Air Force Civil Engineer Center
~~(S//NF)~~ [redacted]	[redacted]
(U) DAF	Department of the Air Force
(U) DCI	Defense Critical Infrastructure
(U) GAO	Government Accountability Office
(U) ISSM	Information System Security Manager
(U) NDAA	National Defense Authorization Act

(U) Glossary

(U) **Cataclysmic.** An event or action causing extensive destruction, or a sudden, violent change considered to be above and beyond catastrophic.

(U) **Catastrophic.** An event or action causing destruction or a violent change.

(U) **Control Systems**. Specialized systems and mechanisms that support infrastructure by ensuring infrastructure services are delivered to accomplish the mission.

(U) **Defense Critical Infrastructure.** Any asset of the DoW of such extraordinary importance to the function of the Department and the operation of the Armed Forces that the incapacitation of destruction of such asset by a cyber attack would have a debilitating effect on the ability of the Department to fulfill its mission.

(U) **Facility-Related Control Systems.** A subset of control systems designed to manage facility-specific systems, such as heating, ventilation, air conditioning, lighting, access control operations, automated building operations, security alarms, and energy efficiency.

(U) **High Vulnerabilities.** Vulnerabilities that, if exploited, would likely cause strategic mission failure or result in a marginal capability to execute assigned missions.

(U) **Significant Vulnerabilities.** Vulnerabilities that, if exploited, may significantly degrade strategic mission capability, leaving diminished ability to execute assigned missions.

Whistleblower Protection
U.S. Department of War

Whistleblower Protection safeguards DoW employees against retaliation for protected disclosures that expose possible fraud, waste, and abuse in Government programs. For more information, please visit the Whistleblower webpage at www.dodig.mil/Components/Administrative-Investigations/Whistleblower-Reprisal-Investigations/Whistleblower-Reprisal/ or contact the Whistleblower Protection Coordinator at Whistleblowerprotectioncoordinator@dodig.mil

For more information about DoW OIG reports or activities, please contact us:

Legislative Affairs Division
legislative.affairs@dodig.mil

Public Affairs Division
public.affairs@dodig.mil

www.dodig.mil

DoD Hotline
www.dodig.mil/hotline

~~SECRET//NOFORN~~

DEPARTMENT OF WAR OFFICE OF INSPECTOR GENERAL

4800 Mark Center Drive
Alexandria, Virginia 22350-1500
www.dodig.mil
DoD Hotline 1.800.424.9098

~~SECRET//NOFORN~~