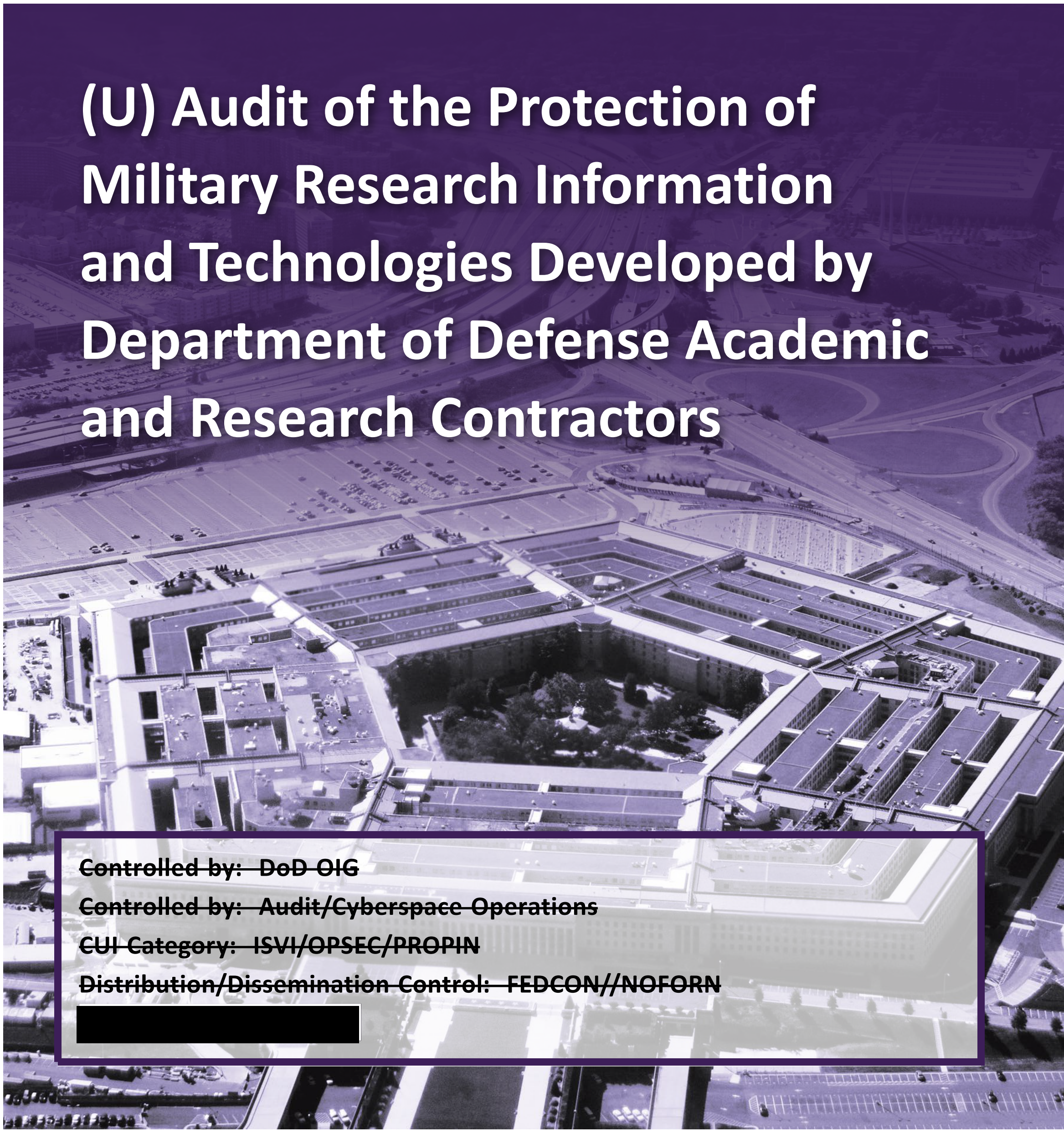
Report No. DODIG-2022-061

~~CUI//NOFORN~~

INSPECTOR GENERAL

U.S. Department of Defense

FEBRUARY 22, 2022



(U) Audit of the Protection of Military Research Information and Technologies Developed by Department of Defense Academic and Research Contractors

~~Controlled by: DoD OIG~~
~~Controlled by: Audit/Cyberspace Operations~~
~~CUI Category: ISVI/OPSEC/PROPIN~~
~~Distribution/Dissemination Control: FEDCON//NOFORN~~
[redacted]

INTEGRITY ★ INDEPENDENCE★ EXCELLENCE

~~CUI//NOFORN~~

(U) Results in Brief

(U) Audit of the Protection of Military Research Information and Technologies Developed by Department of Defense Academic and Research Contractors

February 22, 2022

(U) Objective

(U) The objective of this audit was to determine whether contractors that conduct military research and develop technologies for the DoD have security controls in place to protect controlled unclassified information (CUI) stored on their networks from insider and external cyber threats. CUI is information created or possessed on behalf of the Government that requires safeguarding or dissemination controls according to applicable laws, regulations, and Government-wide policies.

(U) Background

~~(CUI)~~ The DoD works with academia and industry partners that research the development of military technologies. These partners include [redacted], and other DoD contractors that conduct research for the DoD. DoD contracting officers are responsible for oversight of DoD contractors and ensuring compliance with Defense Federal Acquisition Regulation Supplement (DFARS) requirements.

(U) DFARS clause 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting," requires contractors that maintain CUI to implement security controls specified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, which lists security requirements for safeguarding sensitive information on non-Federal information systems. The requirements include controls related to user authentication, user access, media protection, incident response, vulnerability management, and confidentiality of information.

(U) Finding

(U) The 10 academic and research contractors we assessed did not consistently implement required cybersecurity controls to protect CUI stored on their networks from insider and external cyber threats. Specifically,

- (U) four did not enforce the use of multifactor authentication or configure their systems to enforce the use of strong passwords to access their networks and systems;
- (U) three did not identify and mitigate network and system vulnerabilities in a timely manner;
- (U) one did not monitor network traffic and scan its network for viruses;
- (U) two did not encrypt workstation hard drives to protect CUI from unauthorized access or disclosure;
- (U) four did not disable users accounts after extended periods of inactivity;
- (U) five did not protect CUI stored on removable media by using automated controls to restrict the use of removable media;
- ~~(CUI//NF)~~ two did not implement physical security controls, [redacted] and
- (U) one did not develop an incident response plan.

(U) These issues existed because DoD Component contracting officers did not verify whether contractors complied with NIST SP 800-171 cybersecurity requirements. Although the Defense Pricing and Contracting (DPC) Principal Director implemented interim DFARS Rule 2019-D041, "Assessing Contractor Implementation of Cybersecurity Requirements," on September 29, 2020, requiring DoD Component contracting officers to verify contractor implementation of the cybersecurity requirements in NIST SP 800-171, the interim rule only applies to new DoD contracts, task orders, and delivery orders awarded after November 30, 2020, or contracts modified after November 30, 2020, that extend the period of performance.

(U) Finding (cont'd)

(U) The interim rule does not apply to existing contracts, including the contracts that we reviewed during the audit. Without a framework for assessing cybersecurity requirements for existing contractors, the cybersecurity issues identified in this report could remain undetected on DoD contractor networks and systems, increasing the risk of malicious actors targeting vulnerable contractor networks and systems and stealing information related to the development and advancement of DoD technologies.

(U) Recommendations

(U) We recommend that the Principal Director for DPC direct contracting officers to use their authority as outlined in the NIST SP 800-171 DoD Assessment Methodology to assess contractor compliance with NIST SP 800-171 cybersecurity requirements for protecting controlled unclassified information for contracts issued before November 30, 2020.

(U) We also recommend that the Commanding General of the Army Contracting Command; Commander of the Naval Sea Systems Command (NAVSEA); Commander of the Air Force Research Laboratory (AFRL), and the Director of Defense Research and Engineering for Research and Technology (DDR&E [R&T]) direct DoD Component contracting officers to verify that their respective academic and research contractors implement controls related to:

- (U) using multifactor authentication;
- (U) identifying and mitigating vulnerabilities in a timely manner;
- (U) developing plans of action and milestones;
- (U) encrypting CUI;
- (U) disabling inactive user accounts;
- (U) implementing technical security controls to protect CUI stored on removable media;
- (U) implementing physical security controls; and
- (U) documenting and testing incident response plans.

(U) Management Comments and Our Response

(U) The DPC Principal Director disagreed with the recommendation, stating that additional rulemaking and negotiations would be required to make changes applicable to contracts awarded before November 30, 2020, and result in substantial administrative and financial burden to the DoD. In response to the Principal Director's concerns, we revised the report and recommendation to clarify that additional rulemaking and negotiations would not be required because contracting officers had the authority to require additional assessments as outlined in the NIST SP 800-171 DoD Assessment Methodology. Therefore, we request that the Principal Director provide additional comments describing the methods in which contracting officers will use their current authority to conduct assessments of contractor compliance with NIST SP 800-171 security requirements for contracts awarded before November 30, 2020.

(U) The DDR&E (R&T) Acting Director disagreed with the recommendation, stating that the contractor implemented the NIST SP 800-171 security requirements related to encrypting CUI stored on workstations and protecting CUI on removable media. While the contractor relies on physical security controls, the controls were not sufficient to reduce insider threats. Therefore, we request that the Acting Director provide additional comments describing what actions DDR&E (R&T) plans to take to ensure that the contractor establishes the necessary controls.

(U) The Commanding General of the Army Contracting Command, the NAVSEA Inspector General, responding for the NAVSEA Commander, and the AFRL Commander agreed to verify its contractors implement controls related to the security weaknesses we identified. Please see the Recommendations Table on the next page for the status of the recommendations.

(U) Recommendations Table

Management	Recommendations Unresolved	Recommendations Resolved	Recommendations Closed
(U) Defense Pricing and Contracting Principal Director	1	None	None
(U) Commanding General, Army Contracting Command	None	2	None
(U) Commander, Naval Sea Systems Command	None	3.b, 3.c	3.a, 3.d
(U) Commander, Air Force Research Laboratory	None	4.b	4.a
(U) Director of Defense Research and Engineering for Research and Technology	5.b	5.a	None

(U) Please provide Management Comments by March 22, 2022.

(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** – DoD OIG verified that the agreed upon corrective actions were implemented.

INSPECTOR GENERAL

INTEGRITY EFFICIENCY

DEPARTMENT OF DEFENSE

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

February 22, 2022

(U) MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR RESEARCH AND ENGINEERING
PRINCIPAL DIRECTOR, DEFENSE PRICING AND CONTRACTING
AUDITOR GENERAL, DEPARTMENT OF THE NAVY
AUDITOR GENERAL, DEPARTMENT OF THE ARMY
AUDITOR GENERAL, DEPARTMENT OF THE AIR FORCE

(U) SUBJECT: Audit of the Protection of Military Research Information and Technologies Developed by Department of Defense Academic and Research Contractors (Report No. DODIG-2022-061)

(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 recommendations. We considered management's comments on the draft report when preparing the final report. These comments are included in the report.

(U) This report contains two recommendations that are considered unresolved because management officials did not fully address the recommendations. Therefore, as discussed in the Recommendations, Management Comments, and Our Response section of this report, the recommendations will remain unresolved until an agreement is reached on the actions to be taken to address the recommendations. Once an agreement is reached, the recommendations will be considered resolved but will remain open until documentation is submitted showing that the agreed-upon actions are complete. Once we verify that the actions are complete, the recommendations will be closed.

(U) This report contains five recommendations that are considered resolved. Therefore, as discussed in the Recommendations, Management Comments, and Our Response section of this report, the recommendations will remain open until documentation is submitted showing that the agreed-upon actions are complete. Once we verify that the actions are complete, the recommendations will be closed.

(U) This report contains three recommendations that are considered closed as discussed in the Recommendations, Management Comments, and Our Response section of this report. Those recommendations do not require further action.

(U) DoD Instruction 7650.03 requires that recommendations be resolved promptly. For the unresolved recommendations, please provide us within 30 days your response concerning specific actions in process or alternative corrective actions proposed on

(U) the recommendations. For the resolved recommendations, please provide us within 90 days documentation showing that the agreed-upon action has been completed. Your response should be sent as a PDF file to either audcso@dodig.mil if unclassified or [redacted] if classified SECRET. Responses must have the actual signature of the authorizing official for your organization.

(U) We appreciate the cooperation and assistance received during the audit. Please direct questions to me at [redacted].

Carol N. Gorman

Carol N. Gorman
Assistant Inspector General for Audit
Cyberspace Operations

(U) Contents

(U) Introduction

(U) Objective 1

(U) Background 1

(U) Review of Internal Controls 4

(U) Finding. Academic and Research Contractors Did Not Consistently Implement Cybersecurity Controls to Protect CUI on Networks and Systems 5

(U) Academic and Research Contractors Did Not Consistently Implement Cybersecurity Controls to Protect Research Information 6

(U) DoD Component Contracting Officers Did Not Verify Compliance With NIST Requirements 17

(U) DoD Research Data and Technologies Could Be Compromised by Cyberattacks 20

(U) Management Comments on the Finding and Our Response 21

(U) Recommendations, Management Comments, and Our Response 24

(U) Appendixes

(U) Appendix A. Scope and Methodology 33

- (U) Internal Control Assessment and Compliance 35
- (U) Use of Computer-Processed Data 35
- (U) Use of Technical Assistance 36
- (U) Prior Coverage 36

(U) Appendix B. Sampling Approach 39

(U) Management Comments

(U) Army 41

- (U) Assistant Secretary of the Army (ALT) 41
- (U) Army Materiel Command 42
- (U) Army Contracting Command 43

(U) Contents (cont'd)

(U) Navy 45

(U) NAVSEA 45

(U) Air Force 61

(U) AFMC 61

(U) AFRL 63

(U) Defense Research and Engineering for Research and Technology 66

(U) Defense Pricing and Contracting 69

(U) Acronyms and Abbreviations 70

(U) Glossary 71

(U) Introduction

(U) Objective

(U) The objective of this audit was to determine whether contractors that conduct military research and develop technologies for the DoD have security controls in place to protect controlled unclassified information (CUI) stored on their networks from insider and external cyber threats. CUI is information created or possessed on behalf of the Government that requires safeguarding or dissemination controls according to applicable laws, regulations, and Government-wide policies.

(U) This report contains information that may be considered contractor proprietary data, such as information related to contractor internal operating processes. Public release of contractor proprietary data violates criminal provisions in title 18, section 1905, United States Code. Therefore, we identify the 10 academic and research contractors we assessed as Contractors A through J to ensure that these contractors and their associated proprietary information are not identified. See Table 4 in Appendix A for a list of the associated contracting agencies for the 10 contractors. See Appendix A for a discussion on the audit scope and methodology and Appendix B for our detailed sampling approach for selecting and assessing the contractors. See the Glossary for the technical term definitions.

(U) Background

~~(CUI)~~ The DoD works with academia and industry partners that conduct research for the development of military technologies. This includes [redacted], and other contractors that conduct research for the DoD. [redacted] For the purposes of this report, we refer to industry partners that conduct research for developing technologies to meet U.S. military requirements for systems, components, or parts as DoD contractors.

~~(CUI)~~ In [redacted], the DoD established the [redacted]. In [redacted], the DoD [redacted]. [redacted]

~~(CUI)~~ [redacted] and, as of September 2021, the DoD is the [redacted]. The DoD awards contracts to [redacted] and [redacted].

(U) Defense Federal Acquisition Regulation Supplement 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting

(U) The Office of the Under Secretary of Defense for Acquisition and Sustainment establishes DoD contracting and procurement policy, including guidance for safeguarding DoD information in accordance with Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting."[1] DFARS clause 252.204-7012 requires contractors that maintain CUI to implement security controls specified in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171.[2] NIST SP 800-171 requirements include controls related to user authentication, user access, media protection, incident response, vulnerability management, and confidentiality of information.[3]

(U) Cybersecurity Controls Assessed

(U) To determine whether contractors that conduct military research and develop technologies for the DoD had security controls in place to protect CUI stored on their networks from insider and external cyber threats, we assessed selected cybersecurity controls that we consider critical to the protection of CUI. During our audit, we assessed the cybersecurity controls for 10 academic and research contractors for the Army, Navy, Air Force, and Under Secretary of Defense for Research and Engineering.

(U) Cybersecurity controls are safeguards and countermeasures designed to protect the confidentiality, integrity, and availability of CUI information that is processed by, stored on, and transmitted through contractor networks. Table 1 identifies the cybersecurity controls we assessed and their importance.

[1] (U) DFARS 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting," December 2019. Covered defense information is DoD CUI. For the purpose of this report, we refer to covered defense information as CUI.

[2] (U) NIST SP 800-171, "Protecting Controlled Unclassified Information on Nonfederal Systems and Organizations," Revision 2, February 2020.

[3] (U) DFARS clause 252.204-7012 does not apply to the conduct of fundamental research, which is basic and applied research in science and engineering that is ordinarily published and shared. We did not include contracts with basic and applied research projects in our review.

(U) Table 1. Cybersecurity Controls Assessed and Their Importance

~~(CUI//NF)~~ Cybersecurity Control	Importance of Cybersecurity Control
(U) Authentication	(U) Authentication mechanisms verify user identities, processes, or devices as a prerequisite to allowing access to systems. Malicious cyber actors can exploit authentication methods that do not use two or more different authentication factors; enforce a minimum password length; require complex passwords; limit unsuccessful log-on attempts; or automatically end user sessions after a defined period of inactivity.*
(U) Vulnerability Identification and Mitigation	(U) Identifying and mitigating vulnerabilities includes scanning networks and systems to identify potential weaknesses, such as network vulnerabilities, that can be exploited on a computer or network. Identifying and mitigating network and system vulnerabilities reduces a malicious cyber actor's ability to gain unauthorized access to networks and systems, introduce malware, and steal critical research information that could compromise national security. Identifying and mitigating vulnerabilities on academic and research contractors' networks and systems is critical because malicious cyber actors could target U.S. universities, many of which receive funding to conduct DoD research, in attempts to steal sensitive military information.
(U) Boundary Protection	(U) Network boundaries can use firewalls, antivirus software, and intrusion-detective tools to monitor and respond to unusual activity that may contain malicious code. Malicious code includes viruses, worms, Trojan horses, and spyware. Malicious code can be contained within compressed or hidden files and can be inserted into systems in a variety of ways including web accesses, e-mail, e-mail attachments, and portable storage devices.
(U) Encryption of Data at Rest	(U) Information at rest refers to the state of information when it is not in process or in transit and is located on devices such as hard drives and workstations. Academic and research contractors can protect the confidentiality of research information classified as CUI at rest by using encryption.
(U) Access Control	(U) Access controls limit access to authorized users based on their roles and responsibilities. This includes when user access should be disabled after a defined period of inactivity to prevent a malicious actor from exploiting the user account to gain undetected access to information related to military research information.
(U) Digital Media Protection	(U) Media is protected when access to CUI is limited to authorized users. Digital media includes external and removable hard disk drives, flash drives, compact disks, and digital video disks. Academic and research contractors can implement technical safeguards such as encryption to protect the confidentiality of CUI research information on digital media.
(U) Physical Protection	~~(CUI//NF)~~ Academic and research contractors can physically limit access to equipment, such as workstations, and prevent the unauthorized disclosure of CUI research information by implementing physical protections. Physical protections can include security guards, biometric readers, access card readers, and physical access control logs. In addition, academic and research contractors can monitor physical access by using [redacted]. [redacted], academic and research contractors may face challenges in [redacted] **~~(CUI//NF)~~**

(U) *Note: A malicious cyber actor is an individual that uses technology with the intent to cause harm.

(U) Source: The DoD OIG.

(U) Review of Internal Controls

(U) DoD Instruction 5010.40 requires DoD organizations to implement a comprehensive system of internal controls that provides reasonable assurance that programs are operating as intended and to evaluate the effectiveness of the controls.[4] We identified internal control weaknesses related to contractors implementing physical and cybersecurity controls to protect networks and systems that contain DoD CUI. We will provide a copy of the report to the senior officials responsible for internal controls in the Departments of the Army, Navy, Air Force, and Office of the Under Secretary of Defense for Research and Engineering.

[4] (U) DoD Instruction 5010.40, "Managers' Internal Control Program Procedures," May 30, 2013.

(U) Finding

(U) Academic and Research Contractors Did Not Consistently Implement Cybersecurity Controls to Protect CUI on Networks and Systems

(U) The academic and research contractors we reviewed did not consistently implement cybersecurity controls in accordance with Federal and DoD requirements for safeguarding CUI. Specifically, of the 10 academic and research contractors we assessed:

- (U) four did not enforce the use of multifactor authentication or configure their systems to enforce the use of strong passwords to access their networks and systems;
- (U) three did not identify and mitigate network and system vulnerabilites in a timely manner;
- (U) one did not monitor network traffic and scan its network for viruses;
- (U) two did not encrypt workstation hard drives to protect CUI from unauthorized access or disclosure;
- (U) four did not disable users accounts after extended periods of inactivity;
- (U) five did not protect CUI stored on removable media by using automated controls to restrict the use of removable media;
- ~~(CUI//NF)~~ two did not implement physical security controls, such as [redacted]; and
- (U) one did not develop an incident response plan.

(U) These issues occurred because the DoD Component contracting officers did not verify whether contractors complied with NIST SP 800-171 cybersecurity requirements. Although the Defense Pricing and Contracting (DPC) Principal Director implemented interim DFARS Rule 2019-D041, "Assessing Contractor Implementation of Cybersecurity Requirements," on September 29, 2020, requiring DoD Component contracting officers to verify contractor implementation of the cybersecurity requirements in NIST SP 800-171, the interim rule only applies to new DoD contracts, task orders, and delivery orders awarded after November 30, 2020, or contracts modified after November 30, 2020, that extend the period of

(U) performance.[5] The interim rule does not apply to existing contracts, which includes all of the contracts that we reviewed during the audit. Without a framework for assessing cybersecurity requirements for existing contractors, the cybersecurity issues identified in this report could remain undetected on DoD contractor networks and systems, increasing the risk of malicious actors targeting vulnerable contractor networks and systems and stealing information related to the development and advancement of DoD technologies.

(U) Academic and Research Contractors Did Not Consistently Implement Cybersecurity Controls to Protect Research Information

(U) Academic and research contractors that conduct research for the DoD did not consistently implement cybersecurity controls for protecting CUI stored on their networks from insider and external cyber threats. To determine whether academic and research contractors protected CUI, we assessed cybersecurity controls, processes, and technologies used for managing network and system authentication; vulnerabilities; user account management; and the storage and transmittal of data. Based on our analyses and testing, we identified security weaknesses at the 10 academic and research contractors we reviewed. Table 2 identifies the security weaknesses identified, by contractor.

(U) Table 2. Security Weaknesses Identified at Academic and Research Contractors

Control Deficiencies	Contractor									
	A	B	C	D	E	F	G	H	I	J
(U) Multifactor authentication or strong passwords not enforced		X	X			X		X		
(U) Network and system vulnerabilities not identified or mitigated in a timely manner	X					X			X	
(U) Network not configured to monitor network traffic or scan for viruses						X				
(U) CUI not encrypted on workstations			X						X	
(U) User accounts not disabled after extended periods of inactivity	X	X		X		X				

[5] (U) DFARS Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041), September 29, 2020.

(U) Table 2. Security Weaknesses Identified at Academic and Research Contractor (cont'd)

Control Deficiencies	Contractor									
	A	B	C	D	E	F	G	H	I	J
(U) CUI not protected on removable media		X	X		X		X		X	
(U) Physical security controls not implemented to detect unauthorized access		X								X
(U) Incident response plan not developed								X		

(U) Source: The DoD OIG.

(U) Multifactor Authentication and Strong Passwords Not Enforced

(U) Network and cloud administrators for Contractors B, C, F, and H did not enforce multifactor authentication to access contractor networks and cloud environments that stored CUI.[6] NIST SP 800-171 requires organizations to use multifactor authentication to access non-privileged network accounts.[7] In addition, Contractors B, C, and H allowed users to enter only a username and password (single-factor authentication) to access networks, which could make the networks susceptible to brute force password attacks.[8] NIST SP 800-171 also requires the enforcement of a minimum password complexity requirement when using single-factor authentication.

