Report No. DODIG-2025-071

INSPECTOR GENERAL

U.S. Department of Defense

FEBRUARY 21, 2025

(U) Audit of Cyber Vulnerabilities Impacting Defense Critical Infrastructure

~~Classified By: Carol N. Gorman, Assistant Inspector General for Audit, Cyberspace Operations~~
~~Derived From: Multiple Sources~~
~~Declassify On: 20480221~~

~~Controlled By: DoD OIG, Audit, Cyberspace Operations~~
~~CUI Category: DCRIT~~
~~Distribution/Dissemination Control: FEDCON~~
~~POC: Assistant Inspector General for Cyberspace Operations,~~ [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 DoDI 5230.09 prior to public release.~~

INDEPENDENCE ★ INTEGRITY ★ EXCELLENCE ★TRANSPARENCY


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

Results in Brief

Audit of Cyber Vulnerabilities Impacting Defense Critical Infrastructure

January 31, 2025

(U) Objective

(U) The announced objective of this audit was to assess the progress made by the Departments of the Navy (DON) and Air Force in mitigating the Defense Critical Infrastructure (DCI) cybersecurity vulnerabilities identified during the installation evaluations conducted in response to section 1650 of the National Defense Authorization Act (NDAA) for FY 2017. During the audit, we revised the objective to focus on the DON because our initial analysis identified that the DON did not have a plan for responding to the cybersecurity vulnerabilities identified during the Section 1650 assessments. The revised objective of this audit was to assess the progress made by the DON in mitigating the DCI cybersecurity vulnerabilities identified during the installation evaluations conducted in response to section 1650 of the NDAA for FY 2017.

(U) Background

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

(U) 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, required the Secretary of Defense to, among other actions, submit to Congress a plan for evaluating DoD critical infrastructure cyber vulnerabilities, prioritizing military installation evaluations, and identifying DCI cyber vulnerabilities.

(U) Findings

~~(CUI)~~ The DON made minimal progress in mitigating [redacted] cybersecurity vulnerabilities [redacted], DON officials stated that they:

- ~~(CUI)~~ could not provide documentation to support actions that they stated they took to mitigate [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 [redacted].

~~(CUI)~~ The DON made only minimal progress in mitigating [redacted] cybersecurity vulnerabilities because it failed to clearly establish:

- (U) ownership of the assets and control systems associated with the vulnerabilities, or
- (U) expectations for managing the risk associated with the vulnerabilities.

(U) By not mitigating the cybersecurity vulnerabilities affecting DCI, the DON unnecessarily increased the risk that its DCI could be degraded, incapacitated, or exploited. These vulnerabilities, if left unmitigated, provide adversaries or malicious actors with opportunities to adversely affect critical missions or functions and the DON's ability to deploy, support, and sustain military forces worldwide.

(U) The Federal Bureau of Investigation and the Cybersecurity and Infrastructure Security Agency reported that since January 2024, the U.S. Government has publically identified that adversaries or malicious actors have aggressively targeted U.S. critical infrastructure,

Results in Brief

Audit of Cyber Vulnerabilities Impacting Defense Critical Infrastructure

(U) Findings (cont'd)

(U) which further emphasizes the DON's need to take corrective actions.

(U) Recommendation

(U) We recommend that the Secretary of the Navy direct the Assistant Secretary of the Navy for Energy, Installations, and Environment, to, among other actions:

- (U) develop and implement processes that establish asset and control system ownership and clearly define responsibilities for managing cybersecurity risks,
- (U) establish expectations for mitigating the unmitigated cybersecurity vulnerabilities identified during the Section 1650 assessments, and
- (U) hold the Commander, Navy Installations Command, Naval Facilities Engineering Command, and system owners accountable for not taking corrective actions.

(U) Management Comments and Our Response

(U) The Secretary of the Navy did not provide comments on the recommendations. Therefore, the recommendations are unresolved and we request comments on the recommendations within 30 days. Please see the Recommendations Table on the next page.

(U) Recommendation Table

(U) Management	Recommendation Unresolved	Recommendation Resolved	Recommendation Closed
(U) Secretary of the Navy	1.a, 1.b, 1.c, and 1.d	None	None **(U)**

(U) Please provide Management comments by March 24, 2025.

(U) Note: The following categories are used to describe agency management's comments to individual recommendations:

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

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

February 21, 2025

(U) MEMORANDUM FOR SECRETARY OF THE NAVY
AUDITOR GENERAL, DEPARTMENT OF THE NAVY

(U) SUBJECT: Audit of Cyber Vulnerabilities Impacting Defense Critical Infrastructure (Report No. DODIG-2025-071)

(U) This final report provides the results of the DoD Office of Inspector General's audit. We previously provided copies of the draft report and requested written comments on the recommendation. We were not able to consider management's comments on the draft report when preparing the final report because comments were not provided.

(U) This report contains four recommendations that are considered unresolved because the Secretary of the Navy did not provide comments on the recommendations. Therefore, the recommendations remains open. We will track these recommendations until management has agreed to take actions that we determine to be sufficient to meet the intent of the recommendations and management officials submit adequate documentation showing that all agreed-upon actions are completed.

(U) DoD Instruction 7650.03 requires that recommendations be resolved promptly. Therefore, within 30 days please provide us your response concerning specific actions in process or alternative corrective actions proposed on the recommendation. Send your response to either followup@dodig.mil if unclassified or rfunet@dodig.smil.mil if classified SECRET.