~~(CUI//NF)~~ Contractor B recognized the need to implement multifactor authentication; however, it only required single-factor authentication because its operating systems did not support multifactor authentication. Contractor B configured its system to require a [redacted]. The Information System Security Officer and the Interim Information System Security Manager stated that Contractor B was in the process of implementing multifactor authentication, and planned to have the implementation completed by [redacted]. Contractor C was also in the process

[6] (U) Multifactor authentication requires using something in a user's possession, such as a token, in combination with something known only to the user, such as a personal identification number.

[7] (U) Nonprivileged network accounts are for users that are not authorized to perform security-related functions.

[8] (U) Brute force password attacks are a method to gain access to a device by attempting multiple combinations of passwords.

~~(CUI//NF)~~ of implementing multifactor authentication; however, according to the Information System Security Manager, Contractor C delayed the implementation of multifactor authentication to comply with social distancing precautions related to the coronavirus disease–2019 pandemic and reduce the potential of person-to-person contact. Contractor C requires its users to develop passwords that are [redacted]. The Information System Security Manager stated that Contractor C planned to complete implementation of multifactor authentication by [redacted].

~~(CUI//NF)~~ Contractor F enforced multifactor authentication to access CUI in its cloud environment, but allowed users to re-authenticate using single-factor authentication within 72 hours of their system log-on. According to the Cloud Administrator for Contractor F, this was an oversight and he corrected the setting during our audit. The Cloud Administrator provided a screenshot of configuration settings that showed Contractor F had adjusted the setting to require the use of multifactor authentication when users re-authenticate to its cloud environment.[9] Contractor H enforced multifactor authentication for users [redacted]. Contractor H required its users to develop passwords that were [redacted]. The Director of Information Technology for Contractor H stated that the physical safeguards around workstations at Contractor H facilities served as a mitigating control for allowing single-factor authentication. While we agree that physical safeguards can mitigate some vulnerabilities, there are nonphysical methods malicious actors can use to access information. For example, malicious actors can bypass physical safeguards using powerful remote applications to crack single-factor authentication methods and gain access to sensitive information, such as CUI.

(U) According to the Cybersecurity and Infrastructure Security Agency, passwords are one of the most vulnerable cyber defenses, and organizations can improve password security by using longer passwords. While NIST SP 800-171 does not specify a minimum number of characters when using passwords, according to NIST SP 800-63B, "Digital Identity Guidelines: Authentication and Lifecycle Management," passwords that are too short are easily guessed by brute-force password attacks, as well as dictionary attacks using words and commonly chosen passwords.[10] Although there are several password-cracking tools that malicious actors

[9] (U) Due to the coronavirus disease–2019 pandemic, we held virtual site visits using collaboration tools, such as screen sharing, that allowed the audit team to verify cybersecurity controls for the contractors we assessed.

[10] (U) NIST SP 800-63B, "Digital Identity Guidelines: Authentication and Lifecycle Management," June 2017.

(U) can use to guess passwords, choosing strong passwords can make it more difficult for malicious actors to guess the password using this type of software. Using multifactor authentication reduces the risk of malicious actors guessing user passwords.

(U) Contractors Did Not Always Identify and Mitigate Network and System Vulnerabilities

~~(CUI//NF)~~ Network administrators for Contractor I did not consistently perform vulnerability scans to identify weaknesses on its network enclaves that store CUI, and did not mitigate known [redacted] vulnerabilities.[11] In addition, network administrators for Contractors A, F, and I did not develop plans of action and milestones (POA&Ms) for vulnerabilities that they were not able to mitigate. NIST SP 800-171 requires non-Federal organizations to scan for vulnerabilities in their systems and applications periodically, and develop POA&Ms if they are unable to mitigate the vulnerabilities in a timely manner. To determine whether the academic and research contractors we assessed mitigated vulnerabilities in a timely manner, we compared network scan results from [redacted] through [redacted].

~~(CUI//NF)~~ At Contractor I, a [redacted] scan revealed that [redacted] vulnerabilities identified in an [redacted] scan remained unmitigated. The [redacted] vulnerabilities included [redacted] and [redacted] vulnerabilities. [redacted][12] [redacted] For example, an unmitigated [redacted] vulnerability from [redacted], identified on Contractor I's enclave, [redacted]. The NIST assessment of this vulnerability states that [redacted]. Although [redacted] released a solution to fix this vulnerability in 2017, Contractor I still had not mitigated the vulnerability by [redacted].

~~(CUI//NF)~~ Contractor I's guidance requires network administrators to scan networks that contain CUI, including enclaves, for vulnerabilities [redacted]. However, the Information Technology representative stated that network administrators only conducted the scans on an as-needed basis. The network

[11] (U) An enclave is an isolated network that is protected by the security controls in place around the overall organizational or enterprise network.

[12] (U) Privileged access allows users to set access rights for other users.

~~(CUI//NF)~~ administrator for Contractor I stated that the scans were [redacted] because the cybersecurity controls around Contractor I's [redacted] network provided an additional layer of security for the enclave, which reduced the need to scan for vulnerabilities [redacted]. However, if vulnerabilities remain unmitigated on the [redacted] network, malicious actors can exploit those vulnerabilities to gain access to CUI stored in the enclave. We compared [redacted] network scans for Contractor I from [redacted] and [redacted] and identified [redacted] of [redacted] vulnerabilities that remained unmitigated. The [redacted] vulnerabilities included [redacted] and [redacted] vulnerabilities. For example, an unmitigated [redacted] vulnerability from [redacted] identified on Contractor I's [redacted] network [redacted]. Although [redacted] released a solution to fix this vulnerability in 2019, Contractor I still had not mitigated the vulnerability by [redacted]. Therefore, the security of Contractor I's [redacted] network is weakened by the unmitigated vulnerabilities, and malicious actors can gain access to CUI.

(U) Without a POA&M, Contractor I may be unable to correct network weaknesses, establish risk mitigation activities, or determine how long a vulnerability remained unmitigated.

(U) While Contractor I's vulnerability management program included a process for developing POA&Ms to address unmitigated vulnerabilities in a timely manner, Contractor I did not develop POA&Ms for the unmitigated vulnerabilities. Without a POA&M, Contractor I may be unable to correct network weaknesses, establish risk mitigation activities, or determine how long a vulnerability remained unmitigated.

(U) Contractors A and F did not create POA&Ms for vulnerabilities that they could not mitigate in a timely manner. The Associate Director for Contractor A stated that POA&Ms were not developed because the Contractor prioritized implementing the software and tools to strengthen its cybersecurity posture over developing POA&Ms. However, after our virtual site visit, the audit team verified that Contractor A had developed POA&Ms for the unmitigated vulnerabilities. Cloud administrators for Contractor F stated that they were still developing a vulnerability management program, which would include a process for developing POA&Ms.

(U) Contractor F Did Not Configure Its Network to Monitor Network Traffic or Scan for Viruses

(U) Network administrators did not configure the Contractor F network to consistently perform full-disk scans for emerging viruses, malware, and spyware.[13] In addition, network administrators for Contractor F did not configure automated tools to monitor network traffic and alert network administrators of unusual activity by external and internal malicious actors. NIST SP 800-171 requires organizations to perform periodic scans of organizational systems and real-time scans of files from external sources to detect malicious code.[14] NIST SP 800-171 also requires system monitoring to include external and internal monitoring through a variety of tools and techniques including network monitoring software and scanning tools.

~~(CUI//NF)~~ Network administrators for Contractor F did not perform full-disk scans for viruses, malware, and spyware; instead, the network administrators performed quick scans, which only check for the areas of a network that malicious software is most likely to infect. While [redacted] recommends performing quick scans, [redacted] acknowledges that malicious files can be stored in locations that are not included in quick scans. [redacted] recommends that organizations perform antivirus scans 15 minutes after applying antivirus updates, which could occur three times a day or more as needed. The network administrator for Contractor F stated that he could not schedule weekly full-disk antivirus scans because it conflicted with a cost-saving measure that required computers to shut down during off-work hours. As an alternative, the network administrator for Contractor F stated that he manually initiated antivirus quick scans; however, he did not initiate the scans at a defined frequency and the last scan that he performed was 30 days prior to our virtual site visit. After our virtual site visit, the audit team verified that Contractor F had configured its network to perform daily full-disk scans by reviewing a screenshot of Contractor F's antivirus schedule. Therefore, we will not include a recommendation for this issue.

(U) The network administrator for Contractor F stated that the contractor relied on the firewall in its cloud environment to restrict unusual activity. However, Contractor F disabled the firewall's ability to generate logs of network traffic and alerts for unusual activity. Alerts allow network administrators to receive real-time warnings of cybersecurity events, such as unauthorized attempts

[13] (U) A full-disk scan checks all files on the hard disk and all running programs.

[14] (U) Real-time scans occur the moment a user opens and closes a file.

(U) to access networks and systems. The network administrator for Contractor F stated that logs and alerts of unusual activity were disabled because there were few users with access to the research project, and due to his trust in those users, there was not a need to continuously monitor logs for unusual activity. However, after our virtual site visit, the audit team verified that Contractor F enabled business rules to analyze and alert network administrators of unusual activity. Performing daily full-disk scans and updating virus definitions decreases the risk of missing opportunities to identify and mitigate emerging threats, such as malicious code contained within files.

(U) Performing daily full-disk scans and updating virus definitions decreases the risk of missing opportunities to identify and mitigate emerging threats, such as malicious code contained within files.

(U) CUI Was Not Encrypted on Workstations

~~(CUI//NF)~~ System administrators for Contractors C and I did not encrypt CUI stored on workstations.[15] As of August 2021, Contractor C encrypted CUI for only [redacted] of its workstations. NIST SP 800-171 requires organizations to encrypt CUI on both mobile and computing platforms, which includes hardware and software. NIST SP 800-171 also states that organizations must protect the confidentiality of CUI at rest regardless of the location of the physical workstation. The Chief Information Security Officer for Contractor C stated that his department began purchasing the Trusted Platform Module chips to encrypt data at rest on workstations, but has not received the chips because of supply chain delays.[16] The Information Technology representative for Contractor I stated that the physical safeguards around Contractor I's facility mitigated the need to encrypt CUI on its workstations. While Contractor I relies on the physical security controls within its facilities that may be sufficient for reducing external threat actors, there could be potential security gaps with respect to malicious internal actors who are authorized to access the facility. If an insider threat actor stole a hard drive containing CUI, encrypting the data would help to prevent the individual from accessing the information on the hard drive.

[15] (U) A workstation is a desktop computer terminal which is normally connected to a network and more powerful than a personal computer.

[16] (U) The Trusted Platform Module chip is a tamper-resistant circuit that encrypts and protects sensitive information using multiple physical security mechanisms that malicious software is unable to tamper with.

(U) User Accounts Were Not Disabled After Extended Periods of Inactivity

(U) System administrators for Contractors A, B, D, and F did not disable user accounts after extended periods of inactivity. NIST SP 800-171 requires organizations to disable or remove accounts after a defined period of inactivity. Although NIST SP 800-171 does not specify a period of inactivity, Microsoft recommends disabling inactive user accounts every 6 months. Table 3 shows Contractors A, B, D, and F timeframes for disabling inactive accounts.

(U) Table 3. Timeframes for Disabling Inactive Accounts

~~(CUI//NF)~~ Contractor	When Contractors Disabled Inactive Accounts
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted] ~~(CUI//NF)~~

(U) Source: The DoD OIG.

~~(CUI//NF)~~ Although the Information System Security Officer stated that Contractor B performed semi-annual reviews of user accounts based on his knowledge of individuals assigned to the project, we identified two user accounts that remained active on Contractor B's network for [redacted]. The Principal Investigator and System Administrator for Contractor F stated that its process was sufficient since there were only 10 individuals assigned to the project. However, the audit team identified [redacted]. The Principal Investigator stated that he was concerned that disabling or deleting inactive user accounts could cause him to lose the information associated with that user's account. The Principal Investigator also stated that he was unsure if that would happen, but he was being cautious with the information associated with the project. According to [redacted], after a user account is deleted, the account remains suspended for 30 days, and during the 30-day window the user account can be restored, along with all its properties.

(U) Outdated or unused accounts provide network penetration points that may go undetected; therefore, inactive accounts should be disabled until needed, or removed.

(U) The process of disabling a user account is not known to cause a loss of data, and the system administrator can go into the account without enabling it first. This would allow Contractor F to retain access to the information associated with the user account after it is disabled. Outdated or unused accounts provide network penetration points that may go undetected; therefore, inactive accounts should be disabled untilneeded, or removed.

~~(CUI//NF)~~ At the time of our site visit, Contractor A's process for disabling inactive user accounts was based on the system administrator's knowledge of the personnel assigned to the contract. However, the Associate Director stated that the contractor planned to implement an automated process for disabling inactive user accounts. After our site visit, we verified that Contractor A configured its network to disable user accounts after [redacted] of inactivity. In addition, at the time of our site visit, the Information Services Director for Contractor D stated that he added notes to user accounts for users that notified him of their intent to be on extended leave, and removed accounts for individuals that left the organization within [redacted] of departure. However, after the site visit, Contractor D implemented security monitoring software to identify inactive user accounts, which we verified that systems administrators receive notifications from for accounts that need disabling. As a result of Contractors A and D implementing automated processes to disable inactive user accounts, we will not include recommendations to the DoD Component contracting officers for Contractors A and D related to this issue.

(U) CUI Was Not Protected on Removable Media

(U) Although Contractors B, C, E, G, and I developed administrative controls, such as organizational policies, to protect CUI stored on removable media, the contractors did not implement automated controls, such as whitelisting, to enforce its policies to protect CUI stored on removable media.[17] NIST SP 800-171 requires that organizations control the use of removable media on its systems and allows organizations to employ automated and administrative controls, such as limiting the use of removable media to approved devices. NIST SP 800-171 also requires that organizations control the use of removable media on their systems.

[17] (U) Whitelisting is the action of creating a list of devices, such as removable media, approved for use on an organization's systems and network.

~~(CUI//NF)~~ While Contractor B required users to manually encrypt CUI on removable media, it did not implement automated controls to encrypt CUI stored on removable media. According to the interim Information Systems Security Manager, Contractor B relied on its [redacted] to ensure users encrypted CUI on removable media. However, relying only on users to encrypt CUI stored on removable media is not an effective method because users might forget or fail to encrypt the CUI. Implementing automated controls to encrypt CUI on removable media would ensure CUI is protected even if the user forgets to encrypt the information.

~~(CUI//NF)~~ Contractors C, E, G, and I did not implement automated controls to restrict the use of unapproved removable media, and instead relied on their users to use approved removable media. For example, according to the Information System Security Manager, Contractor C did not have the ability to whitelist media devices using its current network tools; however, it developed a POA&M for controlling removable media devices that it expected to implement by [redacted]. Contractor E had policies that required users to only use removable media from trusted sources, such as the Government, but it did not implement automated controls to prevent users from using and storing CUI on removable media from untrusted sources. The Information Security Engineer stated that Contractor E planned to implement automated controls to prevent the use of removable media by [redacted]. Solely relying on administrative controls, such as policies, does not prevent actors with malicious intentions from circumventing policies and using removable media to steal CUI.

(U) Solely relying on administrative controls, such as policies, does not prevent actors with malicious intentions from circumventing policies and using removable media to steal CUI.

~~(CUI//NF)~~ The Information Technology Director for Contractor G stated that Contractor G finalized its CUI Media Policy, and expected to fully implement the policy by [redacted]. In addition, the Information Technology Director stated that DoD acquisition requirements for media protection are not well defined, and he believed that managing removable media through administrative controls was sufficient. While administrative controls such as organizational policies help to inform personnel of the acceptable use of removable media, academic and research contractors can use automated controls to enforce contractor policies against personnel who could circumvent the contractors' administrative controls. Contractor I's Information Technology representative stated that he interpreted NIST SP 800-171 requirement as an administrative control, not a technical control. However, NIST SP 800-171 states that both administrative and technical controls should be used to control the use of removable media on an organization's systems.

(U) According to the United States Computer Emergency Readiness Team, 25 percent of malicious programs are spread through removable media devices. The United States Computer Emergency Readiness Team also states that using portable devices can increase the risk of data loss (when a physical device is lost), data exposure (when sensitive data is exposed to the public or a third party without consent), and increased exposure to network-based attacks, such as viruses, to and from any system connected to the portable device.

(U) Physical Security Controls Were Not Implemented to Detect Unauthorized Access

~~(CUI//NF)~~ Security personnel at Contractors B and J did not monitor physical access throughout facilities that maintained CUI. NIST SP 800-171 requires organizations to protect and monitor the physical facility for organizational systems. While Contractors B and J [redacted], they did not [redacted]. The Facility Security Officer for Contractor B stated that he was unaware that NIST SP 800-171 recommends [redacted] as a means of physical protection. However, NIST SP 800-171 provides examples of methods to monitor physical access within organizational facilities, including [redacted]. According to the Chief Information Security Officer and the Program Security Lead for Contractor J, [redacted] the FY 2019 National Defense Authorization Act.[18] According to the Chief Information Security Officer, Contractor J is acquiring [redacted]; however, [redacted]. Without [redacted], security personnel reduced their ability to promptly identify and respond to security incidents and suspicious activities in and around facilities that maintain CUI.

(CUI//NF) Without [redacted], security personnel reduced their ability to promptly identify and respond to security incidents and suspicious activities in and around facilities that maintain CUI.

[18] ~~(CUI//NF)~~ Public Law 115-232, "John S. McCain National Defense Authorization Act for Fiscal Year 2019," August 13, 2018. According to the FY 2019 National Defense Authorization Act, Federal [redacted] We did not verify or validate that [redacted].

(U) Contractor H Lacked an Incident Response Plan

(U) Contractor H did not develop an incident response plan. An incident response plan is a set of instructions or procedures to help information technology personnel detect, respond to, and limit the effects of a malicious cyberattack. NIST SP 800-171 requires that organizations establish incident-handling capabilities for organizational systems that include preparation, detection, analysis, containment, recovery, and user response activities. According to the Director of Information Technology, Contractor H did not have an approved incident response plan because it was in the process of updating and consolidating its old policies into one enterprise-wide cybersecurity policy, which would include an incident response plan. The Contracts Manager for Contractor H provided a draft of the incident response plan, and stated that the incident response plan would be implemented after the new policies were approved in September 2021.

(U) DoD Component Contracting Officers Did Not Verify Compliance With NIST Requirements

~~(CUI)~~ Although DoD Component contracting officers took steps to require contractors to protect CUI by including DFARS clause 252.204-7012 in contracts, the contracting officers did not develop and implement processes to verify that contractors complied with NIST SP 800-171 cybersecurity requirements for protecting CUI. While DoD Component contracting officers oversee contractor performance, their oversight activities did not include verifying that contractors implemented security controls to protect CUI. For example, the Contracting Officer for the U.S. Army (Contractor D) stated that he was not aware of a requirement for Contracting Officer's Representatives to verify that contractors implemented security controls to protect CUI. In addition, the [redacted] Program Manager for the Air Force (Contractor I) stated that he was not aware of a cybersecurity component when work performance of the contractors is reviewed. However, the Undersecretary of Defense for Acquisition and Sustainment issued a memorandum in November 2018 that gives DoD Component contracting officers the authority to oversee contractor compliance with NIST SP 800-171.[19] Furthermore, the Contracting Officer's

(U) While DoD Component contracting officers oversee contractor performance, their oversight activities did not include verifying that contractors implemented security controls to protect CUI.

[19] (U) Undersecretary of Defense for Acquisition and Sustainment Memorandum "Guidance for Assessing Compliance and Enhancing Protections Required by DFARS Clause 252.204.7012, Safeguarding Covered Defense Information and Cyber Incident Reporting," November 8, 2018.

~~(CUI)~~ Representative for the Navy (Contractors A, B, C, and G) stated that he only meets with contractors to verify that they have policies in place for protecting sensitive information. However, just meeting with contractors is not sufficient for enforcing NIST SP 800-171 requirements.

(U) On September 29, 2020, the DPC Principal Director implemented interim DFARS Rule 2019-D041, "Assessing Contractor Implementation of Cybersecurity Requirements," which requires DoD Component contracting officers to verify contractor implementation of the cybersecurity requirements in NIST SP 800-171. The DPC Principal Director implemented the interim rule in response to Report No. DODIG-2019-105, "Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems," July 23, 2019, where we recommended that the DPC Principal Director require DoD Component contracting officers to assess whether contractors were complying with NIST SP 800-171 cybersecurity requirements for protecting CUI during the period of performance.[20] The DPC Acting Principal Director agreed, stating that the DPC would require offerors to submit documentation when responding to Requests for Proposal that explains how they will implement NIST SP 800-171 security requirements. The Acting Principal Director also stated that the DPC would revise DoD policy and develop a risk-based process to assess contractor compliance with NIST SP 800-171 requirements.

> *(U) As written, when the interim rule is finalized, DoD Component contracting officers will not be required to assess and verify NIST SP 800-171 cybersecurity compliance for contracts in place before November 30, 2020.*

(U) However, the interim rule only applies to new DoD contracts, task orders, delivery orders, or modified contracts that extend the period of performance as of November 30, 2020, and does not apply to existing contracts, including the contracts that we reviewed during the audit.[21] As written, when the interim rule is finalized, DoD Component contracting officers will not be required to assess and verify NIST SP 800-171 cybersecurity compliance for contracts in place before November 30, 2020.

~~(CUI)~~ In November 2019, the DoD implemented the NIST SP 800-171 DoD Assessment Methodology process for strategically assessing a contractor's implementation of NIST SP 800-171 on existing contracts that include DFARS clause 252.204-7012. The 10 contractors we assessed conducted self-assessments

[20] (U) Report No. DODIG-2019-105, "Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems," July 23, 2019.

[21] (U) DFARS Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041), September 29, 2020.

~~(CUI)~~ of their compliance with NIST SP 800-171, but 4 of the 10 contracting officers did not request system security plans from the contractors. In addition, the DoD did not verify that 8 of the 10 contractors implemented the NIST SP 800-171 security requirements.[22] We reviewed the self-assessments and determined that 3 of the 10 contractors' self-assessment scores indicated that [redacted] of the required 110 security controls were implemented. Specifically:

- ~~(CUI//NF)~~ Contractor A had a self-assessment score of [redacted] out of 110 as of December 2020;
- ~~(CUI//NF)~~ Contractor C had a self-assessment score of [redacted] out of 110 as of March 2020; and
- ~~(CUI//NF)~~ Contractor D had a self-assessment score of [redacted] out of 110 as of June 2021.

~~(CUI)~~ Self-assessment scores for another five contractors—Contractors E, F, G, I, and J—were all over [redacted]; however, we identified problems with the contractors' implementation of the security controls that we assessed (see Table 2). Relying on the results of a contractor's self-assessment is not an effective method for determining compliance with NIST SP 800-171 security requirements.

(U) To enhance the cybersecurity of its contractors, the DoD is implementing the Cybersecurity Maturity Model Certification program, which will require that independent, DoD-approved third-party organizations verify that DoD contractors who handle DoD CUI meet specific cybersecurity requirements.[23] However, the DoD will not fully implement the Cybersecurity Maturity Model Certification until at least FY 2025. Therefore, it is critical that in the interim DoD contracting officers use their authority as outlined in the NIST SP 800-171 DoD Assessment Methodology to **independently** [emphasis added] assess, based on risk, and verify whether academic and research institutions comply with NIST SP 800-171 requirements for protecting CUI.

[22] (U) The NIST SP 800-171 DoD Assessment Methodology allows contracting officers to require a medium or high assessment. A medium assessment consists of a DoD review of the contractor's system security plan that describes how the contractor meets each NIST requirement. A high assessment consists of on-site or virtual verification of the contractors' implementation of the NIST SP 800-171.

[23] (U) The Cybersecurity Maturity Model Certification program enhances cyber protection standards for companies in the Defense Industrial Base. It is designed to protect sensitive unclassified information that is shared by the Department with its contractors and subcontractors. The program incorporates a set of cybersecurity requirements into acquisition programs and provides the Department increased assurance that contractors and subcontractors are meeting these requirements.

(U) DoD Research Data and Technologies Could Be Compromised by Cyberattacks

~~(CUI//NF)~~ Academic and research contractors use CUI for research in support of the DoD's long-term goals to improve operations and enhance national security, including cybersecurity. Security measures, such as multifactor authentication, vulnerability management, data encryption, monitoring and scanning networks for viruses, and locking and disabling inactive user accounts decrease the risk of unauthorized access to CUI. In addition, [redacted], reduce the capability of insiders to intentionally compromise networks and systems that contain CUI. Furthermore, documenting and testing incident response plans ensures contractors are able to detect and respond to cyberattacks. Academic and research contractors that do not implement security controls to protect CUI risk disclosing critical details of DoD programs to U.S. adversaries.