(U) If you have any questions, please contact [redacted].

Carol N. Gorman

Carol N. Gorman
Assistant Inspector General for Audit
Cyberspace Operations

Contents

(U) Introduction

(U) Objective

(U) The announced objective of this audit was to assess the progress made by the Departments of the Navy (DON) and Air Force in mitigating the Defense Critical Infrastructure (DCI) cybersecurity vulnerabilities identified during the installation evaluations conducted in response to section 1650 of the National Defense Authorization Act (NDAA) for FY 2017.[1] During the audit, we revised the objective to focus on the DON because our initial analysis identified that the DON did not have a plan for responding to the cybersecurity vulnerabilities identified during Section 1650 assessments.[2] We plan to conduct a separate audit that focuses on the Department of the Air Force.[3]

(U) Background

(U) Presidential Policy Directive 21 provides U.S. policy for strengthening the security and resilience of critical infrastructure against both physical and cyber threats.[4] The Directive 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 DoD asset of such extraordinary importance to the DoD and the operation of the Armed Forces that its incapacitation or destruction would have a debilitating effect on the DoD'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, radars, weapon systems, satellite communications, nuclear reactors, and facilities are DCI when critical to the DoD's mission to deter war and ensure national security.

(U) The DoD's reliance on DCI presents opportunities for adversaries to exploit cybersecurity vulnerabilities to compromise, incapacitate, or degrade DoD missions

[1] (U) This report contains information that has been redacted because it was identified by the Department of Defense 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.

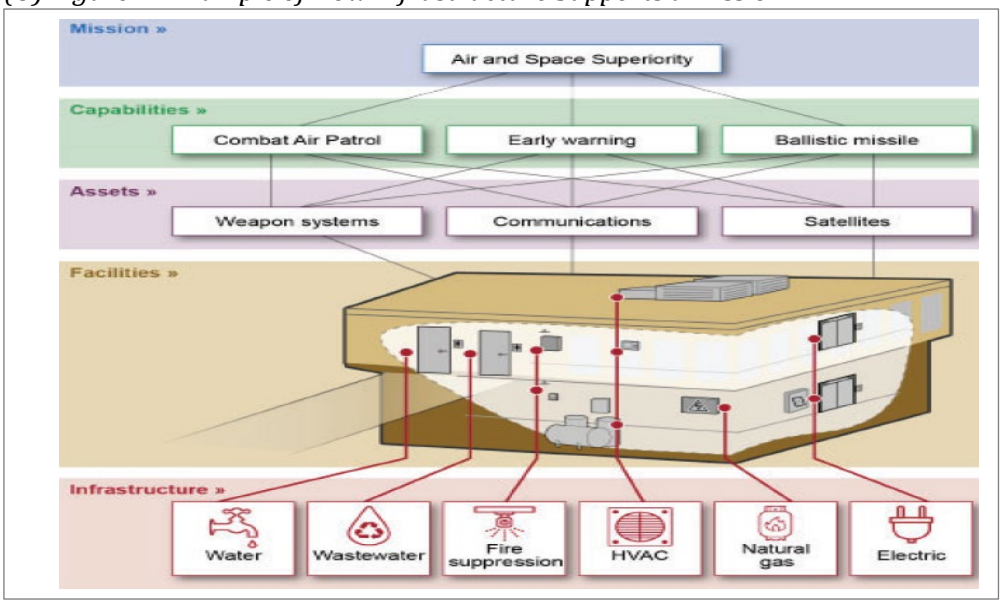
[2] (U) Section 1650 of the FY 2017 NDAA used the term "evaluations" to discuss the reviews required while the DoD called the reviews "assessments." We use the term "assessments," except when discussing the requirement in the NDAA.

[3] (U) The Army Audit Agency is conducting an audit of the Army's response to the Section 1650 assessments.

[4] (U) Presidential Policy Directive 21, "Critical Infrastructure Security and Resilience," February 12, 2013. Presidential Policy Directive 21 was rescinded and replaced by the National Security Memorandum (NSM) on Critical Infrastructure Security and Resilience (NSM-22) on April 30, 2024.

(U) and essential operations. Compromised DCI can severely impact the DoD's ability to deploy, support, and sustain critical missions and operations in the United States and abroad. Figure 1 illustrates an example of how infrastructure supports a DoD mission.

(U) Figure 1. Example of How Infrastructure Supports a Mission



(U) Source: Government Accountability Office, Report No. GAO-21-250SU, "Mission Assurance: Actions Needed to Improve DoD's Cyber Risk Management of Utility-Related Control Systems," August 23, 2021.

(U) Control systems are specialized systems and mechanisms that support infrastructure by ensuring infrastructure services are delivered to accomplish the mission.[5] 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 (FRCS) are a subset of control systems designed to manage facility-specific systems, such as heating, ventilation, air conditioning, lighting and access control or automate building operations, manage security alarms, and improve energy efficiency.

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

(U) DoD Directive 3020.40 requires DoD Components to implement Presidential Policy Directive 21 requirements for protecting DCI.[6] Specifically, DoD Directive 3020.40

[5] (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 Unified Facilities Criteria 4-010-06, "Cybersecurity of Facility-Related Control Systems," effective September 19, 2016.

[6] (U) DoD Directive 3020.40, "Mission Assurance," November 29, 2016 (Change 1 Effective September 11, 2018).

(U) states that the DoD will meet the national and DCI requirements established by the Presidential Policy Directive 21 through mission assurance policy and existing efforts. DoD Directive 3020.40 focuses on mission assurance, which is the DoD's process for protecting or ensuring continuation and resiliency of DoD mission-essential functions, capabilities, and assets, such as DCI. Secretary of the Navy Instruction 5430.7T states that the Assistant Secretary of the Navy for Energy, Installations, and Environment is responsible for coordinating with all levels of the Navy on matters related to mission assurance and critical infrastructure.[7]

(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.[8] DoD Manual 8530.01 requires DoD Components to take corrective actions to mitigate vulnerabilities or threats to a Component's assets, which includes DCI and associated control systems.[9] In addition, the Manual requires DoD Components to track the status of vulnerability remediation in a corrective action plan for the asset or capability.

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

(U) The Under Secretary of Defense for Acquisition and Sustainment, on behalf of the Secretary of Defense, provided Congress the DoD's "Plan for Evaluation of Cyber Vulnerabilities of Department of Defense Critical Infrastructure" (DoD response plan) in May 2018. The DoD response plan provided the framework that the DoD planned to use to accomplish the assessments, including identifying the installations the DoD planned

[7] (U) Secretary of the Navy Instruction 5430.7T, "Assignment of Responsibilities and Authorities in the Office of the Secretary of the Navy," September 9, 2024.

[8] (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. We considered the DON's documented determination to accept the risk associated with a cybersecurity vulnerability.

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

(U) 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 stationed at the installation, and installation threats as determined by the Chairman of Joint Chiefs of Staff. [redacted] The Joint Staff list included 64 installations—24 Army, 12 Navy, and 28 Air Force—with the highest priority critical infrastructure.

(U) Department of the Navy Section 1650 Assessments

(U) The Office of the Chief of Naval Operations (OPNAV), Shore Readiness Division (N4I3), completed Section 1650 assessments between July 2020 and November 2023. OPNAV N4I3 personnel provided the assessment reports and recommendations for corrective actions to installation commanders, who in turn provided the reports and recommendations for corrective actions to tenant commands located on the installation.

(U) The Commander, Navy Installations Command (CNIC), is responsible for inventorying, assessing, and ensuring cybersecurity of FRCSs on Navy installations while the Naval Facilities Engineering Command (NAVFAC) is responsible for authorizing the FRCS under its control.[10] Control system owners are responsible for implementing cybersecurity on their systems to ensure resiliency. In addition, installation commanding officers, chief information officers, public works officers, and mission assurance officials are responsible for mission assurance, cybersecurity, and maintenance in relation to the FRCSs or the assets and missions supported by the FRCSs.

(U) As identified in the DoD response plan and associated Joint Staff prioritized list of critical infrastructure, the DON planned to conduct assessments at 12 installations; however, limitations caused by COVID-19 resulted in the DON conducting assessments at installations they could travel to as COVID-19 restrictions decreased. Based on travel restrictions, the DON conducted assessments at eight of the planned installations. In addition, the DON conducted Section 1650 assessments at six other installations, for a total of 14 assessments as of November 30, 2023. See Appendix B for the list of the planned installations and the installations where the DON conducted Section 1650 assessments.

[10] (U) Joint Letter, "Cybersecurity Tasking for Ashore Control Systems," June 29, 2018. Authorizations, or an authority to operate, are a management decision made by a senior official to authorize operation of an information system on behalf of a Federal agency.

~~(CUI)~~ The DON reports on Section 1650 assessments identified [redacted] vulnerabilities affecting DCI control systems at the 14 installations assessed, [redacted].[11] See Appendix C for a list of the [redacted] cybersecurity vulnerabilities identified at each installation assessed. The DON Section 1650 assessments identified cybersecurity vulnerabilities that included vulnerabilities in security controls effecting access or physical and environment protection. According to the National Institute of Standards and Technology, security controls are critical to effective cybersecurity of control systems because these types of controls are implemented to restrict or limit physical access to facilities with control systems.[12]

(U) What We Reviewed

~~(CUI)~~ To assess the progress made by the DON in mitigating the DCI cybersecurity vulnerabilities identified during the Section 1650 assessments, we focused on the [redacted]. We obtained the mitigation status—mitigated, partially mitigated, unmitigated, or planned—for the [redacted] cybersecurity vulnerabilities from the DON.

(U) We met with and obtained information from chief information officers, mission assurance officials, information systems security managers, public works officials, and other officials responsible for the facilities, assets that the control systems operated or monitored, and cybersecurity. We verified the status of vulnerabilities based on documentation provided by the DON, interviews we held, and observations we made.

[11] ~~(CUI)~~ Critical vulnerabilities have a cataclysmic effect on DoD organizational operations, assets, or individuals. High vulnerabilities have a catastrophic adverse effect. Cataclysmic is considered to be above and beyond catastrophic, causing extensive destruction, or a sudden, violent change. Catastrophic is defined as causing destruction or a violent change. Only four DON Section 1650 assessment reports included cybersecurity vulnerabilities with other than critical and high vulnerabilities. Those reports identified [redacted] vulnerabilities that were considered moderate risk, which are risks that have serious impact on operations or assets, or low risk, which are risks that have limited impact on operations or assets.