(U) According to Executive Order 14028, "Improving the Nation's Cybersecurity," the United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy.[24] To maintain their cybersecurity posture, academic and research contractors should implement basic cyber hygiene practices, which includes regularly patching known vulnerabilities. Without a thorough and systematic process to identify and mitigate vulnerabilities in a timely manner, academic and research contractors increase the risk that cyberattacks or other malicious actions could exploit unmitigated vulnerabilities. As a result, CUI that supports critical DoD programs could be compromised through cyberattacks that are designed to exploit those weaknesses.

(U) Malicious actors can exploit vulnerabilities on the networks and systems of academic and research contractors and steal information related to some of the Nation's most valuable advanced defense technologies.

(U) When academic and research contractors do not fully implement the security controls outlined in NIST SP 800-171, and DoD Component contracting officers do not monitor contractor compliance with these controls, there is an increased risk that academic and research contractors performing work on behalf of the DoD could become victims of cyberattacks. Malicious actors can exploit vulnerabilities on the networks and systems of academic and research contractors and steal information related

[24] (U) Executive Order 14028, "Improving the Nation's Cybersecurity," May 12, 2021.

(U) to some of the Nation's most valuable advanced defense technologies. If the DoD does not verify that all contractors using CUI implement NIST SP 800-171 requirements, regardless of when the contract was awarded or modified, there is an increased risk that DoD CUI related to national security could fall into the hands of our adversaries.

(U) Management Comments on the Finding and Our Response

(U) The Naval Sea Systems Command (NAVSEA) Inspector General, Air Force Materiel Command (AFMC) Deputy Commander, and the Defense Research and Engineering for Research and Technology (DDR&E (R&T)) Acting Director provided the following comments on the Finding. For the full text of these comments, see the Management Comments section of the report.

(U) Naval Sea Systems Command Inspector General Comments

(U) The NAVSEA Inspector General, responding for the NAVSEA Commander, stated that there were instances in the audit report that implied technical controls are required to protect CUI on removable media. The NAVSEA Inspector General stated that he does not believe that technical controls are required by NIST SP 800-171, as long as the intent of the Media Protection control (Control 3.8) is satisfied. The NAVSEA Inspector General acknowledged that technical controls may be necessary in addition to non-technical controls to achieve adequate protection of removable media. However, he also stated that a specific contractor's situation should be considered when requiring technical controls and that it should not be implied that NIST SP 800-171 requires technical controls.

~~(CUI//NF)~~ The NAVSEA Inspector General stated that NAVSEA endorses the contractors approach to monitor and track the movement of personnel to include requiring key card access, entering a personal identification number to access restricted spaces, providing visitor escorts for unauthorized personnel, and using [redacted]. The NAVSEA Inspector General also stated that NAVSEA does not believe that [redacted] are required by NIST SP 800-171 and that the audit report mischaracterized the NAVSEA Facility Security Officer's knowledge of NIST SP 800-171 requirements. Specifically, he stated that the Field Security Officer was aware that [redacted] in NIST SP 800-171.

(U) Our Response

(U) NIST SP 800-171 states that organizations can employ technical and nontechnical controls to control the use of removable media. Nontechnical controls, such as policy and training, set the expectations for compliance; however, technical controls establish physical and logical barriers to prevent malicious actors from circumventing the nontechnical controls. While Contractor B developed policy that required users to manually encrypt CUI on removable media, the contractor did not enforce the policy. Implementing technical controls, such as the automatic encryption of data copied to removable media, will protect DoD CUI whether or not Contractor B personnel comply with the removable media policy.

~~(CUI//NF)~~ We did not suggest to Contractor B's Field Security Office that [redacted] were required by NIST SP 800-171, but stated that NIST SP 800-171 recommends [redacted] as a means of applying layered physical security protection throughout a facility. Contractor B required personnel to [redacted]. However, the contractor did not require [redacted], which provides an opportunity for [redacted] A [redacted] would provide a means for security personnel to [redacted].

(U) Air Force Materiel Command Deputy Commander Comments

(U) The Air Force Materiel Command Deputy Commander stated that there is no formal policy for DoD Components to validate security requirements within the Defense Industrial Base. The Deputy Commander recommended that we amend the final report to acknowledge the lack of policy, and that the Defense Contract Management Agency and the Defense Counterintelligence and Security Agency should take the necessary steps to publish or update existing policy to address DoD Components' role for CUI oversight in the Defense Industrial Base.

(U) Our Response

(U) We agree that there is gap in policy. As stated in the report, DFARS Case 201-D041 requires DoD Component contracting officers to verify contractor implementation of the cybersecurity requirements in NIST SP 800-171, for contracts awarded after November 2020. As a result, we made a recommendation to the Principal Director, Defense Pricing and Contracting (Recommendation 1), who is responsible for all pricing, contracting, and procurement policy matters, to develop and implement a policy and process

(U) that requires DoD Component contracting officers to verify contractor compliance with NIST SP 800-171 cybersecurity requirements for protecting CUI for existing and ongoing contracts awarded before November 30, 2020.

(U) Defense Research and Engineering for Research and Technology Acting Director Comments

~~(CUI)~~ The Acting DDR&E (R&T) Director stated that DDR&E (R&T) provides oversight of [redacted], and requires that contractors properly implement DFARS clause 252.204-7012 in contracts incorporating covered defense information. The Acting Director also stated that the DoD engages [redacted] in fundamental research that does not include covered defense information. He stated that there is a difference between fundamental research and research on networks that store or generate covered defense information. The Acting Director also stated that each security requirement in the NIST SP 800-171 includes a discussion section that provides notional [hypothetical] examples and is not all-inclusive of potential options that are available to organizations. He also stated that contractors are expected to assess the implementation of NIST SP 800-171 using NIST SP 800-171A, "Assessing Security Requirements for Controlled Unclassified Information."[25]

(U) Our Response

(U) We agree that DFARS states that fundamental research does not include CUI. However, we verified with the contracting officers and the contractors that the contractors we assessed maintained DoD CUI on their networks. We also agree that the NIST SP 800-171 discussion sections are used to help organizations clarify or interpret the requirements in the context of mission and business requirements or assessment of risk. However, we considered the layered protections that are outlined for the security requirements throughout the NIST SP 800-171, and compared that with the controls and mitigating actions implemented by the contractor to determine whether the NIST SP 800-171 security requirements were met and determined that the 10 contractors that we assessed did not meet NIST SP 800-171 security requirements. Furthermore, we agree that the NIST SP 800-171A provides procedures for assessing the effectiveness of the safeguards implemented to meet the NIST SP 800-171 requirements. We independently assessed the security controls implemented by the contractors that we reviewed based on the NIST SP 800-171 and identified the security weaknesses discussed in this report.

[25] (U) NIST SP 800-171A, "Assessing Security Requirements for Controlled Unclassified Information," June 2018.

(U) Recommendations, Management Comments, and Our Response

(U) Redirected, Renumbered, and Revised Recommendations

(U) As a result of management comments, we revised Recommendation 1 to clarify that the DPC Principal Director should direct contracting officers to use their authority to assess contractor compliance as outlined in the NIST SP 800-171 DoD Assessment Methodology. The authority allows contracting officers to assess contractor compliance with NIST SP 800-171 cybersecurity requirements for protecting CUI for ongoing contracts awarded before November 30, 2020. We also redirected draft report Recommendation 4 from the Commander of the Naval Facilities Engineering Systems Command to the Commander of the Naval Sea Systems Command because the contract with Contractor G is managed by the Naval Sea Systems Command. We renumbered Recommendation 4 as Recommendation 3.d, Recommendation 5 as Recommendation 4, and Recommendation 6 as Recommendation 5.

(U) Recommendation 1

(U) We recommend that the Principal Director for Defense Pricing and Contracting direct contracting officers to use their authority as outlined in the NIST SP 800-171 DoD Assessment Methodology to assess contractor compliance with National Institute of Standards and Technology Special Publication 800-171 cybersecurity requirements for protecting controlled unclassified information for ongoing contracts awarded before November 30, 2020.

(U) Defense Pricing and Contracting Principal Director Comments

(U) The DPC Principal Director disagreed, stating that Federal Acquisition Regulation changes are generally applied "moving forward" instead of retroactively. The Principal Director stated that additional rulemaking and negotiations would be required to make the changes applicable to contracts awarded before November 30, 2020, and would cause substantial administrative and financial burden for the DoD. The Principal Director stated that the DPC reviewed the status of the 10 contractors assessed and determined that all have provided their self-assessment scores to the DoD, indicating that the contractors are subject to the terms of DFARS 252.204-7020, and the DoD has obtained the benefits intended by DFARS Case 2019-D041.[26]

[26] (U) DFARS Case 2019-D041 is an interim rule to amend the DFARS to implement a DoD Assessment Methodology and Cybersecurity Maturity Model Certification framework designed to assess contractor implementation of cybersecurity requirements and enhance the protection of CUI throughout the DoD supply chain.

(U) Our Response

(U) Comments from the Principal Director did not address the specifics of the recommendation; therefore, the recommendation is unresolved. Our recommendation was not intended to require additional rulemaking and negotiations; change existing contracts; or cause a substantive administrative and financial burden for the DoD. The recommendation was intended to ensure the DoD uses its existing authorities to assess contractor compliance with NIST SP 800-171. Solely relying on the results of a contractor's self-assessment is not an effective method for determining compliance with NIST SP 800-171 security requirements. The NIST SP 800-171 DoD Assessment Methodology allows the contracting officer to require medium and high assessments. A medium assessment consists of a DoD review of the contractor's system security plan that describes how each NIST requirement is met. A high assessment consists of on-site or virtual verification of the contractors' implementation of the NIST SP 800-171. The NIST SP 800-171 DoD Assessment Methodology requires that contractors conduct a self-assessment once every 3 years. The DoD also has the authority to conduct a medium or high assessment of the contractor, unless other factors, such as program risk or a security-relevant change, drive the need for a more frequent assessment. The contractor's low self-assessment scores and the security weaknesses identified in this report support the need for the DoD to conduct medium and high assessments to ensure that contractors are protecting DoD CUI as required by the DFARS clause.

(U) Therefore, we request that the Principal Director provide additional comments to the final report describing the methods in which contracting officers will use their authority as outlined in the NIST SP 800-171 DoD Assessment Methodology to conduct medium and high assessments of contractors' compliance with NIST SP 800-171 security requirements for contracts awarded before November 30, 2020.

(U) Recommendation 2

(U) We recommend that the Commanding General of the Army Contracting Command direct contracting officers to verify that Contractor J implements physical security controls to detect unauthorized access to contractor facilities.

(U) U.S. Army Contracting Command Commanding General Comments

~~(CUI)~~ The Commanding General of the Army Contracting Command agreed, stating that the contracting officer for Contractor J would verify that the contractor implemented physical security controls to detect unauthorized access to the contractor's facility by [redacted].

(U) Our Response

~~(CUI//NF)~~ Comments from the Commanding General addressed all specifics of the recommendation; therefore, the recommendation is resolved but will remain open. We will close the recommendation once the Commanding General provides documentation, such as a completed installation order, showing that Contractor J [redacted] or propose an alternative solution for implementing physical security controls that will detect unauthorized access to the contractor's facilities.

(U) Recommendation 3

(U) We recommend that the Commander of the Naval Sea Systems Command direct contracting officers to verify that:

a. (U) Contractor A develops plans of action and milestones for vulnerabilities that cannot be mitigated in a timely manner.

(U) Naval Sea Systems Command Inspector General Comments

~~(CUI//NF)~~ The NAVSEA Inspector General, responding for the NAVSEA Commander, agreed, stating that Contractor A was [redacted] connected to the network. He also stated that Contractor A formalized processes to assess and remediate vulnerabilities by identifying the level of risk associated with each vulnerability; setting milestones for vulnerabilities that cannot be remediated within the recommended timeframe; and tracking active vulnerabilities on a POA&M.

(U) Our Response

(U) Comments from the NAVSEA Inspector General addressed all specifics of the recommendation. We verified that Contractor A was tracking active vulnerabilities on POA&Ms by comparing the POA&Ms to vulnerability scan results provided after our site visit. Therefore, the recommendation is closed and no further comments are required.

b. **(U) Contractor B enforces multifactor authentication; disables user accounts after extended periods of inactivity; implements technical security controls to protect controlled unclassified information stored on removable media; and implements physical security controls.**

(U) Naval Sea Systems Command Inspector General Comments

~~(CUI//NF)~~ The NAVSEA Inspector General, responding for the NAVSEA Commander, agreed stating that Contractor B had developed a POA&M for fully implementing multifactor authentication by [redacted]. The NAVSEA Inspector General stated that NAVSEA will confirm that Contractor B implements multifactor authentication by [redacted].

~~(CUI//NF)~~ The NAVSEA Inspector General also stated that Contractor B performs [redacted] audits of account logon data and disables accounts [redacted]. He stated that NAVSEA will confirm that Contractor B implements a solution to [redacted] and updates its policy. In addition, he stated that Contractor B will implement automated controls for removable media by [redacted], and that NAVSEA will confirm Contractor B's compliance by [redacted].

~~(CUI//NF)~~ The NAVSEA Inspector General added that, while NAVSEA endorses Contractor B's approach to monitoring and tracking the movement of personnel entering workspaces that maintain CUI, Contractor B is [redacted] to increase protection. NAVSEA will confirm that Contractor B [redacted] at Contractor B's facility by [redacted].

(U) Our Response

~~(CUI//NF)~~ Comments from the NAVSEA Inspector General addressed all specifics of the recommendation; therefore, the recommendation is resolved but will remain open. We will close the recommendation once the NAVSEA Inspector General provides supporting documentation showing that the contracting officer verified the actions taken by Contractor B to implement multifactor authentication, [redacted], implement automated controls for removable media, and [redacted].

c. **(U) Contractor C enforces multifactor authentication; encrypts controlled unclassified information stored on workstations; and implements technical security controls to protect controlled unclassified information stored on removable media.**

(U) Naval Sea Systems Command Inspector General Comments

~~(CUI//NF)~~ The NAVSEA Inspector General, responding for the NAVSEA Commander, agreed, stating that Contractor C has enforced the use of multifactor authentication on [redacted] devices. He also stated that Contractor C has updated its CUI policy to require encryption of data at rest on workstations. The NAVSEA Inspector General stated that Contractor C delayed encryption for workstations and servers at its facility to prioritize encrypting workstations that were moved off-site to allow employees to work from home during the coronavirus disease–2019 pandemic. He stated that global supply chain shortages have also contributed to the delay. The NAVSEA Inspector General stated that, as of April 1, 2021, Contractor C's Controlled Information Policy required approved encryption for removable media with CUI. The Inspector General stated that NAVSEA will confirm that Contractor C fully implemented multifactor authentication, workstation encryption, and automated controls to encrypt removable media by [redacted].

(U) Our Response

(U) Comments from the NAVSEA Inspector General addressed all specifics of the recommendation; therefore, the recommendation is resolved but will remain open. We will close the recommendation once NAVSEA provides documentation showing that the contracting officer has verified the actions taken by Contractor C to implement multifactor authentication; encrypt CUI on workstations; and automate technical controls to protect CUI on removable media.

d. **(U) Contractor G implements technical security controls to protect controlled unclassified information stored on removable media.**

(U) Naval Sea Systems Command Inspector General Comments

~~(CUI//NF)~~ The NAVSEA Inspector General, responding for the NAVSEA Commander, agreed, stating that, in the fourth quarter of FY 2021, Contractor G began implementing technical controls for [redacted] and [redacted] to control the ability of individuals to use removable media on the systems. The NAVSEA Inspector General stated that in November 2021, after the draft report was issued, Contractor G provided the audit team with evidence that it had implemented technical controls to protect CUI stored on removable media.

~~(CUI//NF)~~ He also stated that NAVSEA had received and reviewed the information, and verified that Contractor G had implemented technical controls to protect CUI stored on removable media.

(U) Our Response

(U) Comments from the NAVSEA Inspector General addressed all specifics of the recommendation. We verified, through screenshots of group policy settings, that Contractor G had implemented technical security controls to protect CUI on removable media. Therefore, the recommendation is closed and no further comments are required.

(U) Recommendation 4

(U) We recommend that the Commander of the Air Force Research Laboratory direct contracting officers to verify that:

a. (U) Contractor F develops plans of action and milestones for vulnerabilities that cannot be mitigated in a timely manner; and disables user accounts after extended periods of inactivity.

(U) Air Force Research Laboratory Commander Comments

(U) The Air Force Research Laboratory (AFRL) Commander agreed, stating that, on June 24, 2021, the Contracting Officer for Contractor F incorporated a modification to the statement of work requiring the contractor to submit a system security plan and associated plan of action, which was reviewed by the contracting officer's technical representative and the AFRL's Cybersecurity team. The Commander also stated that the contract with Contractor F ended on September 30, 2021, but the AFRL will consider including a requirement that Contractor F provide its system security plan and associated plans of action in future contracts. In addition, the Commander stated that she plans to implement a process to assess program risk and determine whether similar actions are needed for future contracts.

(U) Our Response

(U) Comments from the AFRL Commander addressed all specifics of the recommendation. Because the contract ended on September 30, 2021, we cannot further validate the actions taken and; therefore, the recommendation is closed and no further comments are required.

b. **(U) Contractor H enforces multifactor authentication and develops an incident response plan.**

(U) Air Force Research Laboratory Comments

~~(CUI//NF)~~ The AFRL Commander agreed, stating that the AFRL had directed Contractor H to establish multifactor authentication and strong passwords to access networks that store CUI. The AFRL Commander stated that Contractor H is in the process of implementing additional measures for authenticating on-site access to servers containing CUI, with a planned completion date of [redacted]. She also stated that Contractor H had completed its incident response plan in October 2021.

(U) Our Response

(U) Comments from the AFRL Commander addressed all specifics of the recommendation; therefore, the recommendation is resolved but will remain open. We will close the recommendation once the AFRL Commander provides documentation, such as screenshots of group policy settings, showing that Contractor H implemented multifactor authentication for its networks and cloud environments that store CUI. We also request that the AFRL Commander provide copy of Contractor H's approved incident response plan.

(U) Recommendation 5

(U) We recommend that the Director of Defense Research and Engineering for Research and Technology direct contracting officers to verify that:

a. **(U) Contractor E implements technical security controls to protect controlled unclassified information stored on removable media.**

(U) Defense Research and Engineering for Research and Technology Acting Director Comments

(U) The DDR&E (R&T) Acting Director disagreed, stating that Contractor E implemented the NIST SP 800-171 security requirements for controlling the use of removable media on system components. The Acting Director stated that the DoD OIG finding focused on a particular implementation of the security requirement for controlling the use of removable media on system components instead of a range of implementations. He also stated that the audit finding combination of the security requirements related to administrative and automated controls is inappropriate, and does not support Recommendation 6.a.[27]

[27] (U) We renumbered Recommendation 6.a to 5.a.

(U) Our Response

(U) Although the Acting Director disagreed, action taken by Contractor E meets the intent of the recommendation. Specifically, Contractor E stated that, in response to the draft report, they disabled USB access on their workstations. Therefore, the recommendation is resolved but will remain open. We will close the recommendation once the Acting Director provides documentation, such as screenshots of group policy settings, verifying that Contractor E disabled USB access to workstations that contain CUI.

b. (U) Contractor I identifies and mitigates vulnerabilities and develops plans of action and milestones for vulnerabilities that cannot be mitigated in a timely manner; encrypts controlled unclassified information stored on workstations; and implements technical security controls to protect controlled unclassified information stored on removable media.

(U) Defense Research and Engineering for Research and Technology Acting Director Comments

(U) The DDR&E (R&T) Acting Director disagreed, stating that the NIST SP 800-171 security requirement on protecting the confidentiality of CUI at rest allows organizations to use different mechanisms to achieve confidentiality protections, including cryptographic mechanisms and file share scanning. The Acting Director stated that the NIST SP 800-171 allows organizations to use other controls such as secure off-line storage or continuous monitoring when protecting information at rest cannot otherwise be achieved. He also stated that encryption is not the only means to protect the confidentiality of CUI at rest. The Acting Director stated that the audit finding combination of the security requirements related to encrypting CUI on mobile devices and mobile computing platforms with a requirement to encrypt CUI on a physical workstation is inappropriate. In addition, the Acting Director stated that Contractor I implemented the NIST SP 800-171 security requirements for controlling the use of removable media on system components.

(U) Our Response

(U) Comments from the Acting Director did not address the specifics of the recommendation; therefore, the recommendation is unresolved. NIST SP 800-171 states that organizations should implement cryptographic mechanisms to prevent unauthorized disclosure of CUI on internal and external networks, and any system components that can transmit information, such as internal hard drives, servers, notebook computers, **desktop computers** [emphasis added],

(U) mobile devices, printers, copiers, scanners, and facsimile machines. While Contractor I relies on physical security controls, the controls were not sufficient to reduce insider threats. A malicious internal actor with authorized access could bypass the physical security measures in place, and steal or compromise the information that is stored on the machines. Applying layered protections give organizations the option of incorporating physical and technical controls to protect the DoD information stored on contractor networks. Therefore, we request that the Acting Director provide additional comments to the final report describing what actions DDR&E (R&T) plans to take to ensure contracting officers verify that Contractor I identifies and mitigates vulnerabilities, encrypts CUI stored on workstations, and implements technical security controls to protect CUI stored on removable media.

(U) Appendix A

(U) Scope and Methodology

(U) We conducted this performance audit from January 2021 through October 2021 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) To understand the process used to protect DoD research information, we interviewed officials from the:

- (U) Office of the Under Secretary of Defense for Research and Engineering;
- (U) Office of the Under Secretary of Defense for Acquisition and Sustainment; and
- (U) Protecting Critical Technology Task Force.

(U) We also interviewed information technology directors, information system security personnel, cybersecurity engineers, and physical security officers at select academic and research contractors to identify security protocols implemented to protect CUI stored on their networks. Additionally, we reviewed Federal laws and DoD policy concerning DFARS clause 252.204-7012 and NIST SP 800-171 requirements for security controls on non-DoD networks and systems to protect CUI. Furthermore, we interviewed DoD Component contracting officers and contracting officer's representatives to assess what oversight activities were performed to verify that contractors complied with DFARS clause 252.204-7012 and implemented NIST SP 800-171 requirements.

~~(CUI)~~ We selected a nonstatistical sample of 15 of 15,187 contracts awarded to conduct research on behalf of the DoD. Of the 15 contracts selected, we assessed 10 academic and research contractors to evaluate the security controls that were implemented to protect CUI. Of the 10 contractors that we assessed, [redacted] that conducted research on behalf of the DoD. We did not assess 5 of the 15 contracts because the contractors did not handle CUI, the contract period of performance ended during the audit, or the contractor was recently assessed during a previous DoD Office of Inspector General (DoD OIG) audit.[28] Therefore, we assessed a total of 10 academic and

[28] (U) Report No. DODIG-2019-105, "Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems," July 13, 2019.

~~(CUI)~~ research contractors, Contractors A through J, for this audit. Table 4 lists the 10 academic and research contractors we assessed, and the associated contracting agencies.

(U) Table 4. DoD Component Contracting Offices and Contractors Visited

DoD Component Contracting Offices	Contractor
(U) Department of the Navy	Contractor A
(U) Department of the Navy	Contractor B
(U) Department of the Navy	Contractor C
(U) Department of the Army	Contractor D
(U) Under Secretary of Defense for Research and Engineering[1]	Contractor E
(U) Department of the Air Force	Contractor F
(U) Department of the Navy	Contractor G
(U) Department of the Air Force	Contractor H
(U) Under Secretary of Defense for Research and Engineering[2]	Contractor I
(U) Department of the Army	Contractor J

[1] (U) This contract is managed by the Department of the Army, Communications-Electronics Command, Office of Acquisition Support.

[2] (U) This contract is managed by the Air Force Life Cycle Management Center.

(U) Source: The DoD OIG.