[12] (U) National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cyber," version 1.1, April 16, 2018; Special Publication 800-82, Revision 3, "Guide to Operational Technology Security," September 2023; and Special Publication 800-53, Revision 5, "Security and Privacy Controls for Information Systems and Organizations," including updates as of December 10, 2020.

(U) Finding

(U) The Department of the Navy Made Minimal Progress Mitigating Cybersecurity Vulnerabilities from Section 1650 Assessments

~~(CUI)~~ The DON made minimal progress in mitigating the [redacted] cybersecurity vulnerabilities [redacted], DON officials:

- ~~(CUI)~~ could not provide documentation to support actions that they stated they took to mitigate [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 [redacted].

~~(CUI)~~ The DON made only minimal progress in mitigating the [redacted] cybersecurity vulnerabilities because it failed to clearly establish:

- (U) ownership of the assets and control systems associated with the vulnerabilities, or
- (U) expectations for managing the risk associated with the vulnerabilities.

(U) By not mitigating the cybersecurity vulnerabilities affecting DCI, the DON unnecessarily increased the risk that its DCI could be degraded, incapacitated, or exploited. These vulnerabilities, if left unmitigated, provide adversaries or malicious actors with opportunities to adversely affect critical missions or functions and the DON's ability to deploy, support, and sustain military forces worldwide.

(U) The Federal Bureau of Investigation and the Cybersecurity and Infrastructure Security Agency reported that since January 2024, the U.S. Government has publically identified that adversaries or malicious actors have aggressively targeted U.S. critical infrastructure, which further emphasizes the DON's need to take corrective actions.[13]

[13] (U) Federal Bureau of Investigation and Cybersecurity and Infrastructure Security Agency, Joint Statement, "FBI and CISA on PRC [People's Republic of China] Activity Targeting Telecommunications," October 25, 2024.

(U) The DON Made Minimal Progress Mitigating Cybersecurity Vulnerabilities Impacting DCI

~~(CUI)~~ The DON made minimal progress in mitigating [redacted] cybersecurity vulnerabilities [redacted]. DoD Manual 8530.01 requires DoD Components to take corrective actions to mitigate vulnerabilities or threats to a Component's asset, which includes DCI and associated control systems. In addition, the Manual requires DoD Components to prioritize actions taken, validate the effectiveness of corrective actions, and track the status of actions to mitigate the vulnerability in a corrective action plan for the asset or capability.

(U) To assess whether the actions taken or planned were supported, we conducted site visits at two installations; conducted virtual walkthroughs for two additional installations; conducted interviews with officials responsible for DCI and control system cybersecurity; and obtained documentation, such as network diagrams, configuration screenshots, funding requests, statements of work, and management briefings related to the DON's actions taken or planned.

(U) Supported Actions and Plans to Mitigate Cybersecurity Vulnerabilities

~~(S)~~ The DON supported actions taken [redacted].

~~(S)~~ [redacted].

~~(S)~~ In addition, the DON supported actions taken [redacted]

~~(S)~~ [redacted].

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

~~(S)~~ Furthermore, the DON provided plans that included associated resources and timelines needed [redacted]

(U) Unsupported Actions and Plans or Unknown Actions to Mitigate Cybersecurity Vulnerabilities

~~(CUI)~~ The DON did not support actions taken or planned for [redacted] cybersecurity vulnerabilities [redacted]. Specifically, DON officials:

- ~~(CUI)~~ could not provide documentation to support actions that they stated they took [redacted];

[14] (U) The Control System Platform Enclave provides the Navy the ability to identify, detect, react, and recover from malicious attacks to control systems.

- ~~(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 [redacted].

(U) Actions to Mitigate [redacted] Cybersecurity Vulnerabilities Were Unsupported

~~(S//NF)~~ DON officials could not provide documentation, such as network diagrams, plans of action and milestones, and statements of work, to support actions that they stated they took [redacted].[15]

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

(U) Plans to Mitigate [redacted] Cybersecurity Vulnerabilities Were Unsupported

~~(S)~~ DON officials could not produce documentation, such as implementation plans or requests for funding, to support plans they stated were developed [redacted].

[15] (U) An Internet Protocol address is a unique numerical label assigned to each device connected to a computer network that uses the Internet for communication.

~~(S)~~ [redacted]

~~(S)~~ [redacted]

(U) Actions to Mitigate [redacted] Cybersecurity Vulnerabilities Were Unknown

~~(S)~~ DON officials stated that they did not know the status [redacted]

- ~~(S)~~ [redacted]
- ~~(S)~~ [redacted]
- ~~(S)~~ [redacted]

(U) The Deputy Public Works Officer for NAVFAC Mid-Atlantic Public Works Division Oceana and the NAVFAC Chief Information Officer stated that they were unaware of any actions taken or planned to mitigate these vulnerabilities or who was responsible for mitigating them.

~~(S)~~ [redacted]

(U) Ownership of the Control Systems Assessed and Navy Expectations for Managing Risk Was Not Established

~~(CUI)~~ The DON made only minimal progress in mitigating [redacted] cybersecurity vulnerabilities [redacted] because it failed to clearly establish:

- (U) ownership of the assets and control systems associated with the vulnerabilities, or
- (U) expectations for managing the risk associated with vulnerabilities.

(U) Control System Ownership Was Not Consistently Known or Could Not Be Agreed Upon

(U) CNIC, NAVFAC, and system owners did not always know or could not agree which organization owned each control system associated with the cybersecurity vulnerabilities identified during the Section 1650 assessments. According to NAVFAC officials, individuals responsible for mitigating vulnerabilities included NAVFAC, system owners, mission owners, or a combination of the three.

~~(S)~~ Although the Commanders for CNIC and NAVFAC signed a Joint Letter (agreement) to delineate responsibilities related to the cybersecurity of FRCS, the agreement did not address all issues encountered by the Navy in determining ownership for the cybersecurity vulnerabilities. The agreement established that CNIC was responsible for the cybersecurity of all control systems on Navy installations while NAVFAC was responsible for granting each system's authority to operate.[16] However, the agreement provided responsibilities for only the cybersecurity of FRCSs for CNIC and NAVFAC and did not clarify ownership for each control system with cybersecurity vulnerabilities identified in the Section 1650 assessments. [redacted]

[16] (U) Commander, Navy Installations Command and Commander, Naval Facilities Engineering Command Joint Letter, "Cybersecurity Tasking for Ashore Control Systems, Serial 2," June 29, 2018.

~~(S)~~ [redacted][17]

~~(S)~~ In addition, CNIC, NAVFAC, and system owners could not always agree on who was responsible for funding the corrective actions when ownership was determined. [redacted]

(U) DON guidance for managing risk associated with control system cybersecurity vulnerabilities was insufficient to ensure corrective actions were taken for cybersecurity vulnerabilities identified during Section 1650 assessments. While the Joint Letter from the Commanders of CNIC and NAVFAC defined control system responsibilities for systems under their purview, the DON has other control systems and assets on Navy installations, some of which were assessed as part of the Section 1650 assessments, that are not covered by the Joint Letter. Additionally, NAVFAC guidance relates only to control systems under NAVFAC's purview, which did not cover all control systems assessed during the Section 1650 assessments.[19] Therefore, the Secretary of the Navy should direct the Assistant Secretary of the Navy for Energy, Installations, and Environment, in coordination with OPNAV N4I3, CNIC, NAVFAC, and other offices as appropriate, to develop and implement processes that establish control system ownership and clearly define responsibilities for managing the risk associated with control system cybersecurity.

(U) Clear Expectations for Managing Risk Were Not Established

(U) OPNAV N4I3 did not establish clear expectations for the DON in managing the risk associated with cybersecurity vulnerabilities identified during the Section 1650 assessments. After OPNAV N4I3 completed the Section 1650 assessments, OPNAV N4I3 officials provided the assessment reports and recommendations for corrective actions

[17] (U) The Facilities Monitoring and Control Systems Platform Network is a NAVFAC Northwest legacy industrial control system environment.

[18] (U) The Electronic Security System is an automated system used to support physical security protection requirements at facilities.

[19] (U) NAVFAC Echelon II Risk Management Framework Business Rules for Facility-Related Control Systems, Version 3.2, April 2023.

(U) to CNIC and NAVFAC. However, OPNAV N4I3 officials did not provide CNIC or NAVFAC guidance for mitigating cybersecurity vulnerabilities identified during the assessments, tracking the status of the vulnerabilities, or documenting corrective actions taken or planned.

(U) According to an OPNAV N4I3 official, the DON believed that it was not required to mitigate the vulnerabilities and instead, required only to identify them based on the Section 1650 requirements. Although the DoD response plan did not specifically state that the DoD would mitigate all vulnerabilities identified during Section 1650 assessments, DoD Manual 8530.01 specifically requires DoD Components to mitigate identified vulnerabilities. In addition, DoD Instruction 3020.45 requires DoD Components to develop and document corrective action plans for vulnerabilities affecting DCI assets or capabilities. Therefore, the Secretary of the Navy should direct the Assistant Secretary of the Navy for Energy, Installations, and Environment, in coordination with OPNAV N4I3, CNIC, NAVFAC, and other offices as appropriate, to establish expectations for mitigating the unmitigated cybersecurity vulnerabilities identified during the Section 1650 assessments, require the Office of the Chief of Naval Operations to develop and document corrective action plans for unmitigated cybersecurity vulnerabilities, and hold CNIC, NAVFAC, and system owners accountable for not taking corrective actions.

(U) In addition, OPNAV N4I3 did not require the DON to track the status—mitigated, partially mitigated, or planned—of the Section 1650 cybersecurity vulnerabilities. We requested the status of each vulnerability; however, an OPNAV N4I3 official stated that they could not provide that type of information and would need to verify the status of actions taken with CNIC and NAVFAC. The official further stated that CNIC and NAVFAC were responsible for tracking the status of the vulnerabilities; however, neither CNIC nor NAVFAC tracked the status of all cybersecurity vulnerabilities identified during Section 1650 assessments. Although the Assistant Secretary of the Navy for Energy, Installations, and Environment coordinates all levels of the Navy about matters related to mission assurance and critical infrastructure, the Assistant Secretary of the Navy did not have visibility of DON actions taken or planned for the cybersecurity vulnerabilities identified during Section 1650 assessments. However, DoD Manual 8530.01 requires DoD Components to track corrective actions taken to mitigate identified vulnerabilities. Therefore, the Secretary of the Navy should direct the Assistant Secretary of the Navy for Energy, Installations, and Environment, in coordination with OPNAV N4I3, CNIC, NAVFAC, and other offices as appropriate, to develop and implement processes with periodic reporting requirements to track the status of the cybersecurity vulnerabilities identified during the Section 1650 assessments.