(U) To determine whether the academic and research contractors implemented cybersecurity controls to protect CUI, we:

- (U) virtually observed a demonstrations of how users authenticated to networks and systems with CUI using multifactor authentication;
- (U) obtained screenshots of the academic and research contractors' authentication settings;
- (U) obtained network vulnerability scan results and compared the timeframes in which scans were performed to each academic and research contractor's respective internal policy;
- (U) virtually observed network settings to verify that network administrators configured group policies in accordance with NIST SP 800-171;
- (U) compared lists of active users from an active directory with lists of personnel who no longer needed access to networks and systems to identify any active accounts that should have been disabled; and
- (U) virtually observed configuration settings to limit the use of removable media.

(U) Initially, we planned to review controls for preventing access to CUI by unauthorized foreign nationals. However, on February 2, 2021, the Government Accountability Office (GAO) initiated engagement 104362, "Safeguarding Sensitive U.S. University Research from Transfer to China." Therefore, we did not assess the controls in place regarding foreign nationals' access to CUI.

(U) This report was reviewed by the DoD 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 DoD CUI program. In preparing and marking this report, we considered any comments submitted by the DoD Components about the CUI treatment of their information. If the DoD 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.

(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 control environment related to:

- (U) physical protection of CUI;
- (U) removable media;
- (U) use of encryption for data stored on systems (at rest) and data transmitted across the network (in transit);
- (U) system access and authentication;
- (U) incident response;
- (U) risk assessments;
- (U) audit logging; and
- (U) network protection.

(U) 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

~~(CUI)~~ We used computer-processed data that was extracted from the Federal Procurement Database System (FPDS) to develop a universe of active contracts with academic and research contractors. We conducted a keyword search in FPDS to identify contracts with the following keywords mentioned in the contract: [redacted].

~~(CUI)~~ Based on the information extracted from FPDS, the DoD Component contracting offices verified the accuracy of their list of contracts with academic and research contractors. We used the information from FPDS and DoD Component contracting offices to develop our universe of active contracts with academic and research contractors. To assess the reliability of the data, we contacted the contracting offices of the 15 contracts we selected in our nonstatistical sample to verify that the contractor maintained CUI on its networks and systems as part of the identified contract. Of the 15 contracts we selected, five contractors did not handle CUI, the contract period of performance ended during the audit, or the contractor was recently assessed during a previous DoD OIG audit.

(U) We also used computer-processed data that was extracted from the networks and systems active directories maintained by the contractors that we assessed to develop a universe of active user accounts. We used the list of accounts from the active directories to select a nonstatistical sample of up to 44 users to determine whether users were authorized and trained to access the contractor's networks and systems. We also compared the list of accounts from the active directories to a list of users who no longer needed access to the contractor networks and systems to verify that inactive or unused user accounts were removed in a timely manner.

(U) Use of Technical Assistance

(U) The DoD OIG Quantitative Methods Division provided assistance in developing the nonstatistical sampling methodology that we used to select the DoD contractors and compare network vulnerability scans.

(U) Prior Coverage

(U) During the last 5 years, the GAO and the DoD OIG issued three reports discussing the protection of DoD information maintained on contractor networks and systems. Unrestricted GAO reports can be accessed at http://www.gao.gov. Unrestricted DoD OIG reports can be accessed at http://www.dodig.mil/reports.html/.

(U) GAO

(U) GAO-18-407, "Protecting Classified Information: Defense Security Service Should Address Challenges as New Approach is Piloted," May 14, 2018

> (U) The Defense Security Service (DSS) upgraded its capabilities but faced challenges in administering the National Industrial Security Program, which applies to all Executive Branch departments and agencies. The program was established to safeguard Government classified information that current or prospective contractors may access. Although the DSS was formulating a new approach to improve its capabilities, the GAO determined that the DSS had not addressed immediate challenges that are critical to piloting its new approach. Specifically, the GAO found it was unclear how the DSS would determine what resources it needed as it had not identified its roles and responsibilities. Moreover, the DSS had not established how it would collaborate with stakeholders—Government contracting activities, the Government intelligence community, other Government agencies, and contractors—under the new approach.

(U) DoD OIG

(U) DODIG-2019-105, "Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems," July 23, 2019

> (U) The DoD OIG determined that DoD contractors did not consistently implement DoD-mandated system security controls for safeguarding DoD information. In addition, DoD Component contracting offices and requiring activities did not verify that contractors' networks and systems met security requirements or that contractors implemented minimum security controls for protecting CUI. Furthermore, DoD Component contracting offices and requiring activities did not implement processes and procedures to track which contractors maintain CUI on contractor-owned networks and systems.

(U) DODIG-2018-094, "Logical and Physical Access Controls at Missile Defense Agency Contractor Locations," March 29, 2018

> (U) The DoD OIG determined that Missile Defense Agency contractors did not consistently implement security controls and processes to protect classified and unclassified ballistic missile defense system technical information. Specifically, system and network administrators at three contractors that managed ballistic missile defense system technical information on classified networks did not identify and mitigate vulnerabilities on their networks and systems. In addition, two contractors did not conduct risk assessments associated with

(U) systems that contained classified ballistic missile defense system technical information. Furthermore, the system and network administrators of the seven contractors that managed ballistic missile defense system technical information on their unclassified networks did not consistently implement system security controls in accordance with DoD requirements for safeguarding DoD information.

(U) Appendix B

(U) Sampling Approach

(U) The audit used two different sampling approaches – one to select a sample of contractors and DoD Component contracting offices to assess what oversight activities contracting officer are performing to ensure academic or research contractors implemented NIST 800-171 security controls, and another to select a sample of users at each assessed contractor, to test system access and privileges. The audit team used nonstatistical sampling to ensure representation of different contractors across the population of active DoD contracts.

~~(CUI)~~ The audit team obtained a list from the FPDS of 1,928 DoD contracts for academic and research contractors. To obtain the list of contracts, the audit team generated an FPDS report that included the [redacted] [redacted], and had an estimated completion date after September 30, 2021.[29] The team corroborated this listing with DoD Component contracting offices, and identified a universe of 15,187 contracts. The following 17 DoD Components had contracts included in the sample universe.

- (U) Department of the Army
- (U) Department of the Navy
- (U) Department of the Air Force
- (U) Office of the Under Secretary of Defense for Research and Engineering
- (U) Office of the Under Secretary of Defense for Acquisition and Sustainment
- (U) U.S. Cyber Command
- (U) U.S. Special Operations Command
- (U) U.S. Strategic Command
- (U) Defense Advanced Research Projects Agency
- (U) Defense Counterintelligence and Security Agency
- (U) Defense Health Agency
- (U) Defense Information Systems Agency

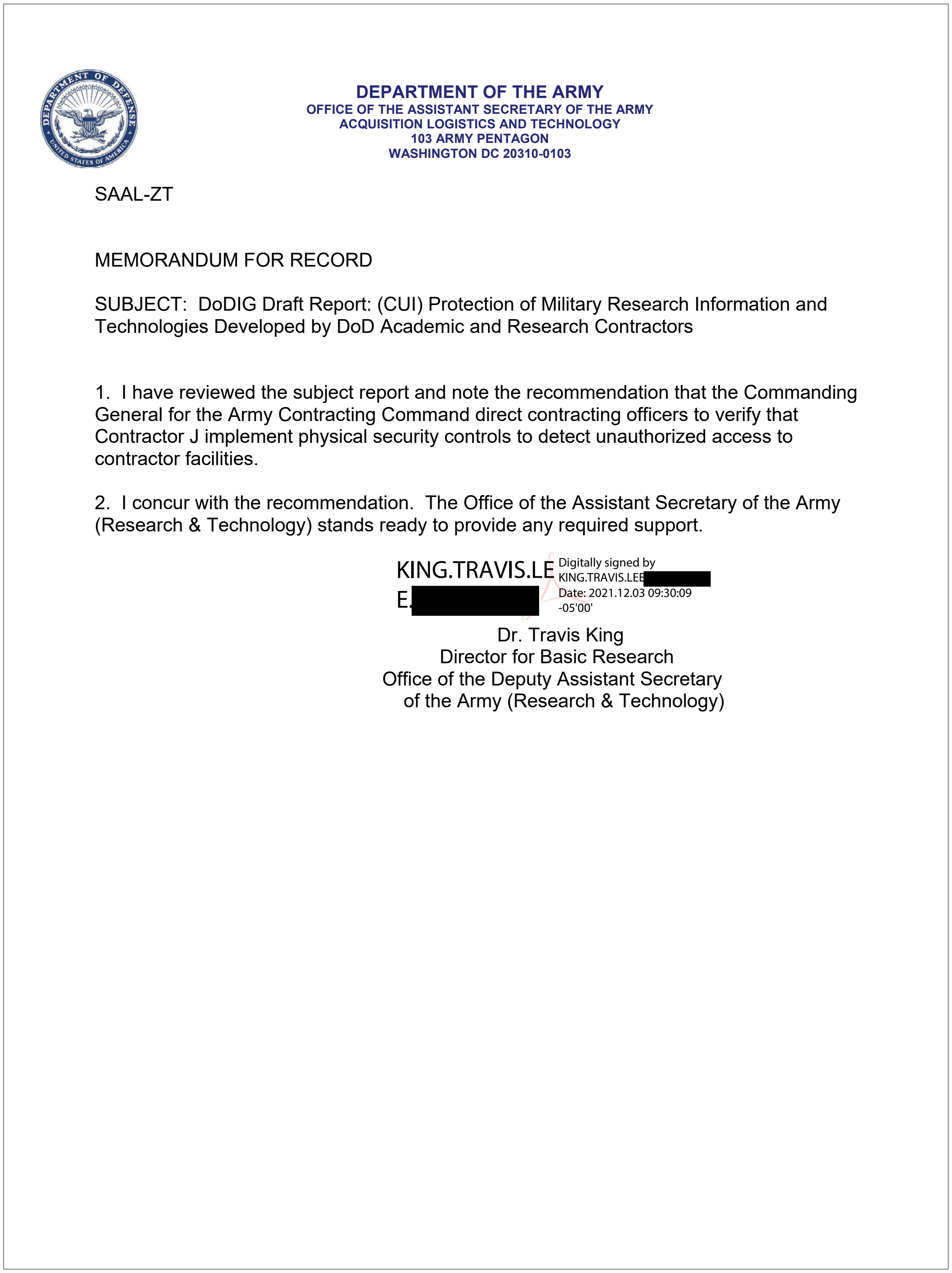
[29] (U) For the purposes of this report, research contractors are DoD contractors that conduct research for developing technologies to meet U.S. military requirements.

- (U) Defense Logistics Agency
- (U) Defense Threat Reduction Agency
- (U) Missile Defense Agency
- (U) Washington Headquarters Services
- (U) Uniformed Services University of the Health Sciences

(U) Management Comments

(U) Army

(U) Assistant Secretary of the Army (ALT)



DEPARTMENT OF THE ARMY
OFFICE OF THE ASSISTANT SECRETARY OF THE ARMY
ACQUISITION LOGISTICS AND TECHNOLOGY
103 ARMY PENTAGON
WASHINGTON DC 20310-0103

SAAL-ZT

MEMORANDUM FOR RECORD

SUBJECT: DoDIG Draft Report: (CUI) Protection of Military Research Information and Technologies Developed by DoD Academic and Research Contractors

1. I have reviewed the subject report and note the recommendation that the Commanding General for the Army Contracting Command direct contracting officers to verify that Contractor J implement physical security controls to detect unauthorized access to contractor facilities.

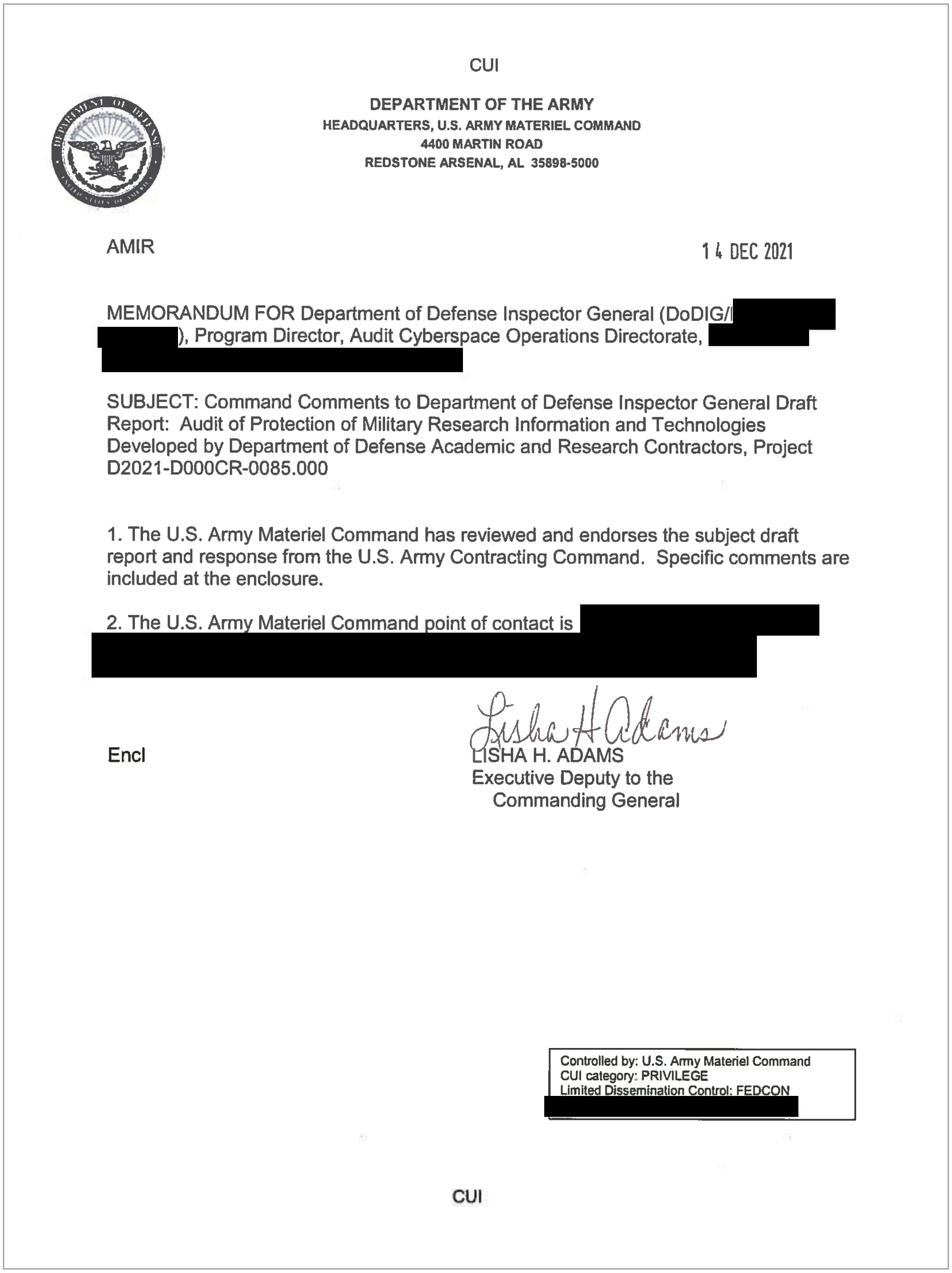
2. I concur with the recommendation. The Office of the Assistant Secretary of the Army (Research & Technology) stands ready to provide any required support.

KING.TRAVIS.LEE.[redacted]
Digitally signed by KING.TRAVIS.LEE[redacted]
Date: 2021.12.03 09:30:09 -05'00'

Dr. Travis King
Director for Basic Research
Office of the Deputy Assistant Secretary
of the Army (Research & Technology)

(U) Army (cont'd)

(U) Army Materiel Command



CUI

DEPARTMENT OF THE ARMY
HEADQUARTERS, U.S. ARMY MATERIEL COMMAND
4400 MARTIN ROAD
REDSTONE ARSENAL, AL 35898-5000

AMIR

14 DEC 2021

MEMORANDUM FOR Department of Defense Inspector General (DoDIG/[redacted]), Program Director, Audit Cyberspace Operations Directorate, [redacted]

SUBJECT: Command Comments to Department of Defense Inspector General Draft Report: Audit of Protection of Military Research Information and Technologies Developed by Department of Defense Academic and Research Contractors, Project D2021-D000CR-0085.000

1. The U.S. Army Materiel Command has reviewed and endorses the subject draft report and response from the U.S. Army Contracting Command. Specific comments are included at the enclosure.

2. The U.S. Army Materiel Command point of contact is [redacted]

Encl

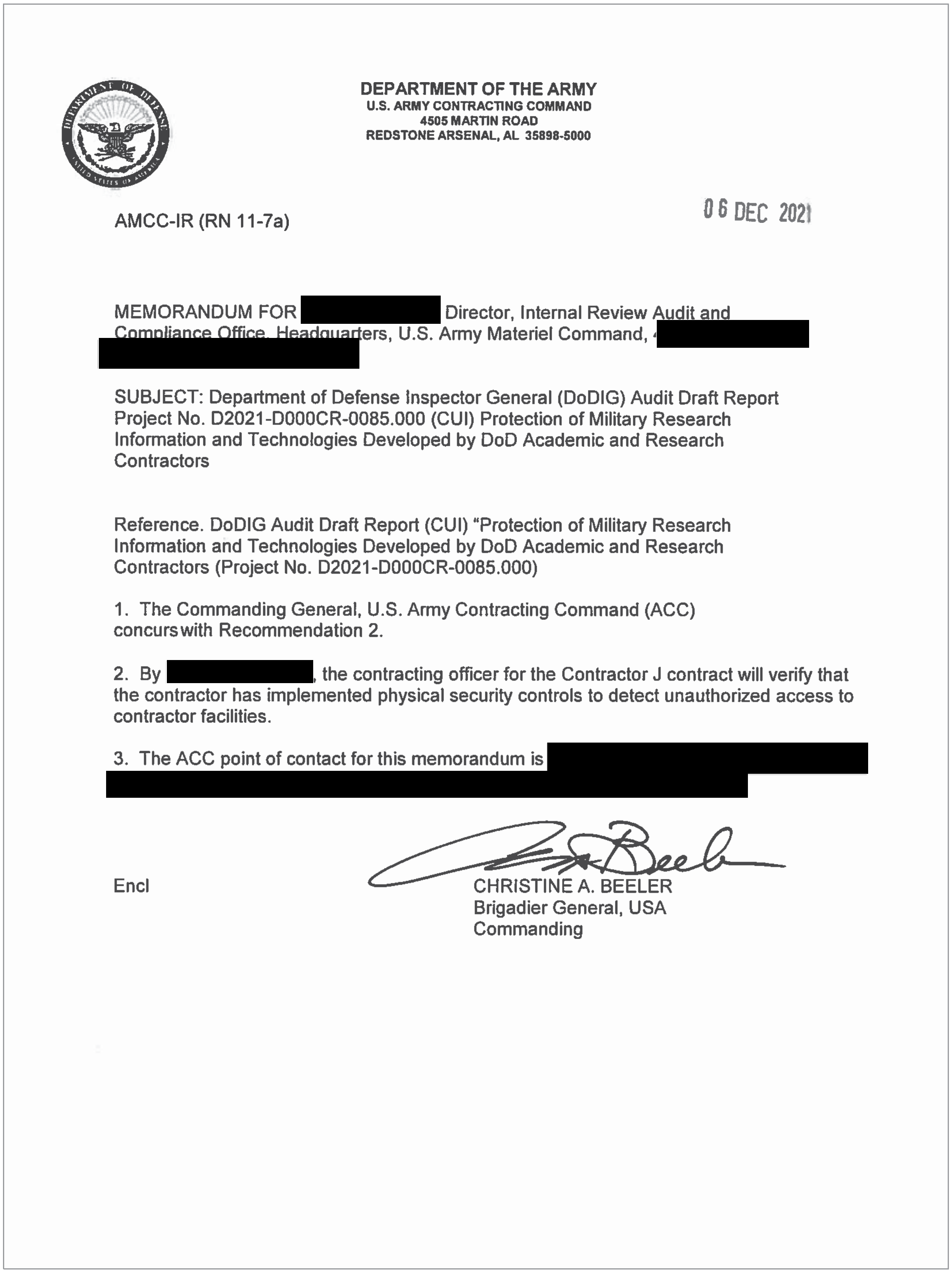
Lisha H Adams
LISHA H. ADAMS
Executive Deputy to the
Commanding General

Controlled by: U.S. Army Materiel Command
CUI category: PRIVILEGE
Limited Dissemination Control: FEDCON
[redacted]

CUI

(U) Army (cont'd)

(U) Army Contracting Command



DEPARTMENT OF THE ARMY
U.S. ARMY CONTRACTING COMMAND
4505 MARTIN ROAD
REDSTONE ARSENAL, AL 35898-5000

AMCC-IR (RN 11-7a)

06 DEC 2021

MEMORANDUM FOR [redacted] Director, Internal Review Audit and Compliance Office, Headquarters, U.S. Army Materiel Command, [redacted]

SUBJECT: Department of Defense Inspector General (DoDIG) Audit Draft Report Project No. D2021-D000CR-0085.000 (CUI) Protection of Military Research Information and Technologies Developed by DoD Academic and Research Contractors

Reference. DoDIG Audit Draft Report (CUI) "Protection of Military Research Information and Technologies Developed by DoD Academic and Research Contractors (Project No. D2021-D000CR-0085.000)

1. The Commanding General, U.S. Army Contracting Command (ACC) concurs with Recommendation 2.

2. By [redacted], the contracting officer for the Contractor J contract will verify that the contractor has implemented physical security controls to detect unauthorized access to contractor facilities.

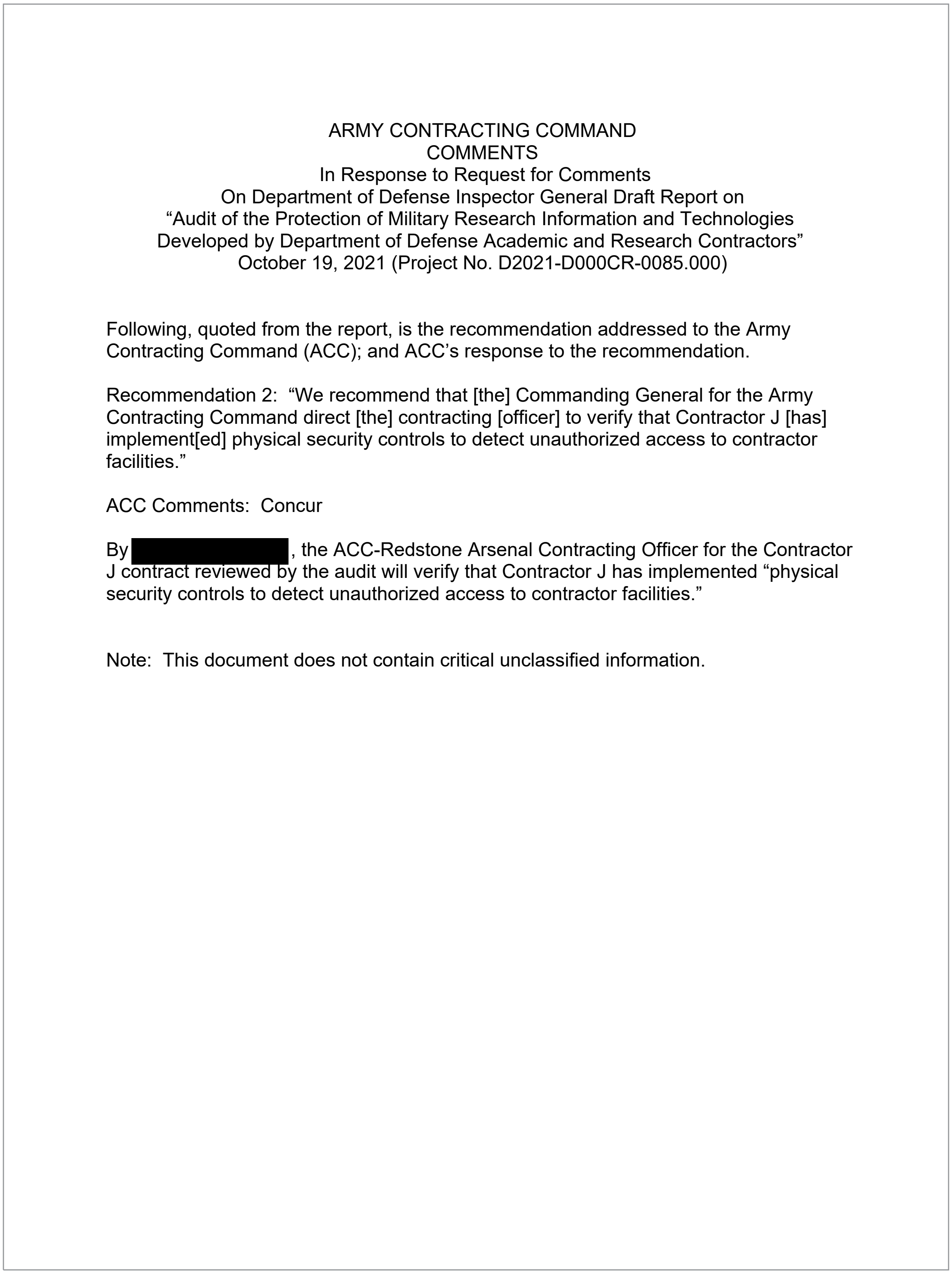
3. The ACC point of contact for this memorandum is [redacted]

Encl

CHRISTINE A. BEELER
Brigadier General, USA
Commanding

(U) Army (cont'd)

(U) Army Contracting Command (cont'd)



ARMY CONTRACTING COMMAND
COMMENTS
In Response to Request for Comments
On Department of Defense Inspector General Draft Report on
"Audit of the Protection of Military Research Information and Technologies
Developed by Department of Defense Academic and Research Contractors"
October 19, 2021 (Project No. D2021-D000CR-0085.000)

Following, quoted from the report, is the recommendation addressed to the Army Contracting Command (ACC); and ACC's response to the recommendation.