~~(CUI)~~ Furthermore, CNIC, NAVFAC, and system owners at the installations did not consistently documented actions taken or planned for the cybersecurity vulnerabilities

~~(CUI)~~ identified in the Section 1650 assessment reports. Although we requested documentation to support actions taken or planned for [redacted] cybersecurity vulnerabilities, CNIC, NAVFAC, and system owners at the 14 installations provided documentation for actions taken or planned for [redacted] vulnerabilities. In many instances, officials with responsibilities for cybersecurity, control systems, or DCI at the time of the audit stated that personnel who had been involved with or aware of the assessments were no longer in their current positions or with the command, and those personnel did not provide documentation before their transition.

~~(CUI)~~ As previously identified in the "Unsupported Actions and Plans or Unknown Actions to Mitigate Cybersecurity Vulnerabilities" section of this report, DON officials stated that they had taken or planned actions [redacted] cybersecurity vulnerabilities, but they could not provide evidence or the evidence provided did not support the corrective actions stated. Therefore, the Secretary of the Navy should direct the Assistant Secretary of the Navy for Energy, Installations, and Environment, in coordination with OPNAV N4I3, CNIC, NAVFAC, and other offices as appropriate, to develop and implement processes for documenting corrective actions and retaining documentation of corrective actions to mitigate cybersecurity vulnerabilities identified during the Section 1650 assessments.

(U) The Department of the Navy Took Some Action to Manage Risk Associated with Section 1650 Cybersecurity Vulnerabilities

(U) In March 2024, during the audit, OPNAV N4I3 began addressing gaps in oversight of the Navy's response to Section 1650 assessments and integrated the assessment methodology into the DON's Enhanced Cyber Assessment element of its Mission Assurance Program. OPNAV N4I3 officials explained that they began including the results from the Section 1650 assessments into the mission assurance corrective action plan tracker they maintained. They used the tracker to monitor the status of vulnerabilities for the Assistant Secretary of the Navy for Energy, Installations, and Environment until the vulnerability was mitigated and support of the mitigation was provided to OPNAV N4I3.

(U) The Enhanced Cyber Assessment provides an in-depth technical review to determine the operational resiliency and the cybersecurity posture of systems connected to or supporting critical infrastructure and assets. An OPNAV N4I3 official stated that OPNAV conducted mission assurance assessments at installations every 3 to 5 years, depending on the priority of the installation. In response to the results of mission assurance assessments, Navy commands and tenants are required to develop a corrective action plan for the identified vulnerabilities, take corrective action to

(U) mitigate the vulnerabilities, prioritize mitigation efforts based on resources, and document risk acceptance.

(U) By not taking corrective actions to mitigate the vulnerabilities or having processes in place to track and document actions taken or planned, the DON unnecessarily increased its risk that an adversary could exploit one or more of the cybersecurity vulnerabilities.

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

~~(CUI)~~ By not mitigating the known cybersecurity vulnerabilities affecting DCI, the DON 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 DON completed 11 of the 14 assessments between 2020 and 2022, as of November 2024, the Navy could support that corrective actions had been taken for [redacted] vulnerabilities impacting its DCI.

~~(S)~~ These vulnerabilities, if left unmitigated, provide adversaries or malicious actors with opportunities to adversely affect critical missions and the DON's ability to deploy, support, and sustain military forces worldwide. [redacted]

(U) In a joint statement, the Federal Bureau of Investigation and Cybersecurity and Infrastructure Security Agency reported that since January 2024, the U.S. Government has publically acknowledged that adversaries or malicious actors have aggressively targeted U.S. critical infrastructure, which further emphasizes the DON's need to take corrective actions to minimize the threat that adversaries and other malicious actors pose to DCI. For example, in April 2024, the Federal Bureau of Investigation issued an alert about the Chinese government's access to critical U.S. infrastructure. In May 2024, the Environmental Protection Agency reported that hackers aligned with Iran carried out malicious cyber attacks against critical infrastructure entities in the U.S., including drinking water systems.

(U) Recommendation, Management Comments, and Our Response

(U) Recommendation 1

(U) We recommend that the Secretary of the Navy direct the Assistant Secretary of the Navy for Energy, Installations, and Environment, in coordination with the Office of the Chief of Naval Operations, Shore Readiness Division; Commander, Navy Installations Command; Naval Facilities Engineering Command; and other Department of the Navy organizations as appropriate:

a. **(U) Develop and implement processes that establish control system ownership and clearly define responsibilities for managing the risk associated with control system cybersecurity vulnerabilities in accordance with DoD and Navy;**

b. **(U) Establish expectations for mitigating the unmitigated cybersecurity vulnerabilities identified during the Section 1650 assessments, require the Office of the Chief of Naval Operations to develop and document corrective action plans for unmitigated cybersecurity vulnerabilities, and hold the Commander, Navy Installations Command, Naval Facilities Engineering Command, and system owners accountable for not taking corrective actions;**

c. **(U) Develop and implement processes with periodic reporting requirements to track the status of the cybersecurity vulnerabilities identified during the Section 1650 assessments; and**

d. **(U) Develop and implement processes for documenting corrective actions and retaining documentation of corrective actions to mitigate cybersecurity vulnerabilities identified during the Section 1650 assessments.**

Management Comments Required

(U) The Navy did not provide comments to the draft report. Therefore, the recommendations are unresolved. We request comments from the Secretary of the Navy within 30 days of this report.

(U) Appendix A

(U) Scope and Methodology

(U) We conducted this performance audit from September 2023 through December 2024 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.

~~(CUI)~~ We obtained 14 DON Section 1650 assessment reports and associated recommendations for corrective actions to identify the types of cybersecurity vulnerabilities identified during the assessments. Although the reports included [redacted], we focused our review on [redacted] cybersecurity vulnerabilities because of the impact exploitation or compromise could have on the DON's ability to conduct mission critical operations or perform mission essential functions.

(U) To determine responsibilities for mitigating control system cybersecurity vulnerabilities, we interviewed personnel from the:

- (U) OPNAV and OPNAV Mission Assurance;
- (U) CNIC;
- (U) NAVFAC Headquarters and all NAVFAC Regions;[20]
- (U) U.S. Fleet Cyber Command/Commander, U.S. 10th Fleet;
- (U) DON Principal Cyber Advisor;
- (U) Office of the Assistant Secretary to the Navy for Energy, Installations, and Environment; and
- (U) system owners at the installations.

~~(S)~~ [redacted]

[20] (U) The seven NAVFAC regions are the District Washington Region; Mid-Atlantic Region; Northwest Region; Southwest Region; Southeast Region; Europe, Africa, Central Region; and Joint Region Marianas.

(S) We interviewed personnel responsible for the facilities, the assets that the control systems operated or monitored, and cybersecurity to determine actions taken or planned to mitigate the vulnerabilities.

(U) We reviewed the following Federal, DoD, and Navy criteria.

- (U) Public Law 114-328, NDAA for FY 17 , December 23, 2016
- (U) Presidential Policy Directive, "Critical Infrastructure Security and Resilience," February 12, 2013
- (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) Secretary of the Navy Instruction 5430.7T, "Assignment of the Responsibilities and Authorities in the Office of the Secretary of the Navy," September 9, 2024
- ~~(CUI)~~ [redacted], April 2023
- (U) Naval Facilities Engineering Systems Command Instruction 11000.4, "Cybersecurity and Sustainment for Facility Related Control Systems (FRCS)," September 28, 2023

(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 DON. Specifically, we were provided Assured Compliance Assessment Solution scan results in Microsoft Excel for the cybersecurity

(U) vulnerabilities identified during the Section 1650 assessments.[21] To determine the reliability of the data, we interviewed the DON 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 DON, we considered the information to be sufficiently reliable for the purpose of our audit.

(U) Prior Coverage

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

(U) Unrestricted GAO reports can be accessed at http://www.gao.gov. Naval Audit Service reports are not available over the Internet. Unrestricted Air Force Audit Agency reports can be accessed from http://www.afaa.af.mil/ by clicking on Freedom of Information Act Reading Room and then selecting audit reports.

(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 that lead agencies for four sectors had taken initial steps to adopt the framework while lead agencies for nine sectors had not. 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.

[21] (U) Assured Compliance Assessment Solution is a program that is used by the Defense Information System Agency to assess DoD networks and information technology systems.

(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) Report No. GAO-21-250U, "Actions Needed to Improve DoD's Cyber Risk Management Utility-Related Control Systems," August 2021

(U) The GAO determined that the military services had taken steps to address leading practices from the National Institute of Standards and Technology for enhancing the organization-wide risk management of cybersecurity for equipment and control systems used to monitor and operate utilities, but collectively had not fully addressed five of six leading practices. The GAO made 10 recommendations, including that the DoD and military services take actions to fully address the five leading practices, issue guidance to establish program standards for assessing control system risks, and implement a detailed process to integrate actions to prioritize risk management efforts. The DoD agreed with six and disagreed with four of the recommendations.

(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 Department of the Air Force 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 Department of the Air Force 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; deconflict guidance for civil engineer control system incident response, incident recovery, and contingency plans; 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) Planned and Conducted Section 1650 Assessments at Department of the Navy Installations

(U) As identified in the DoD response plan and associated Joint Staff prioritized list of critical infrastructure, the DON planned to conduct assessments at 12 installations, but it conducted assessments at only 8 of the planned installations. The DON conducted assessments at 6 other installations as of November 30, 2023, for a total of 14 DON Section 1650 assessments. Table 1 lists the planned installations and the installations where the DON conducted Section 1650 assessments and the date of the assessment report.

(U) Table 1. Installations Where DON Planned and Conducted Section 1650 Assessments

(S) Installation	Planned Section 1650 Assessments	Conducted Section 1650 Assessments	Report Date
[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[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)

(S) Installation	Planned Section 1650 Assessments	Conducted Section 1650 Assessments	Report Date
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted] (S)

(U) *Although the DON planned to conduct assessments at these four locations, the DON did not conduct the assessments.

(U) Source: The DoD OIG.

(U) Appendix C

(U) Critical and High Cybersecurity Vulnerabilities at Department of the Navy Installations

~~(CUI)~~ The DON Section 1650 assessment reports identified [redacted] cybersecurity vulnerabilities on DCI control systems at the 14 installations assessed. Table 2 identifies the number of [redacted] cybersecurity vulnerabilities, by installation, identified in DON Section 1650 assessment reports.

(U) Table 2. Critical and High Cybersecurity Vulnerabilities by Installation

~~(S)~~ Installation	Number of Critical Vulnerabilities from Section 1650 Assessment	Number of High Vulnerabilities from Section 1650 Assessment
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[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)~~

(U) Source: The DoD OIG.