Recommendation 2: "We recommend that [the] Commanding General for the Army Contracting Command direct [the] contracting [officer] to verify that Contractor J [has] implement[ed] physical security controls to detect unauthorized access to contractor facilities."

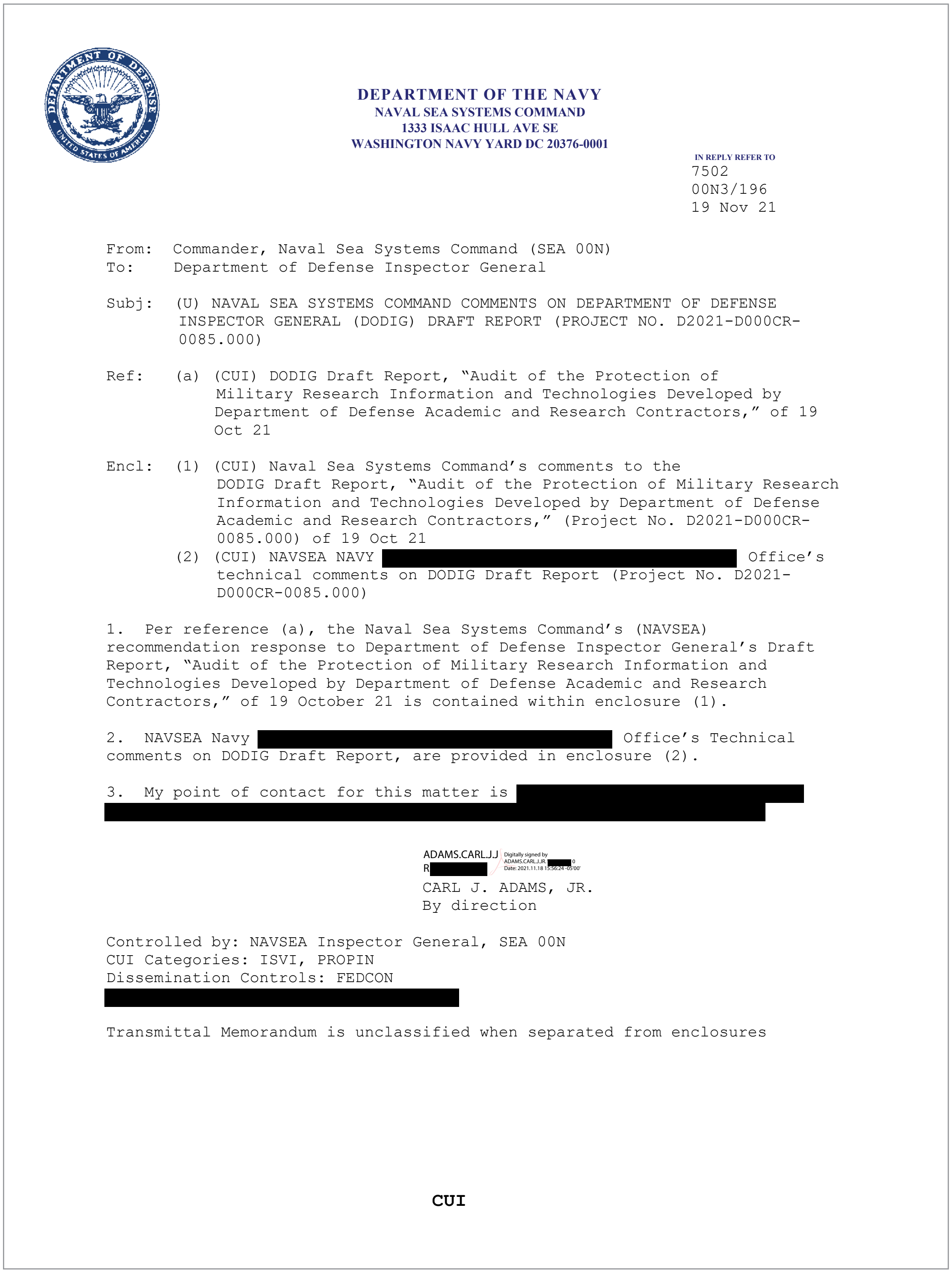
ACC Comments: Concur

By [redacted], the ACC-Redstone Arsenal Contracting Officer for the Contractor J contract reviewed by the audit will verify that Contractor J has implemented "physical security controls to detect unauthorized access to contractor facilities."

Note: This document does not contain critical unclassified information.

(U) Navy

(U) NAVSEA



DEPARTMENT OF THE NAVY
NAVAL SEA SYSTEMS COMMAND
1333 ISAAC HULL AVE SE
WASHINGTON NAVY YARD DC 20376-0001

IN REPLY REFER TO
7502
00N3/196
19 Nov 21

From: Commander, Naval Sea Systems Command (SEA 00N)
To: Department of Defense Inspector General

Subj: (U) NAVAL SEA SYSTEMS COMMAND COMMENTS ON DEPARTMENT OF DEFENSE INSPECTOR GENERAL (DODIG) DRAFT REPORT (PROJECT NO. D2021-D000CR-0085.000)

Ref: (a) (CUI) DODIG Draft Report, "Audit of the Protection of Military Research Information and Technologies Developed by Department of Defense Academic and Research Contractors," of 19 Oct 21

Encl: (1) (CUI) Naval Sea Systems Command's comments to the DODIG Draft Report, "Audit of the Protection of Military Research Information and Technologies Developed by Department of Defense Academic and Research Contractors," (Project No. D2021-D000CR-0085.000) of 19 Oct 21
(2) (CUI) NAVSEA NAVY [redacted] Office's technical comments on DODIG Draft Report (Project No. D2021-D000CR-0085.000)

1. Per reference (a), the Naval Sea Systems Command's (NAVSEA) recommendation response to Department of Defense Inspector General's Draft Report, "Audit of the Protection of Military Research Information and Technologies Developed by Department of Defense Academic and Research Contractors," of 19 October 21 is contained within enclosure (1).

2. NAVSEA Navy [redacted] Office's Technical comments on DODIG Draft Report, are provided in enclosure (2).

3. My point of contact for this matter is [redacted]

ADAMS.CARL.J.J
R[redacted]
Digitally signed by
ADAMS.CARL.J.JR.[redacted]0
Date: 2021.11.18 15:56:24 -05'00'

CARL J. ADAMS, JR.
By direction

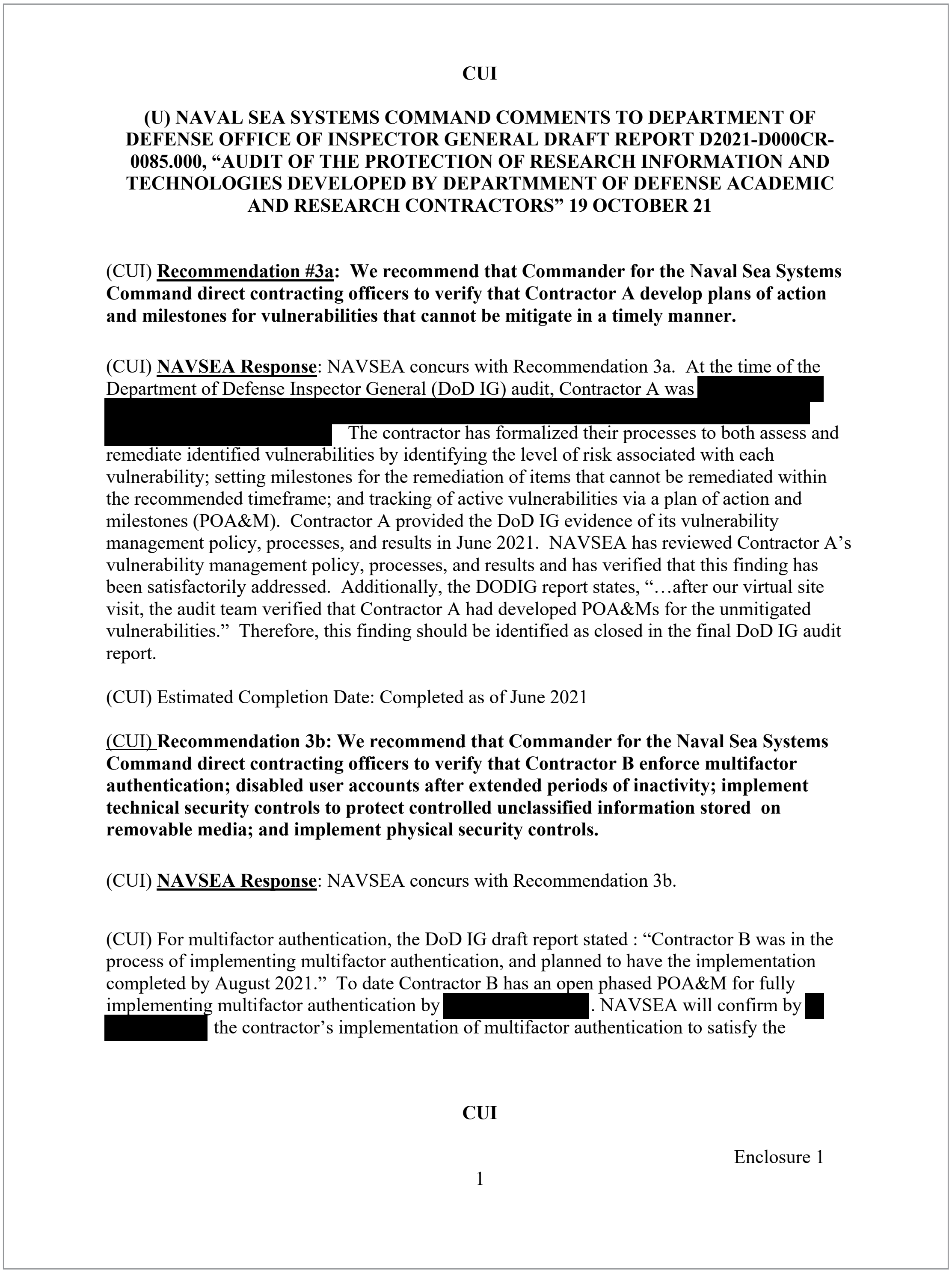
Controlled by: NAVSEA Inspector General, SEA 00N
CUI Categories: ISVI, PROPIN
Dissemination Controls: FEDCON
[redacted]

Transmittal Memorandum is unclassified when separated from enclosures

CUI

(U) Navy (cont’d)

(U) NAVSEA (cont’d)



CUI

(U) NAVAL SEA SYSTEMS COMMAND COMMENTS TO DEPARTMENT OF DEFENSE OFFICE OF INSPECTOR GENERAL DRAFT REPORT D2021-D000CR-0085.000, “AUDIT OF THE PROTECTION OF RESEARCH INFORMATION AND TECHNOLOGIES DEVELOPED BY DEPARTMMENT OF DEFENSE ACADEMIC AND RESEARCH CONTRACTORS” 19 OCTOBER 21

(CUI) **Recommendation #3a: We recommend that Commander for the Naval Sea Systems Command direct contracting officers to verify that Contractor A develop plans of action and milestones for vulnerabilities that cannot be mitigate in a timely manner.**

(CUI) **NAVSEA Response**: NAVSEA concurs with Recommendation 3a. At the time of the Department of Defense Inspector General (DoD IG) audit, Contractor A was [redacted] The contractor has formalized their processes to both assess and remediate identified vulnerabilities by identifying the level of risk associated with each vulnerability; setting milestones for the remediation of items that cannot be remediated within the recommended timeframe; and tracking of active vulnerabilities via a plan of action and milestones (POA&M). Contractor A provided the DoD IG evidence of its vulnerability management policy, processes, and results in June 2021. NAVSEA has reviewed Contractor A’s vulnerability management policy, processes, and results and has verified that this finding has been satisfactorily addressed. Additionally, the DODIG report states, “…after our virtual site visit, the audit team verified that Contractor A had developed POA&Ms for the unmitigated vulnerabilities.” Therefore, this finding should be identified as closed in the final DoD IG audit report.

(CUI) Estimated Completion Date: Completed as of June 2021

(CUI) **Recommendation 3b: We recommend that Commander for the Naval Sea Systems Command direct contracting officers to verify that Contractor B enforce multifactor authentication; disabled user accounts after extended periods of inactivity; implement technical security controls to protect controlled unclassified information stored on removable media; and implement physical security controls.**

(CUI) **NAVSEA Response**: NAVSEA concurs with Recommendation 3b.

(CUI) For multifactor authentication, the DoD IG draft report stated : “Contractor B was in the process of implementing multifactor authentication, and planned to have the implementation completed by August 2021.” To date Contractor B has an open phased POA&M for fully implementing multifactor authentication by [redacted]. NAVSEA will confirm by [redacted] the contractor’s implementation of multifactor authentication to satisfy the

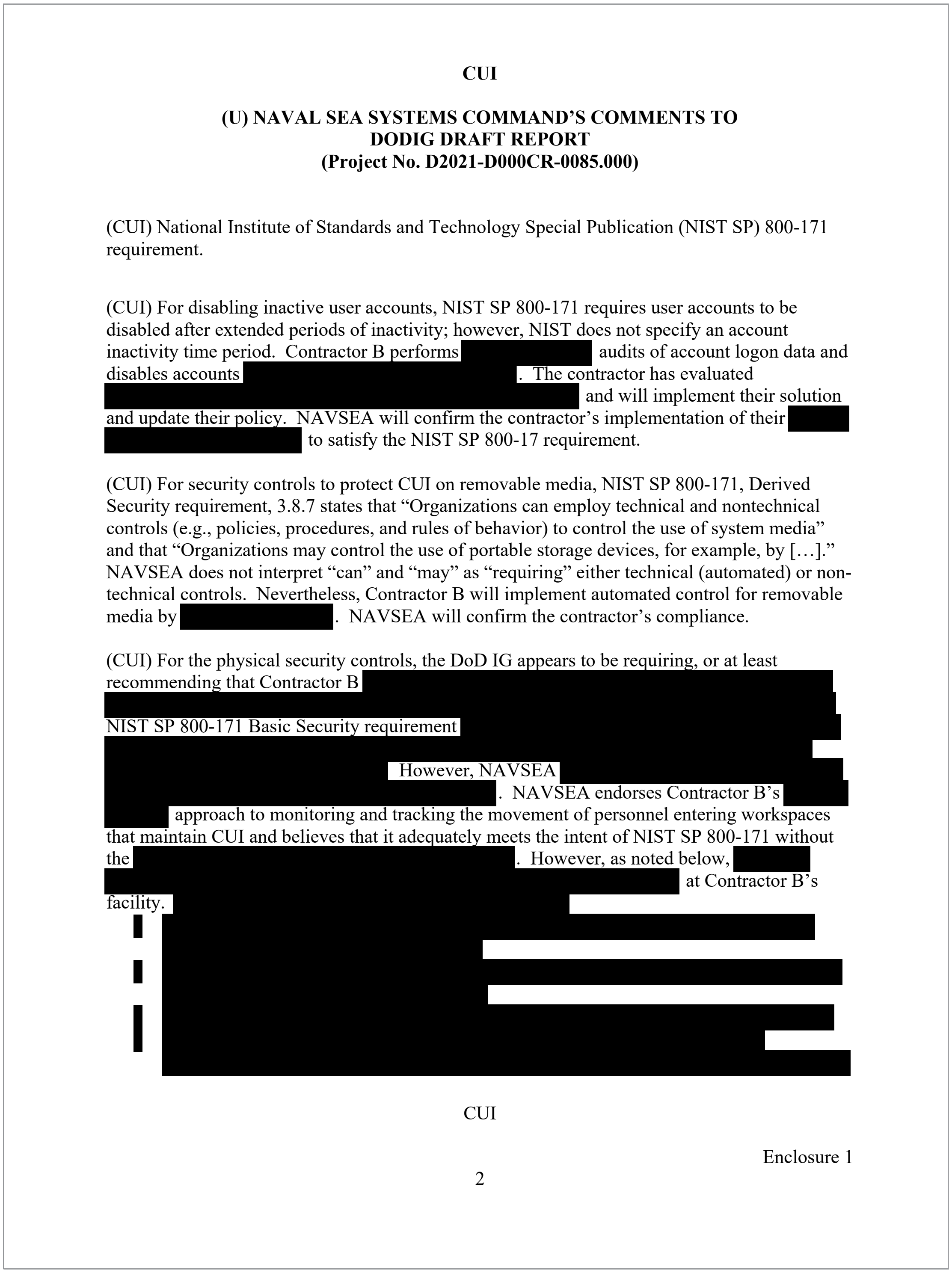
CUI

Enclosure 1

1

(U) Navy (cont'd)

(U) NAVSEA (cont'd)



CUI

(U) NAVAL SEA SYSTEMS COMMAND'S COMMENTS TO DODIG DRAFT REPORT (Project No. D2021-D000CR-0085.000)

(CUI) National Institute of Standards and Technology Special Publication (NIST SP) 800-171 requirement.

(CUI) For disabling inactive user accounts, NIST SP 800-171 requires user accounts to be disabled after extended periods of inactivity; however, NIST does not specify an account inactivity time period. Contractor B performs [redacted] audits of account logon data and disables accounts [redacted]. The contractor has evaluated [redacted] and will implement their solution and update their policy. NAVSEA will confirm the contractor's implementation of their [redacted] to satisfy the NIST SP 800-17 requirement.

(CUI) For security controls to protect CUI on removable media, NIST SP 800-171, Derived Security requirement, 3.8.7 states that "Organizations can employ technical and nontechnical controls (e.g., policies, procedures, and rules of behavior) to control the use of system media" and that "Organizations may control the use of portable storage devices, for example, by […]." NAVSEA does not interpret "can" and "may" as "requiring" either technical (automated) or non-technical controls. Nevertheless, Contractor B will implement automated control for removable media by [redacted]. NAVSEA will confirm the contractor's compliance.

(CUI) For the physical security controls, the DoD IG appears to be requiring, or at least recommending that Contractor B [redacted] NIST SP 800-171 Basic Security requirement [redacted] However, NAVSEA [redacted]. NAVSEA endorses Contractor B's [redacted] approach to monitoring and tracking the movement of personnel entering workspaces that maintain CUI and believes that it adequately meets the intent of NIST SP 800-171 without the [redacted]. However, as noted below, [redacted] at Contractor B's facility. [redacted]

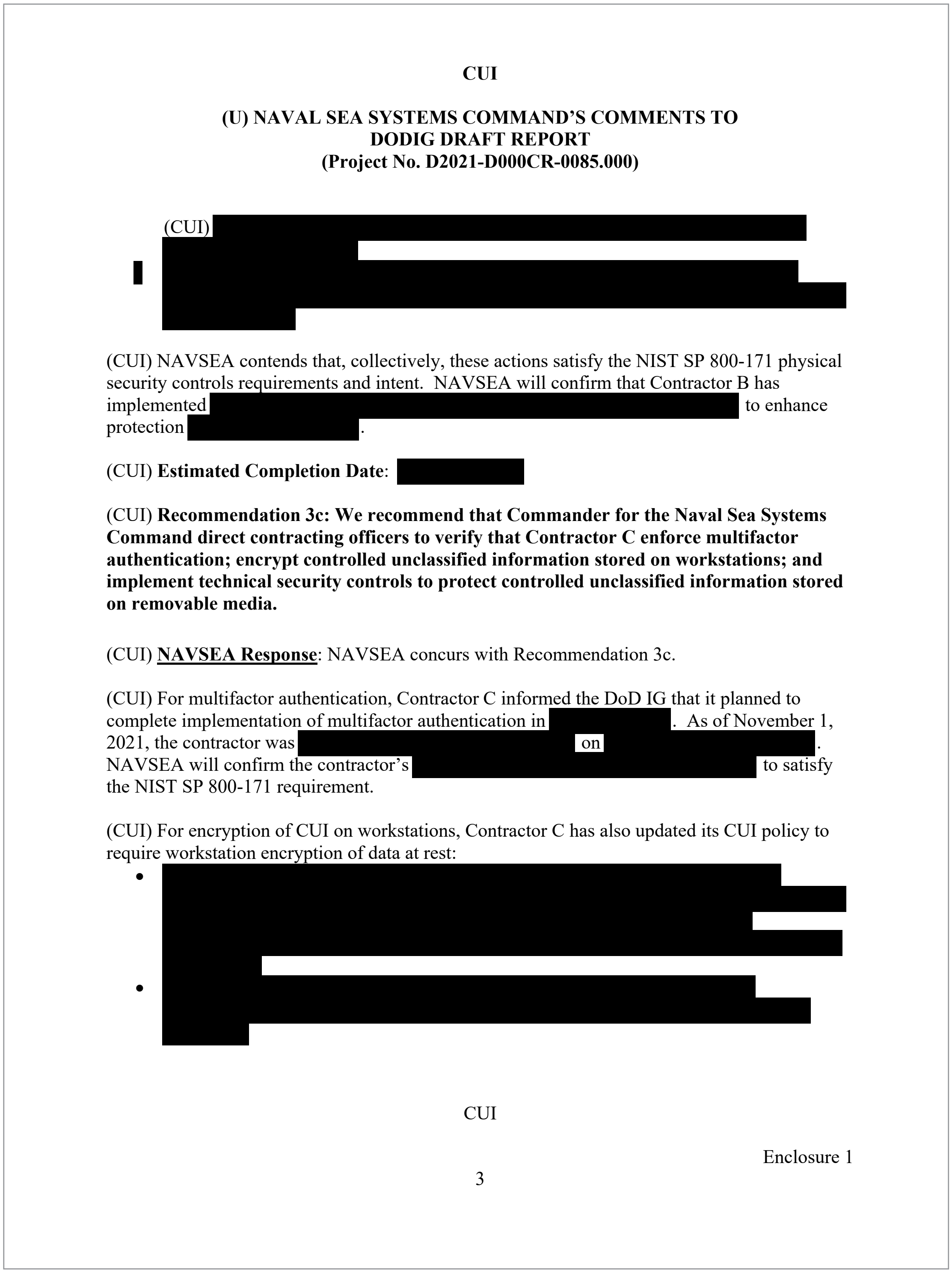
CUI

Enclosure 1

2

(U) Navy (cont'd)

(U) NAVSEA (cont'd)



CUI

(U) NAVAL SEA SYSTEMS COMMAND'S COMMENTS TO
DODIG DRAFT REPORT
(Project No. D2021-D000CR-0085.000)

(CUI) [redacted]

(CUI) NAVSEA contends that, collectively, these actions satisfy the NIST SP 800-171 physical security controls requirements and intent. NAVSEA will confirm that Contractor B has implemented [redacted] to enhance protection [redacted].

(CUI) **Estimated Completion Date**: [redacted]

(CUI) **Recommendation 3c: We recommend that Commander for the Naval Sea Systems Command direct contracting officers to verify that Contractor C enforce multifactor authentication; encrypt controlled unclassified information stored on workstations; and implement technical security controls to protect controlled unclassified information stored on removable media.**

(CUI) **NAVSEA Response**: NAVSEA concurs with Recommendation 3c.

(CUI) For multifactor authentication, Contractor C informed the DoD IG that it planned to complete implementation of multifactor authentication in [redacted]. As of November 1, 2021, the contractor was [redacted] on [redacted]. NAVSEA will confirm the contractor's [redacted] to satisfy the NIST SP 800-171 requirement.

(CUI) For encryption of CUI on workstations, Contractor C has also updated its CUI policy to require workstation encryption of data at rest:

- [redacted]
- [redacted]

CUI

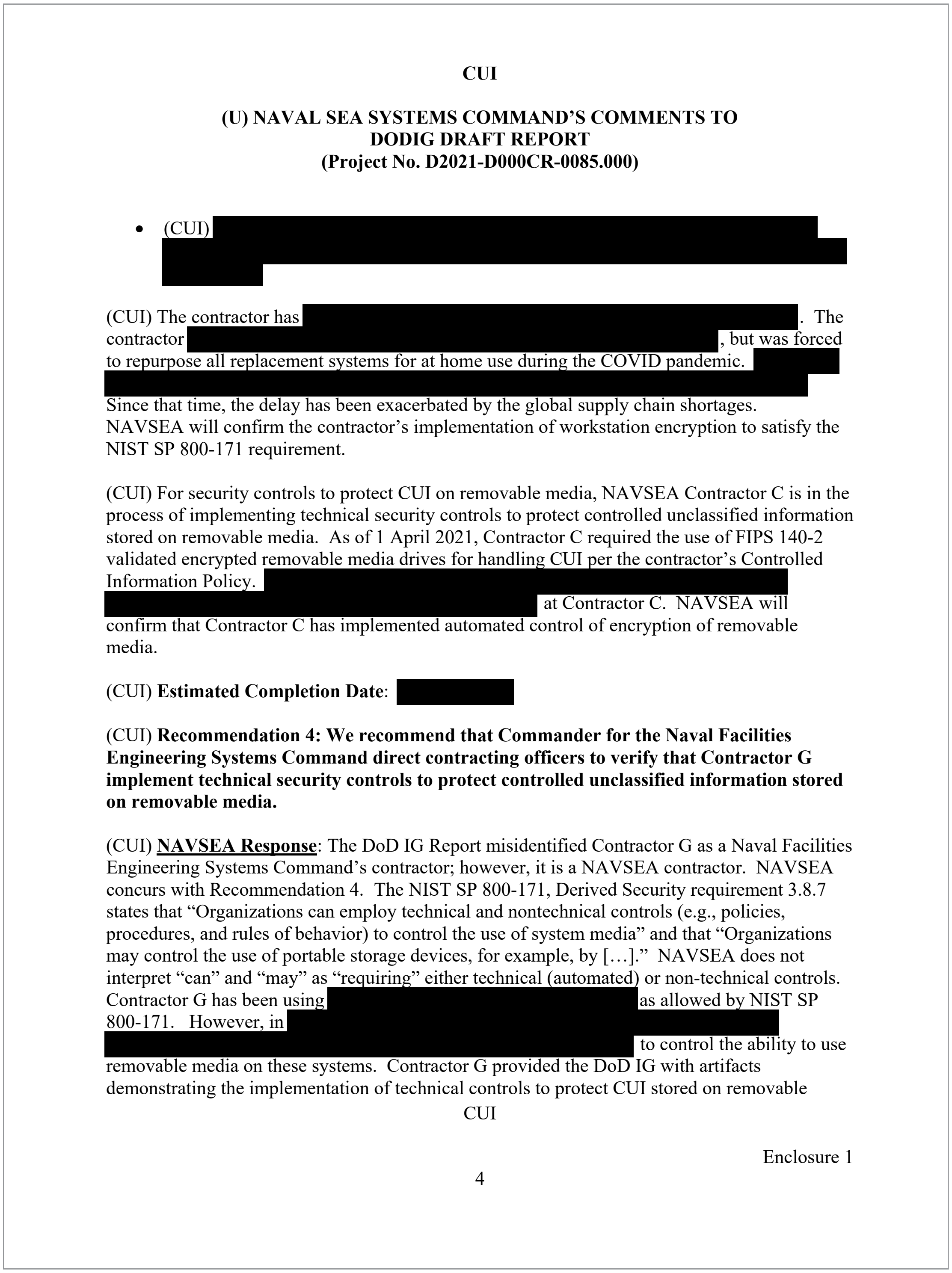
Enclosure 1

3

(U) Navy (cont'd)

(U) NAVSEA (cont'd)

Final
Report Reference



**(U) NAVAL SEA SYSTEMS COMMAND'S COMMENTS TO
DODIG DRAFT REPORT
(Project No. D2021-D000CR-0085.000)**

- (CUI) [redacted]

(CUI) The contractor has [redacted]. The contractor [redacted], but was forced to repurpose all replacement systems for at home use during the COVID pandemic. [redacted] Since that time, the delay has been exacerbated by the global supply chain shortages. NAVSEA will confirm the contractor's implementation of workstation encryption to satisfy the NIST SP 800-171 requirement.

(CUI) For security controls to protect CUI on removable media, NAVSEA Contractor C is in the process of implementing technical security controls to protect controlled unclassified information stored on removable media. As of 1 April 2021, Contractor C required the use of FIPS 140-2 validated encrypted removable media drives for handling CUI per the contractor's Controlled Information Policy. [redacted] at Contractor C. NAVSEA will confirm that Contractor C has implemented automated control of encryption of removable media.

(CUI) **Estimated Completion Date**: [redacted]

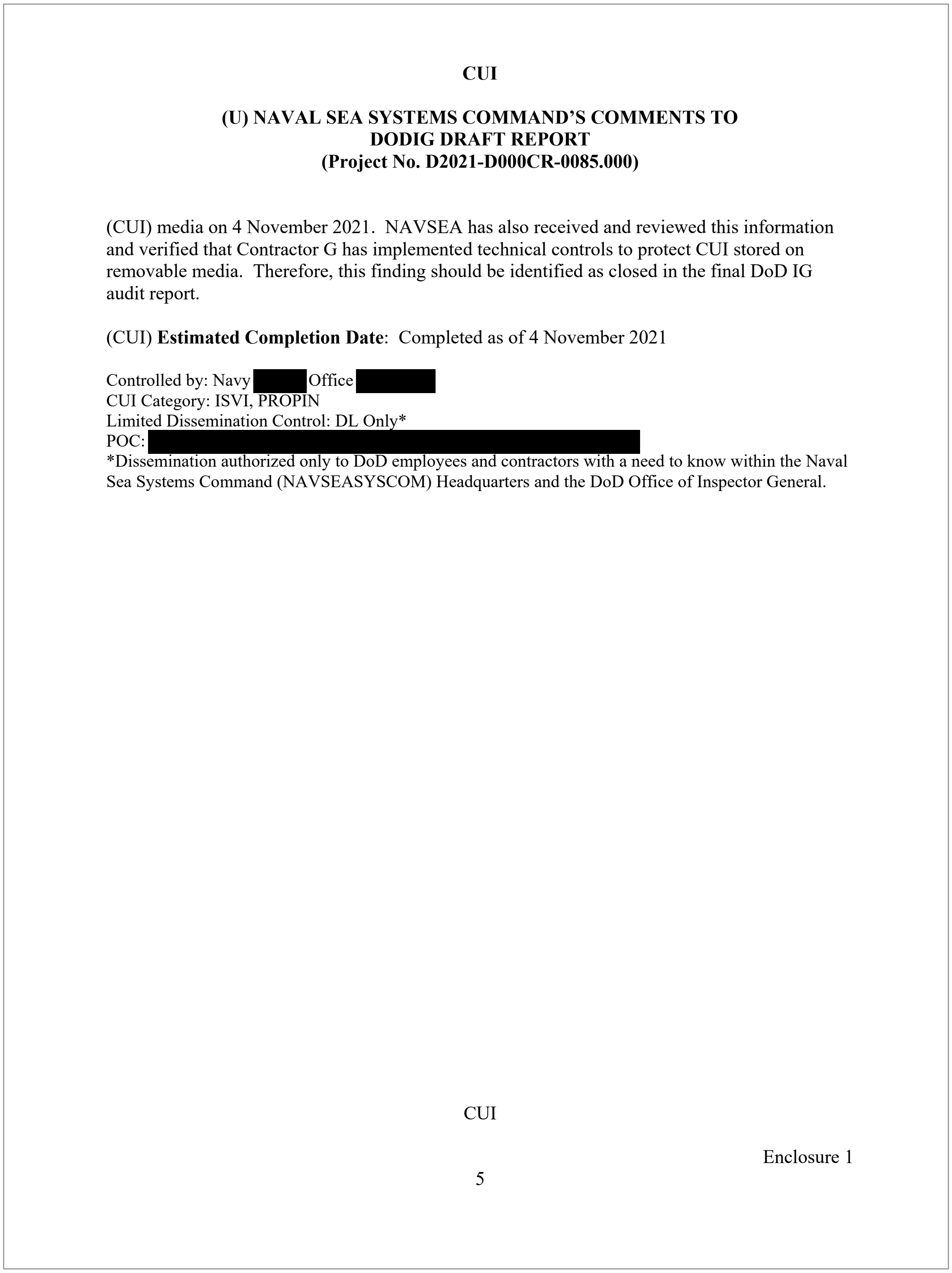
(CUI) **Recommendation 4: We recommend that Commander for the Naval Facilities Engineering Systems Command direct contracting officers to verify that Contractor G implement technical security controls to protect controlled unclassified information stored on removable media.**

Redirected and
Renumbered as
Recommendation 3.d

(CUI) **NAVSEA Response**: The DoD IG Report misidentified Contractor G as a Naval Facilities Engineering Systems Command's contractor; however, it is a NAVSEA contractor. NAVSEA concurs with Recommendation 4. The NIST SP 800-171, Derived Security requirement 3.8.7 states that "Organizations can employ technical and nontechnical controls (e.g., policies, procedures, and rules of behavior) to control the use of system media" and that "Organizations may control the use of portable storage devices, for example, by […]." NAVSEA does not interpret "can" and "may" as "requiring" either technical (automated) or non-technical controls. Contractor G has been using [redacted] as allowed by NIST SP 800-171. However, in [redacted] to control the ability to use removable media on these systems. Contractor G provided the DoD IG with artifacts demonstrating the implementation of technical controls to protect CUI stored on removable

(U) Navy (cont'd)

(U) NAVSEA (cont'd)



CUI

(U) NAVAL SEA SYSTEMS COMMAND'S COMMENTS TO DODIG DRAFT REPORT (Project No. D2021-D000CR-0085.000)

(CUI) media on 4 November 2021. NAVSEA has also received and reviewed this information and verified that Contractor G has implemented technical controls to protect CUI stored on removable media. Therefore, this finding should be identified as closed in the final DoD IG audit report.

(CUI) **Estimated Completion Date**: Completed as of 4 November 2021

Controlled by: Navy [redacted] Office [redacted]
CUI Category: ISVI, PROPIN
Limited Dissemination Control: DL Only*
POC: [redacted]
*Dissemination authorized only to DoD employees and contractors with a need to know within the Naval Sea Systems Command (NAVSEASYSCOM) Headquarters and the DoD Office of Inspector General.

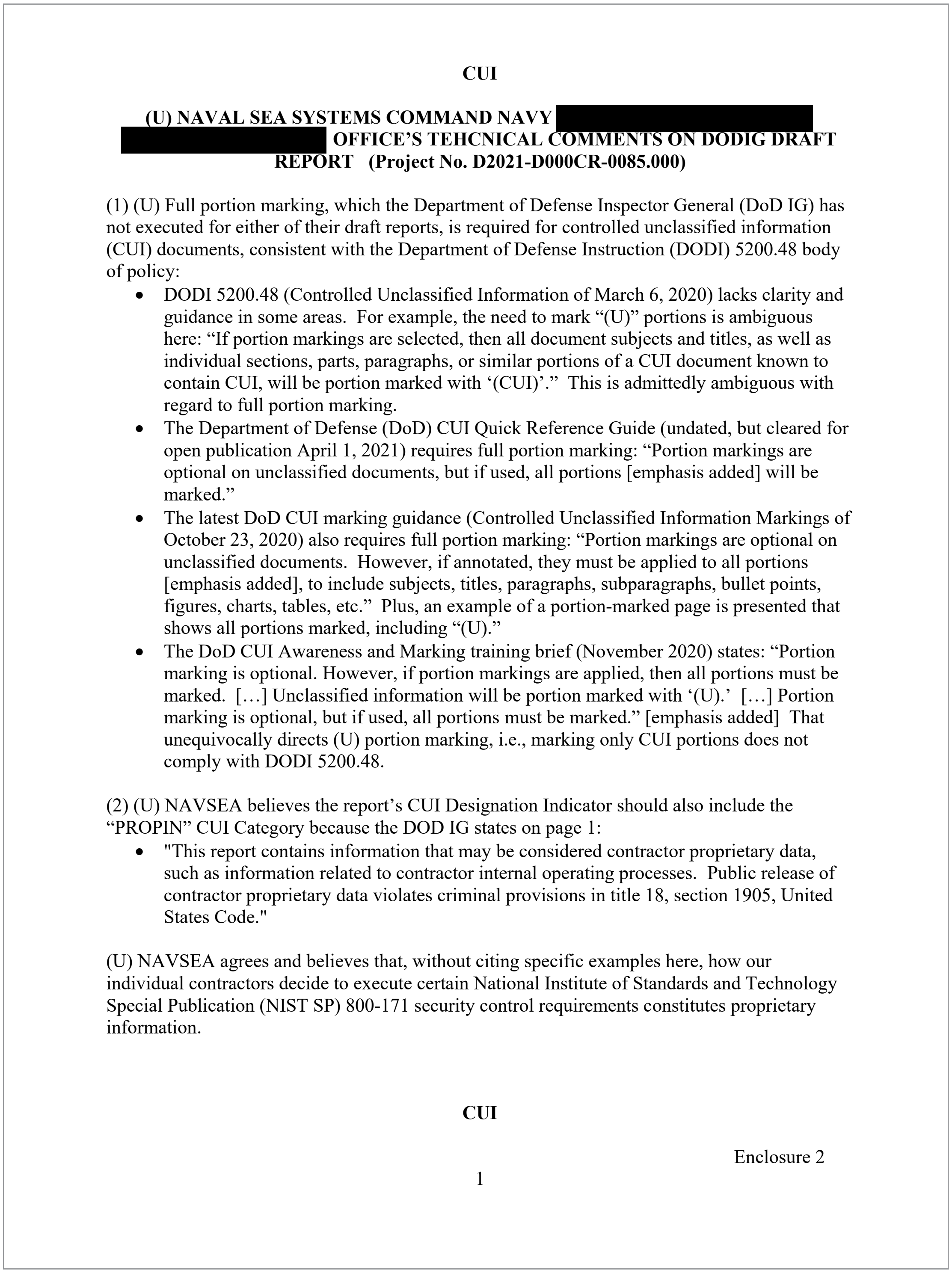
CUI

Enclosure 1

5

(U) Navy (cont’d)

(U) NAVSEA (cont’d)



CUI

(U) NAVAL SEA SYSTEMS COMMAND NAVY [redacted] [redacted] OFFICE’S TEHCNICAL COMMENTS ON DODIG DRAFT REPORT (Project No. D2021-D000CR-0085.000)

(1) (U) Full portion marking, which the Department of Defense Inspector General (DoD IG) has not executed for either of their draft reports, is required for controlled unclassified information (CUI) documents, consistent with the Department of Defense Instruction (DODI) 5200.48 body of policy:

- DODI 5200.48 (Controlled Unclassified Information of March 6, 2020) lacks clarity and guidance in some areas. For example, the need to mark “(U)” portions is ambiguous here: “If portion markings are selected, then all document subjects and titles, as well as individual sections, parts, paragraphs, or similar portions of a CUI document known to contain CUI, will be portion marked with ‘(CUI)’.” This is admittedly ambiguous with regard to full portion marking.
- The Department of Defense (DoD) CUI Quick Reference Guide (undated, but cleared for open publication April 1, 2021) requires full portion marking: “Portion markings are optional on unclassified documents, but if used, all portions [emphasis added] will be marked.”
- The latest DoD CUI marking guidance (Controlled Unclassified Information Markings of October 23, 2020) also requires full portion marking: “Portion markings are optional on unclassified documents. However, if annotated, they must be applied to all portions [emphasis added], to include subjects, titles, paragraphs, subparagraphs, bullet points, figures, charts, tables, etc.” Plus, an example of a portion-marked page is presented that shows all portions marked, including “(U).”
- The DoD CUI Awareness and Marking training brief (November 2020) states: “Portion marking is optional. However, if portion markings are applied, then all portions must be marked. […] Unclassified information will be portion marked with ‘(U).’ […] Portion marking is optional, but if used, all portions must be marked.” [emphasis added] That unequivocally directs (U) portion marking, i.e., marking only CUI portions does not comply with DODI 5200.48.

(2) (U) NAVSEA believes the report’s CUI Designation Indicator should also include the “PROPIN” CUI Category because the DOD IG states on page 1:

- "This report contains information that may be considered contractor proprietary data, such as information related to contractor internal operating processes. Public release of contractor proprietary data violates criminal provisions in title 18, section 1905, United States Code."

(U) NAVSEA agrees and believes that, without citing specific examples here, how our individual contractors decide to execute certain National Institute of Standards and Technology Special Publication (NIST SP) 800-171 security control requirements constitutes proprietary information.

CUI

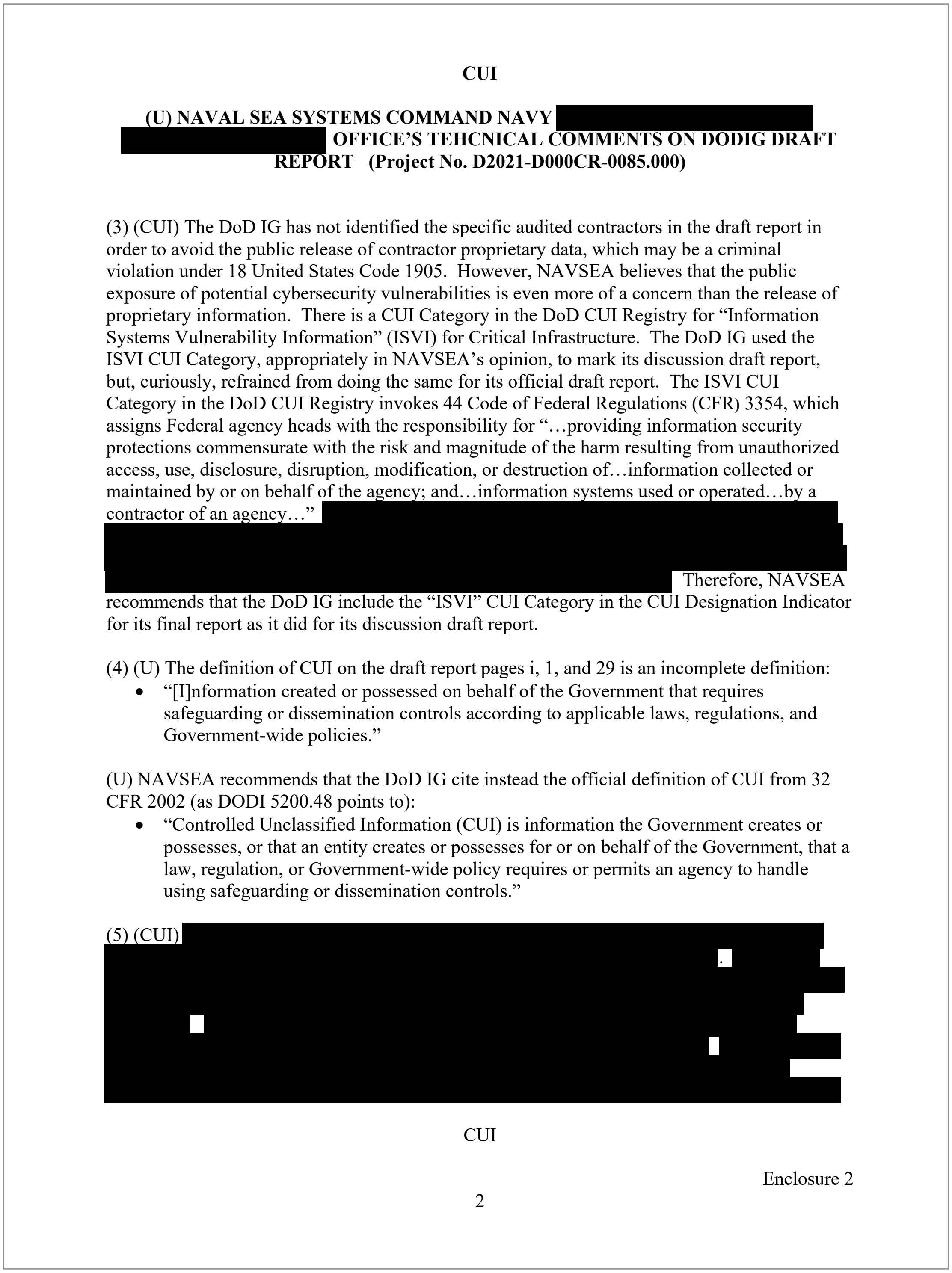
Enclosure 2

1

(U) Navy (cont'd)

(U) NAVSEA (cont'd)

Final Report Reference



CUI

(U) NAVAL SEA SYSTEMS COMMAND NAVY [redacted] [redacted] OFFICE'S TEHCNICAL COMMENTS ON DODIG DRAFT REPORT (Project No. D2021-D000CR-0085.000)

(3) (CUI) The DoD IG has not identified the specific audited contractors in the draft report in order to avoid the public release of contractor proprietary data, which may be a criminal violation under 18 United States Code 1905. However, NAVSEA believes that the public exposure of potential cybersecurity vulnerabilities is even more of a concern than the release of proprietary information. There is a CUI Category in the DoD CUI Registry for "Information Systems Vulnerability Information" (ISVI) for Critical Infrastructure. The DoD IG used the ISVI CUI Category, appropriately in NAVSEA's opinion, to mark its discussion draft report, but, curiously, refrained from doing the same for its official draft report. The ISVI CUI Category in the DoD CUI Registry invokes 44 Code of Federal Regulations (CFR) 3354, which assigns Federal agency heads with the responsibility for "…providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of…information collected or maintained by or on behalf of the agency; and…information systems used or operated…by a contractor of an agency…" [redacted] Therefore, NAVSEA recommends that the DoD IG include the "ISVI" CUI Category in the CUI Designation Indicator for its final report as it did for its discussion draft report.

(4) (U) The definition of CUI on the draft report pages i, 1, and 29 is an incomplete definition:

- "[I]nformation created or possessed on behalf of the Government that requires safeguarding or dissemination controls according to applicable laws, regulations, and Government-wide policies."

Page 71

(U) NAVSEA recommends that the DoD IG cite instead the official definition of CUI from 32 CFR 2002 (as DODI 5200.48 points to):

- "Controlled Unclassified Information (CUI) is information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls."