(U) Appendix D

(U) Sources of Classified Information

(U) Source 1: ~~(S)~~ [redacted] (SECRET)
Declassification Date: August 17, 2031
Date of Source: August 17, 2021

(U) Source 2: ~~(S)~~ [redacted] (SECRET)
Declassification Date: August 17, 2031
Date of Source: February 24, 2022

(U) Source 3: ~~(S)~~ [redacted] (SECRET)
Declassification Date: December 6, 2032
Date of Source: December 6, 2022

(U) Source 4: ~~(S)~~ [redacted] (SECRET)
Declassification Date: December 6, 2032
Date of Source: July 31, 2024

(U) Source 5: ~~(S)~~ [redacted] (SECRET)
Declassification Date: December 9, 2031
Date of Source: December 9, 2021

(U) Source 6: ~~(S)~~ [redacted] (SECRET)
Declassification Date: December 9, 2031
Date of Source: June 13, 2024

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

(U) Source 8: ~~(S)~~ [redacted] (SECRET)
Declassification Date: July 1, 2045
Date of Source: August 2, 2024

(U) Source 9: ~~(S)~~ [redacted] (SECRET)
Declassification Date: July 27, 2033
Date of Source: July 27, 2023

(U) Source 10: ~~(S//NF)~~ [redacted] (SECRET//NOFORN)
Declassification Date: July 20, 2045
Date of Source: July 20, 2020

(U) Source 11: ~~(S)~~ [redacted] (SECRET)
Declassification Date: July 20, 2045
Date of Source: July 20, 2020

(U) Source 12: ~~(S)~~ [redacted] (SECRET)
Declassification Date: May 20, 2031
Date of Source: May 20, 2021

(U) Source 13: ~~(S)~~ [redacted] (SECRET)
Declassification Date: May 20, 2031
Date of Source: July 11, 2024

(U) Source 14: ~~(S)~~ [redacted] (SECRET)
Declassification Date: November 28, 2033
Date of Source: November 28, 2023

(U) Source 15: ~~(S)~~ [redacted] (SECRET)
Declassification Date: November 28, 2033
Date of Source: November 28, 2023

(U) Source 16: ~~(S)~~ [redacted] (SECRET)
Declassification Date: June 27, 2033
Date of Source: June 27, 2023

(U) Source 17: ~~(S)~~ [redacted] (SECRET)
Declassification Date: June 27, 2033
Date of Source: June 27, 2023

(U) Source 18: ~~(S)~~ [redacted] (SECRET)
Declassification Date: November 9, 2031
Date of Source: November 9, 2021

(U) Source 19: ~~(S)~~ [redacted] (SECRET)
Declassification Date: November 9, 2031
Date of Source: March 2024

(U) Source 20: ~~(S)~~ [redacted] (SECRET)
Declassification Date: October 18, 2031
Date of Source: October 18, 2022

(U) Source 21: ~~(S//NF)~~ [redacted]
(SECRET//NOFORN)
Declassification Date: December 9, 2031
Date of Source: December 9, 2021

(U) Source 22: ~~(S//NF)~~ [redacted]
(SECRET//NOFORN)
Declassification Date: November 15, 2040
Date of Source: July 17, 2023

(U) Acronyms and Abbreviations

(U) CNIC	Commander, Navy Installations Command
(U) CSPE	Control System Platform Enclave
(U) DCI	Defense Critical Infrastructure
(U) DON	Department of the Navy
(U) FRCS	Facility-Related Control Systems
(U) NAVFAC	Naval Facilities Engineering Command
(U) NDAA	National Defense Authorization Act
(U) OPNAV	Office of the Chief of Naval Operations

(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 ensure infrastructure services, such as electricity, fluids, gas, air movement, traffic control, and water distribution, are delivered when and where required to accomplish the mission.

(U) Control System Platform Enclave (CSPE): A segmented network that provides a standardized approach to identify, detect, react, and recover from malicious attacks to control systems.

(U) Critical Vulnerabilities: Vulnerabilities that have a cataclysmic effect.

(U) Electronic Security System: A physical security system used for facility protection.

(U) Enhanced Cyber Assessment: An assessment process and framework that provides an in-depth technical review of the cybersecurity and resiliency posture of critical and supporting infrastructure such as FRCS.

(U) Facility-Related Control Systems (FRCS): A subset of control systems that are used to monitor and control equipment and systems related to DoD facilities.

(U) High Vulnerabilities: Vulnerabilities that have a catastrophic adverse effect on DoD organizational operations, assets, or individuals.

(U) Internet Protocol Address: An Internet Protocol address is a unique numerical label assigned to each device connected to a computer network that uses the Internet for communication.

(U) Mission Assurance Assessment: A review to protect or ensure the continued function and resilience of capabilities and assets critical to the DoD's performance of mission-essential functions in any operating environment or condition.

Whistleblower Protection
U.S. Department of Defense

Whistleblower Protection safeguards DoD 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 DoD OIG reports or activities, please contact us:

Congressional Liaison
703.604.8324

Media Contact
public.affairs@dodig.mil; 703.604.8324

Twitter
www.twitter.com/DoD_IG

DoD Hotline
www.dodig.mil/hotline

~~SECRET//NOFORN~~

DEPARTMENT OF DEFENSE | OFFICE OF INSPECTOR GENERAL

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

~~SECRET//NOFORN~~