(5) (CUI) [redacted]

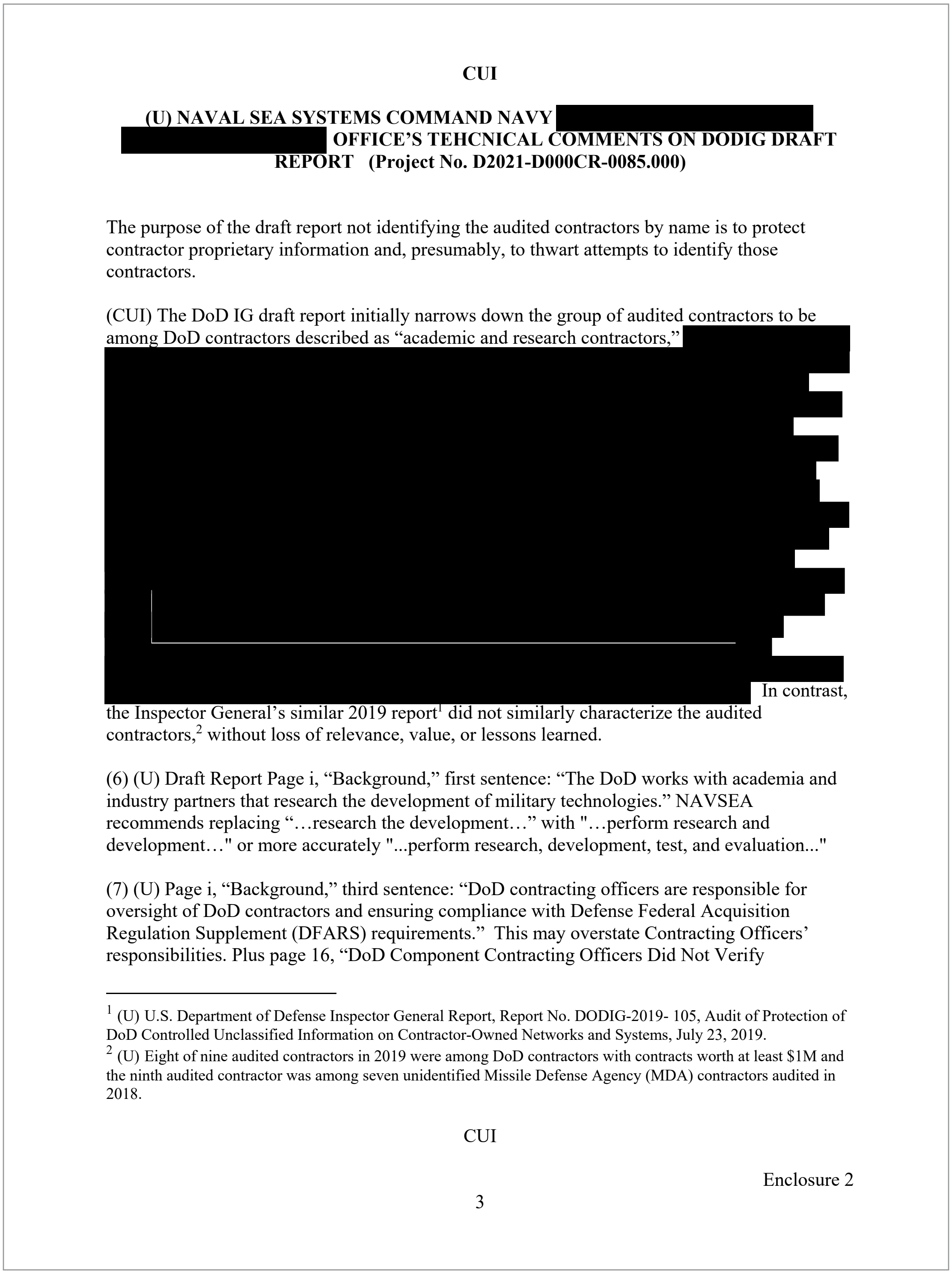
CUI

Enclosure 2

2

(U) Navy (cont'd)

(U) NAVSEA (cont'd)



CUI

(U) NAVAL SEA SYSTEMS COMMAND NAVY [redacted] [redacted] OFFICE'S TEHCNICAL COMMENTS ON DODIG DRAFT REPORT (Project No. D2021-D000CR-0085.000)

The purpose of the draft report not identifying the audited contractors by name is to protect contractor proprietary information and, presumably, to thwart attempts to identify those contractors.

(CUI) The DoD IG draft report initially narrows down the group of audited contractors to be among DoD contractors described as "academic and research contractors," [redacted] In contrast, the Inspector General's similar 2019 report[1] did not similarly characterize the audited contractors,[2] without loss of relevance, value, or lessons learned.

(6) (U) Draft Report Page i, "Background," first sentence: "The DoD works with academia and industry partners that research the development of military technologies." NAVSEA recommends replacing "…research the development…" with "…perform research and development…" or more accurately "...perform research, development, test, and evaluation..."

(7) (U) Page i, "Background," third sentence: "DoD contracting officers are responsible for oversight of DoD contractors and ensuring compliance with Defense Federal Acquisition Regulation Supplement (DFARS) requirements." This may overstate Contracting Officers' responsibilities. Plus page 16, "DoD Component Contracting Officers Did Not Verify

[1] (U) U.S. Department of Defense Inspector General Report, Report No. DODIG-2019- 105, Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems, July 23, 2019.

[2] (U) Eight of nine audited contractors in 2019 were among DoD contractors with contracts worth at least $1M and the ninth audited contractor was among seven unidentified Missile Defense Agency (MDA) contractors audited in 2018.

CUI

Enclosure 2

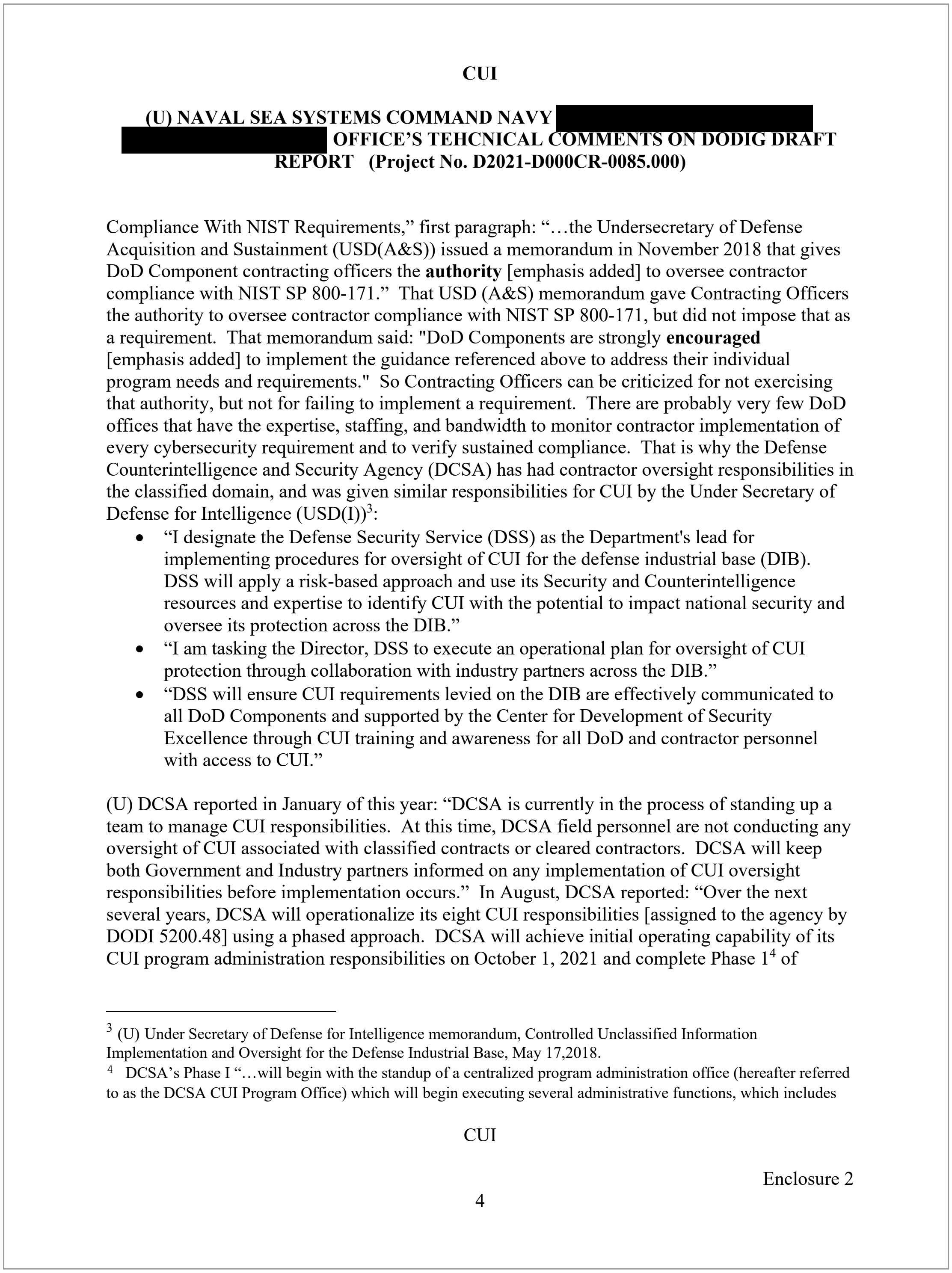
3

Final Report Reference

Page 17

(U) Navy (cont'd)

(U) NAVSEA (cont'd)



CUI

(U) NAVAL SEA SYSTEMS COMMAND NAVY [redacted] [redacted] OFFICE'S TEHCNICAL COMMENTS ON DODIG DRAFT REPORT (Project No. D2021-D000CR-0085.000)

Compliance With NIST Requirements," first paragraph: "…the Undersecretary of Defense Acquisition and Sustainment (USD(A&S)) issued a memorandum in November 2018 that gives DoD Component contracting officers the **authority** [emphasis added] to oversee contractor compliance with NIST SP 800-171." That USD (A&S) memorandum gave Contracting Officers the authority to oversee contractor compliance with NIST SP 800-171, but did not impose that as a requirement. That memorandum said: "DoD Components are strongly **encouraged** [emphasis added] to implement the guidance referenced above to address their individual program needs and requirements." So Contracting Officers can be criticized for not exercising that authority, but not for failing to implement a requirement. There are probably very few DoD offices that have the expertise, staffing, and bandwidth to monitor contractor implementation of every cybersecurity requirement and to verify sustained compliance. That is why the Defense Counterintelligence and Security Agency (DCSA) has had contractor oversight responsibilities in the classified domain, and was given similar responsibilities for CUI by the Under Secretary of Defense for Intelligence (USD(I))[3]:

- "I designate the Defense Security Service (DSS) as the Department's lead for implementing procedures for oversight of CUI for the defense industrial base (DIB). DSS will apply a risk-based approach and use its Security and Counterintelligence resources and expertise to identify CUI with the potential to impact national security and oversee its protection across the DIB."
- "I am tasking the Director, DSS to execute an operational plan for oversight of CUI protection through collaboration with industry partners across the DIB."
- "DSS will ensure CUI requirements levied on the DIB are effectively communicated to all DoD Components and supported by the Center for Development of Security Excellence through CUI training and awareness for all DoD and contractor personnel with access to CUI."

(U) DCSA reported in January of this year: "DCSA is currently in the process of standing up a team to manage CUI responsibilities. At this time, DCSA field personnel are not conducting any oversight of CUI associated with classified contracts or cleared contractors. DCSA will keep both Government and Industry partners informed on any implementation of CUI oversight responsibilities before implementation occurs." In August, DCSA reported: "Over the next several years, DCSA will operationalize its eight CUI responsibilities [assigned to the agency by DODI 5200.48] using a phased approach. DCSA will achieve initial operating capability of its CUI program administration responsibilities on October 1, 2021 and complete Phase 1[4] of

[3] (U) Under Secretary of Defense for Intelligence memorandum, Controlled Unclassified Information Implementation and Oversight for the Defense Industrial Base, May 17,2018.

[4] DCSA's Phase I "…will begin with the standup of a centralized program administration office (hereafter referred to as the DCSA CUI Program Office) which will begin executing several administrative functions, which includes

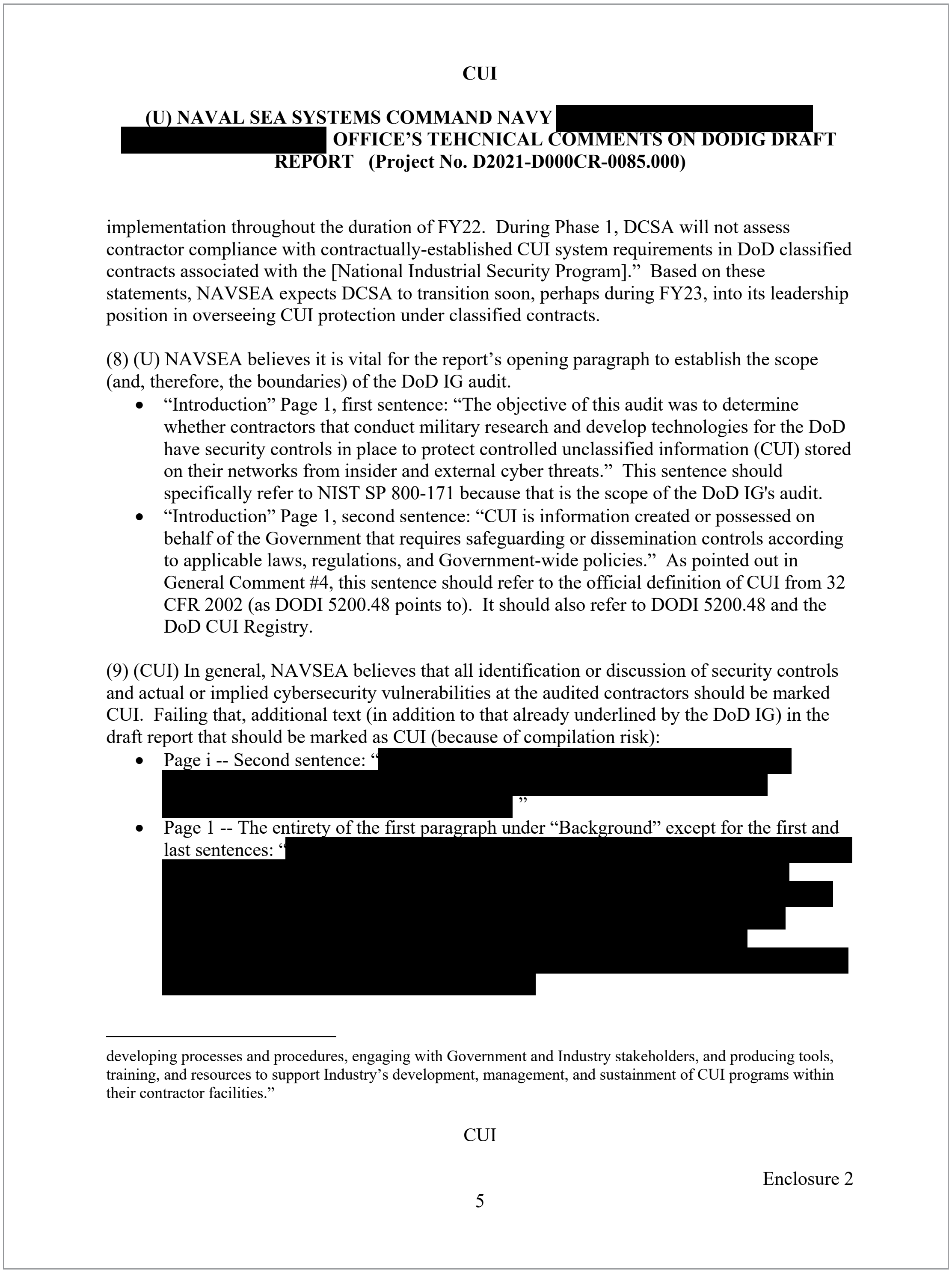
CUI

Enclosure 2

4

(U) Navy (cont'd)

(U) NAVSEA (cont'd)



CUI

(U) NAVAL SEA SYSTEMS COMMAND NAVY [redacted] [redacted] OFFICE'S TEHCNICAL COMMENTS ON DODIG DRAFT REPORT (Project No. D2021-D000CR-0085.000)

implementation throughout the duration of FY22. During Phase 1, DCSA will not assess contractor compliance with contractually-established CUI system requirements in DoD classified contracts associated with the [National Industrial Security Program]." Based on these statements, NAVSEA expects DCSA to transition soon, perhaps during FY23, into its leadership position in overseeing CUI protection under classified contracts.

(8) (U) NAVSEA believes it is vital for the report's opening paragraph to establish the scope (and, therefore, the boundaries) of the DoD IG audit.

- "Introduction" Page 1, first sentence: "The objective of this audit was to determine whether contractors that conduct military research and develop technologies for the DoD have security controls in place to protect controlled unclassified information (CUI) stored on their networks from insider and external cyber threats." This sentence should specifically refer to NIST SP 800-171 because that is the scope of the DoD IG's audit.
- "Introduction" Page 1, second sentence: "CUI is information created or possessed on behalf of the Government that requires safeguarding or dissemination controls according to applicable laws, regulations, and Government-wide policies." As pointed out in General Comment #4, this sentence should refer to the official definition of CUI from 32 CFR 2002 (as DODI 5200.48 points to). It should also refer to DODI 5200.48 and the DoD CUI Registry.

(9) (CUI) In general, NAVSEA believes that all identification or discussion of security controls and actual or implied cybersecurity vulnerabilities at the audited contractors should be marked CUI. Failing that, additional text (in addition to that already underlined by the DoD IG) in the draft report that should be marked as CUI (because of compilation risk):

- Page i -- Second sentence: "[redacted]"
- Page 1 -- The entirety of the first paragraph under "Background" except for the first and last sentences: "[redacted]

developing processes and procedures, engaging with Government and Industry stakeholders, and producing tools, training, and resources to support Industry's development, management, and sustainment of CUI programs within their contractor facilities."

CUI

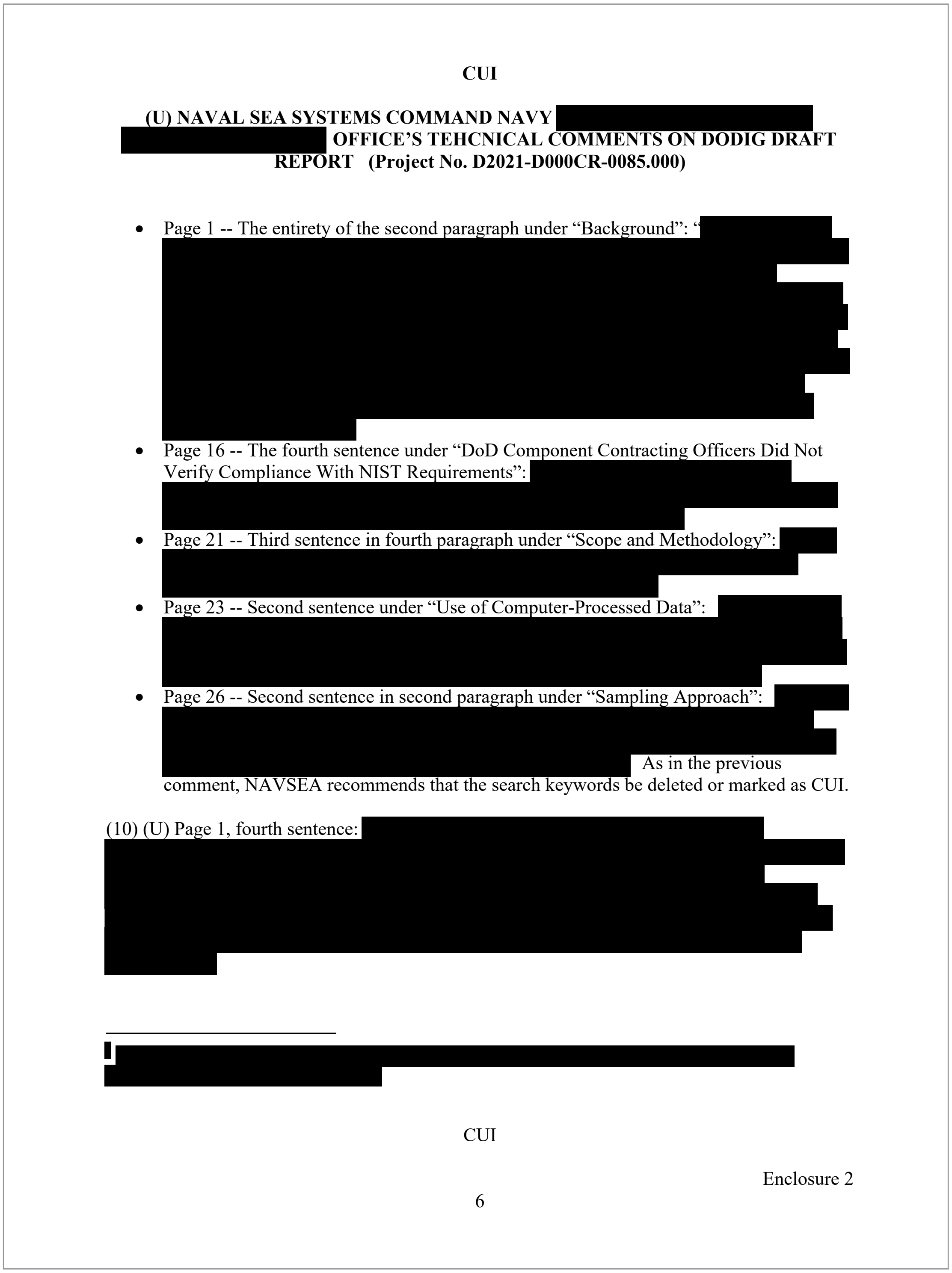
Enclosure 2

5

(U) Navy (cont'd)

(U) NAVSEA (cont'd)

Final Report Reference



CUI

(U) NAVAL SEA SYSTEMS COMMAND NAVY [redacted] OFFICE'S TEHCNICAL COMMENTS ON DODIG DRAFT REPORT (Project No. D2021-D000CR-0085.000)

- Page 1 -- The entirety of the second paragraph under "Background": "[redacted]
- Page 16 -- The fourth sentence under "DoD Component Contracting Officers Did Not Verify Compliance With NIST Requirements": [redacted]

Page 17

- Page 21 -- Third sentence in fourth paragraph under "Scope and Methodology": [redacted]

Page 33

- Page 23 -- Second sentence under "Use of Computer-Processed Data": [redacted]

Page 35

- Page 26 -- Second sentence in second paragraph under "Sampling Approach": [redacted] As in the previous comment, NAVSEA recommends that the search keywords be deleted or marked as CUI.

Page 39

(10) (U) Page 1, fourth sentence: [redacted]

[redacted]

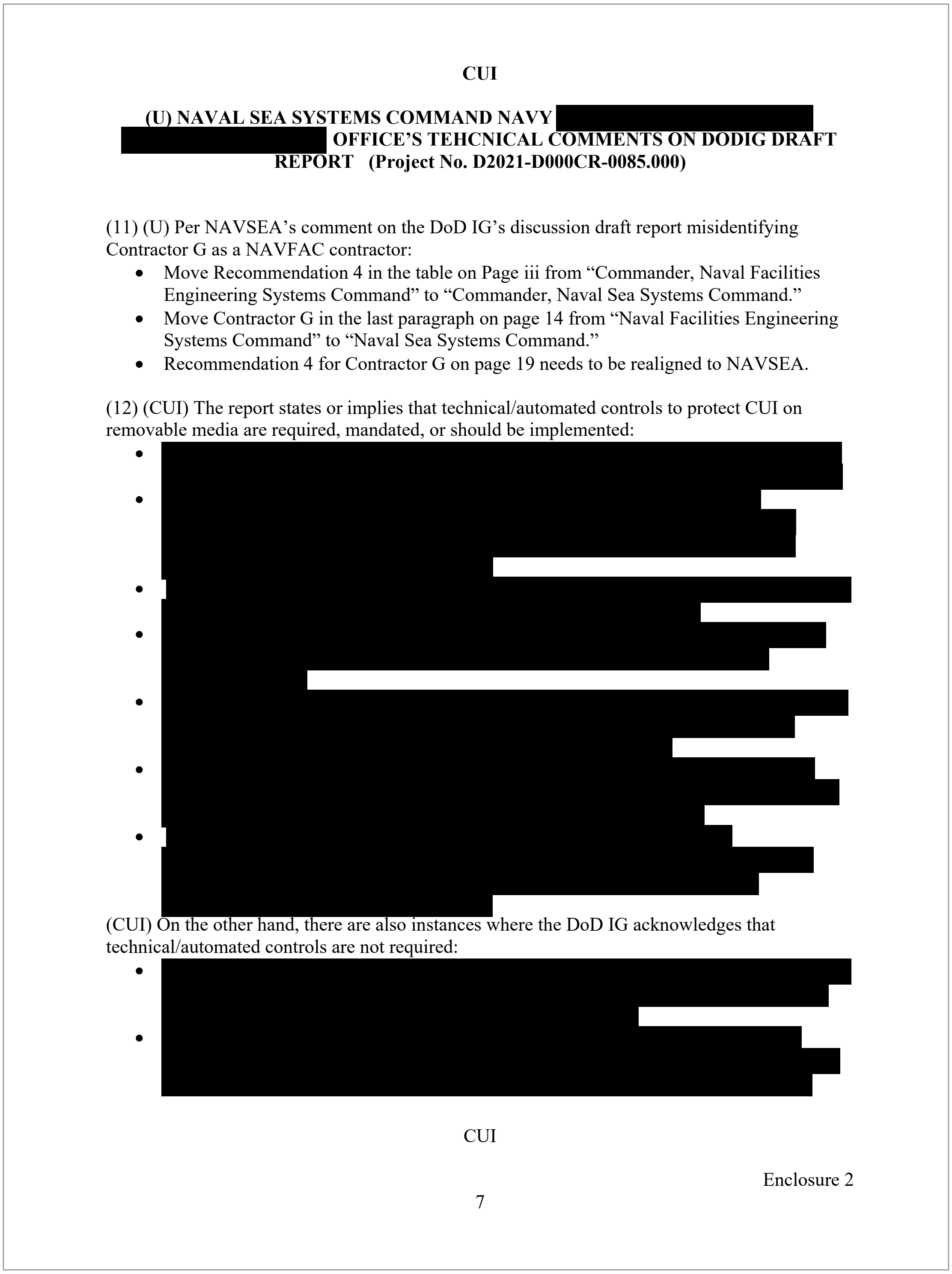
CUI

Enclosure 2

6

(U) Navy (cont’d)

(U) NAVSEA (cont’d)



CUI

(U) NAVAL SEA SYSTEMS COMMAND NAVY [redacted] [redacted] OFFICE’S TEHCNICAL COMMENTS ON DODIG DRAFT REPORT (Project No. D2021-D000CR-0085.000)

(11) (U) Per NAVSEA’s comment on the DoD IG’s discussion draft report misidentifying Contractor G as a NAVFAC contractor:

- Move Recommendation 4 in the table on Page iii from “Commander, Naval Facilities Engineering Systems Command” to “Commander, Naval Sea Systems Command.”
- Move Contractor G in the last paragraph on page 14 from “Naval Facilities Engineering Systems Command” to “Naval Sea Systems Command.”
- Recommendation 4 for Contractor G on page 19 needs to be realigned to NAVSEA.

(12) (CUI) The report states or implies that technical/automated controls to protect CUI on removable media are required, mandated, or should be implemented:

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

(CUI) On the other hand, there are also instances where the DoD IG acknowledges that technical/automated controls are not required:

- [redacted]
- [redacted]

CUI

Enclosure 2

7

Final Report Reference

Redirected and Renumbered as Recommendation 3.d

Page 14

Page 15

Deleted

Page 27

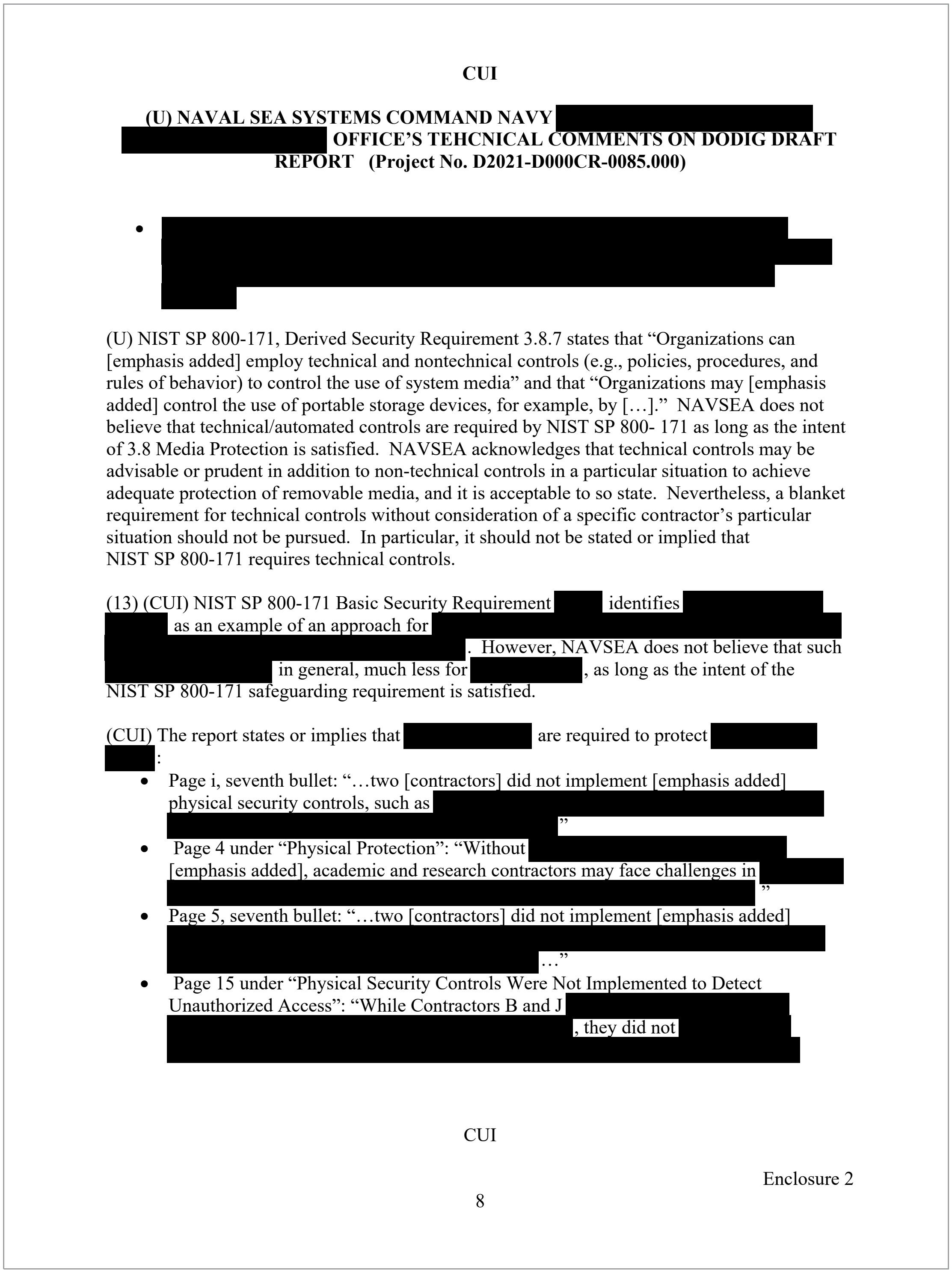
Page 3

Page 14

(U) Navy (cont'd)

(U) NAVSEA (cont'd)

Final Report Reference



CUI

(U) NAVAL SEA SYSTEMS COMMAND NAVY [redacted] OFFICE'S TEHCNICAL COMMENTS ON DODIG DRAFT REPORT (Project No. D2021-D000CR-0085.000)

- [redacted]

Page 15

(U) NIST SP 800-171, Derived Security Requirement 3.8.7 states that "Organizations can [emphasis added] employ technical and nontechnical controls (e.g., policies, procedures, and rules of behavior) to control the use of system media" and that "Organizations may [emphasis added] control the use of portable storage devices, for example, by […]." NAVSEA does not believe that technical/automated controls are required by NIST SP 800- 171 as long as the intent of 3.8 Media Protection is satisfied. NAVSEA acknowledges that technical controls may be advisable or prudent in addition to non-technical controls in a particular situation to achieve adequate protection of removable media, and it is acceptable to so state. Nevertheless, a blanket requirement for technical controls without consideration of a specific contractor's particular situation should not be pursued. In particular, it should not be stated or implied that NIST SP 800-171 requires technical controls.

(13) (CUI) NIST SP 800-171 Basic Security Requirement [redacted] identifies [redacted] as an example of an approach for [redacted]. However, NAVSEA does not believe that such [redacted] in general, much less for [redacted], as long as the intent of the NIST SP 800-171 safeguarding requirement is satisfied.

(CUI) The report states or implies that [redacted] are required to protect [redacted]:

- Page i, seventh bullet: "…two [contractors] did not implement [emphasis added] physical security controls, such as [redacted]"
- Page 4 under "Physical Protection": "Without [redacted] [emphasis added], academic and research contractors may face challenges in [redacted]"

Page 3

- Page 5, seventh bullet: "…two [contractors] did not implement [emphasis added] [redacted]…"
- Page 15 under "Physical Security Controls Were Not Implemented to Detect Unauthorized Access": "While Contractors B and J [redacted], they did not [redacted]

Page 16

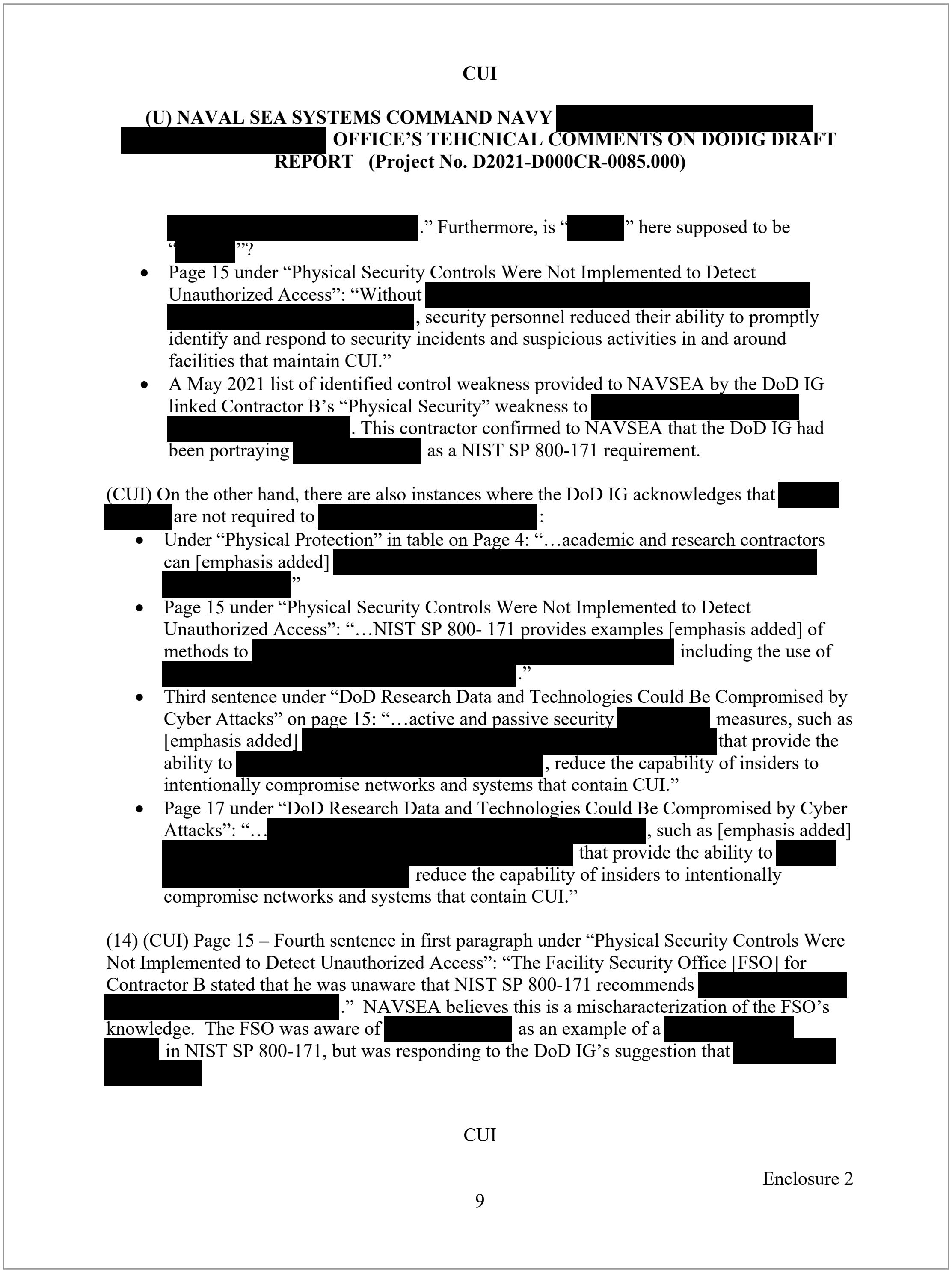
CUI

Enclosure 2

8

(U) Navy (cont’d)

(U) NAVSEA (cont’d)



CUI

(U) NAVAL SEA SYSTEMS COMMAND NAVY [redacted] OFFICE’S TEHCNICAL COMMENTS ON DODIG DRAFT REPORT (Project No. D2021-D000CR-0085.000)

[redacted].” Furthermore, is “[redacted]” here supposed to be “[redacted]”?

- Page 15 under “Physical Security Controls Were Not Implemented to Detect Unauthorized Access”: “Without [redacted], security personnel reduced their ability to promptly identify and respond to security incidents and suspicious activities in and around facilities that maintain CUI.”
- A May 2021 list of identified control weakness provided to NAVSEA by the DoD IG linked Contractor B’s “Physical Security” weakness to [redacted]. This contractor confirmed to NAVSEA that the DoD IG had been portraying [redacted] as a NIST SP 800-171 requirement.

(CUI) On the other hand, there are also instances where the DoD IG acknowledges that [redacted] are not required to [redacted]:

- Under “Physical Protection” in table on Page 4: “…academic and research contractors can [emphasis added] [redacted]”
- Page 15 under “Physical Security Controls Were Not Implemented to Detect Unauthorized Access”: “…NIST SP 800- 171 provides examples [emphasis added] of methods to [redacted] including the use of [redacted].”
- Third sentence under “DoD Research Data and Technologies Could Be Compromised by Cyber Attacks” on page 15: “…active and passive security [redacted] measures, such as [emphasis added] [redacted] that provide the ability to [redacted], reduce the capability of insiders to intentionally compromise networks and systems that contain CUI.”
- Page 17 under “DoD Research Data and Technologies Could Be Compromised by Cyber Attacks”: “…[redacted], such as [emphasis added] [redacted] that provide the ability to [redacted] reduce the capability of insiders to intentionally compromise networks and systems that contain CUI.”

(14) (CUI) Page 15 – Fourth sentence in first paragraph under “Physical Security Controls Were Not Implemented to Detect Unauthorized Access”: “The Facility Security Office [FSO] for Contractor B stated that he was unaware that NIST SP 800-171 recommends [redacted].” NAVSEA believes this is a mischaracterization of the FSO’s knowledge. The FSO was aware of [redacted] as an example of a [redacted] in NIST SP 800-171, but was responding to the DoD IG’s suggestion that [redacted]

CUI

Enclosure 2

9

Final Report Reference

Page 16

Page 3

Page 16

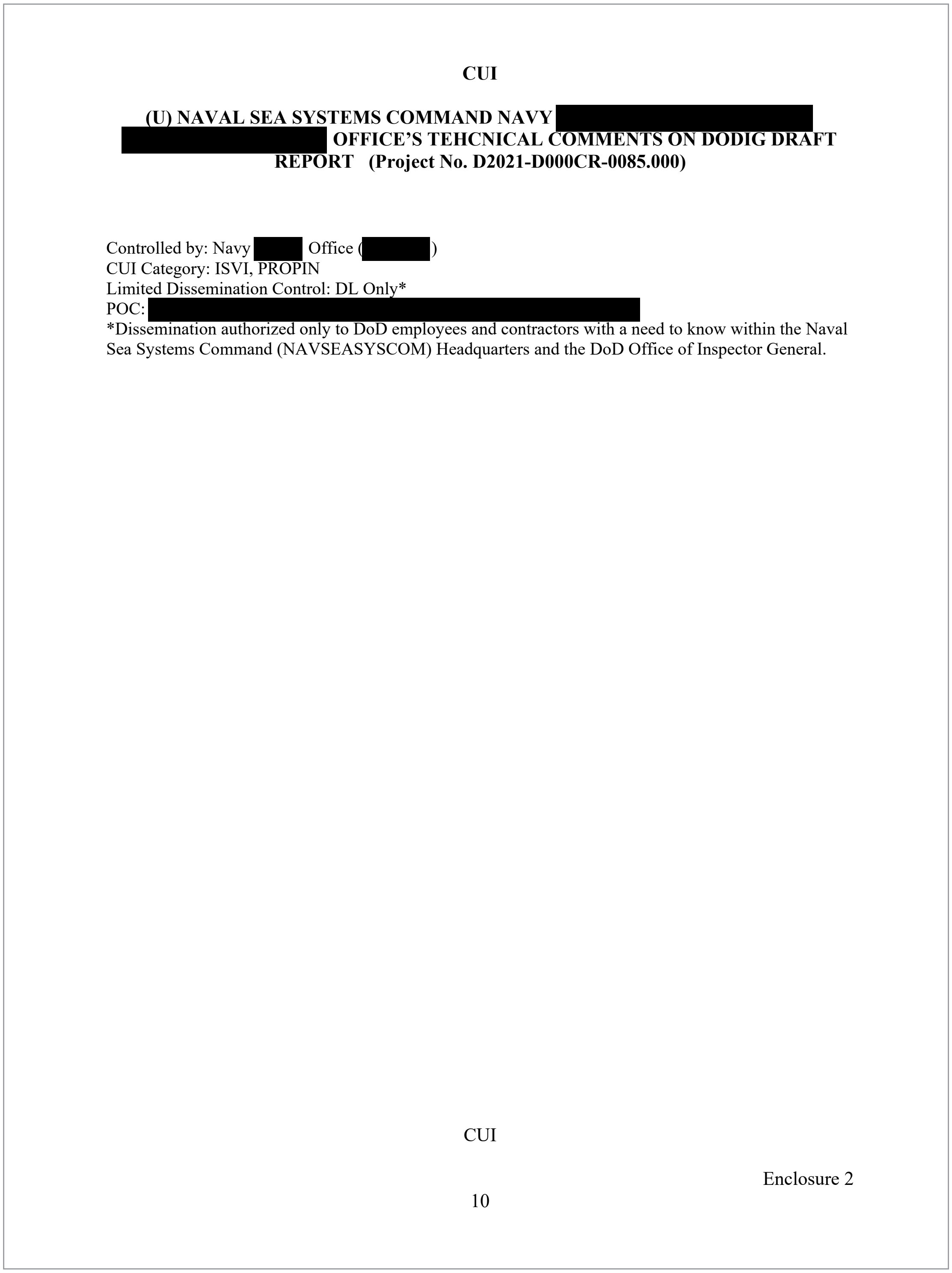
Page 20

Page 20

Page 16

(U) Navy (cont'd)

(U) NAVSEA (cont'd)



CUI

(U) NAVAL SEA SYSTEMS COMMAND NAVY [redacted] [redacted] OFFICE'S TEHCNICAL COMMENTS ON DODIG DRAFT REPORT (Project No. D2021-D000CR-0085.000)

Controlled by: Navy [redacted] Office ([redacted])
CUI Category: ISVI, PROPIN
Limited Dissemination Control: DL Only*
POC: [redacted]
*Dissemination authorized only to DoD employees and contractors with a need to know within the Naval Sea Systems Command (NAVSEASYSCOM) Headquarters and the DoD Office of Inspector General.

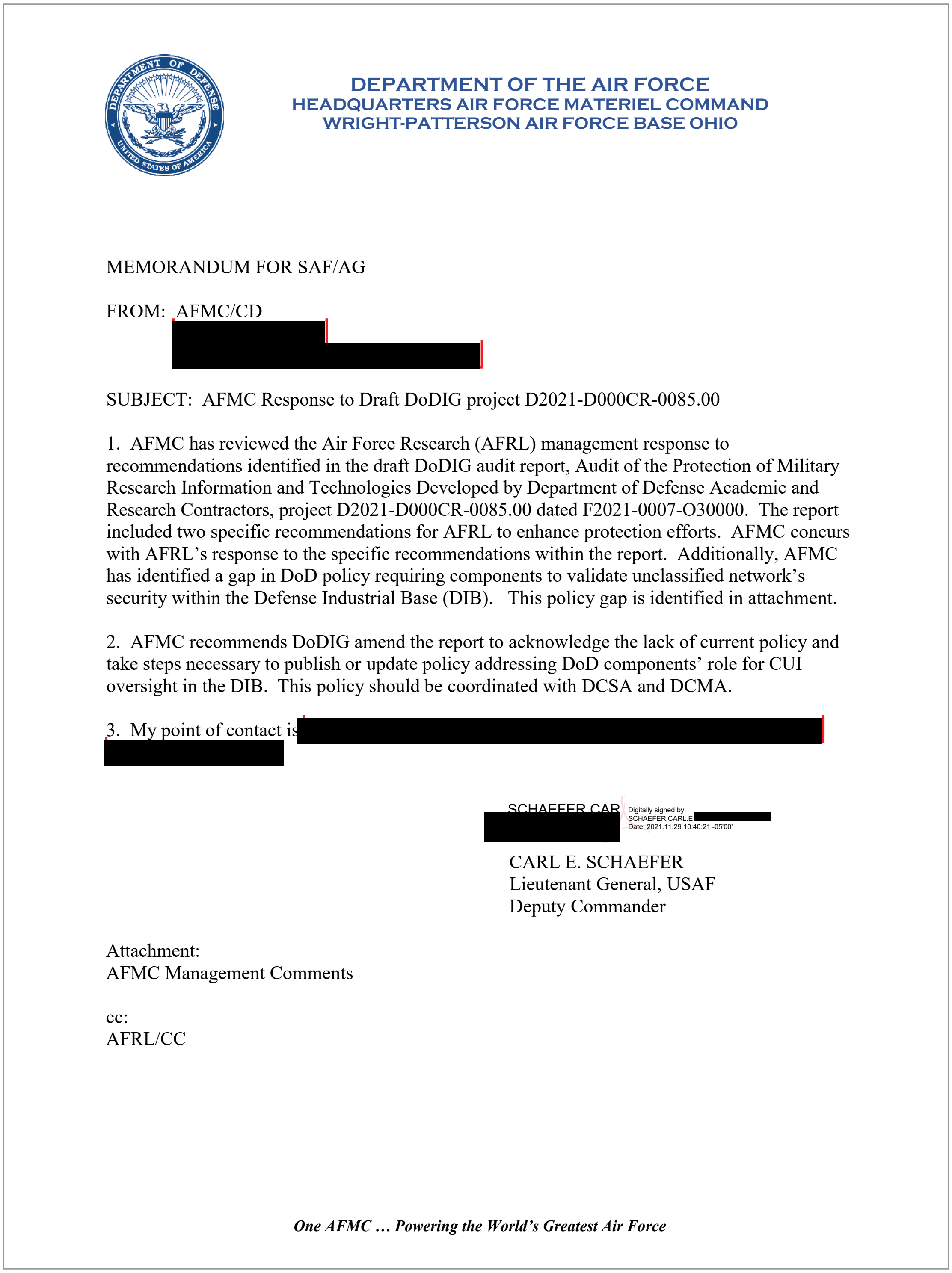
CUI

Enclosure 2

10

(U) Air Force

(U) AFMC



DEPARTMENT OF THE AIR FORCE
HEADQUARTERS AIR FORCE MATERIEL COMMAND
WRIGHT-PATTERSON AIR FORCE BASE OHIO

MEMORANDUM FOR SAF/AG

FROM: AFMC/CD
[redacted]

SUBJECT: AFMC Response to Draft DoDIG project D2021-D000CR-0085.00

1. AFMC has reviewed the Air Force Research (AFRL) management response to recommendations identified in the draft DoDIG audit report, Audit of the Protection of Military Research Information and Technologies Developed by Department of Defense Academic and Research Contractors, project D2021-D000CR-0085.00 dated F2021-0007-O30000. The report included two specific recommendations for AFRL to enhance protection efforts. AFMC concurs with AFRL's response to the specific recommendations within the report. Additionally, AFMC has identified a gap in DoD policy requiring components to validate unclassified network's security within the Defense Industrial Base (DIB). This policy gap is identified in attachment.

2. AFMC recommends DoDIG amend the report to acknowledge the lack of current policy and take steps necessary to publish or update policy addressing DoD components' role for CUI oversight in the DIB. This policy should be coordinated with DCSA and DCMA.

3. My point of contact is [redacted]

SCHAEFER.CAR [redacted] Digitally signed by SCHAEFER.CARL.E[redacted] Date: 2021.11.29 10:40:21 -05'00'

CARL E. SCHAEFER
Lieutenant General, USAF
Deputy Commander

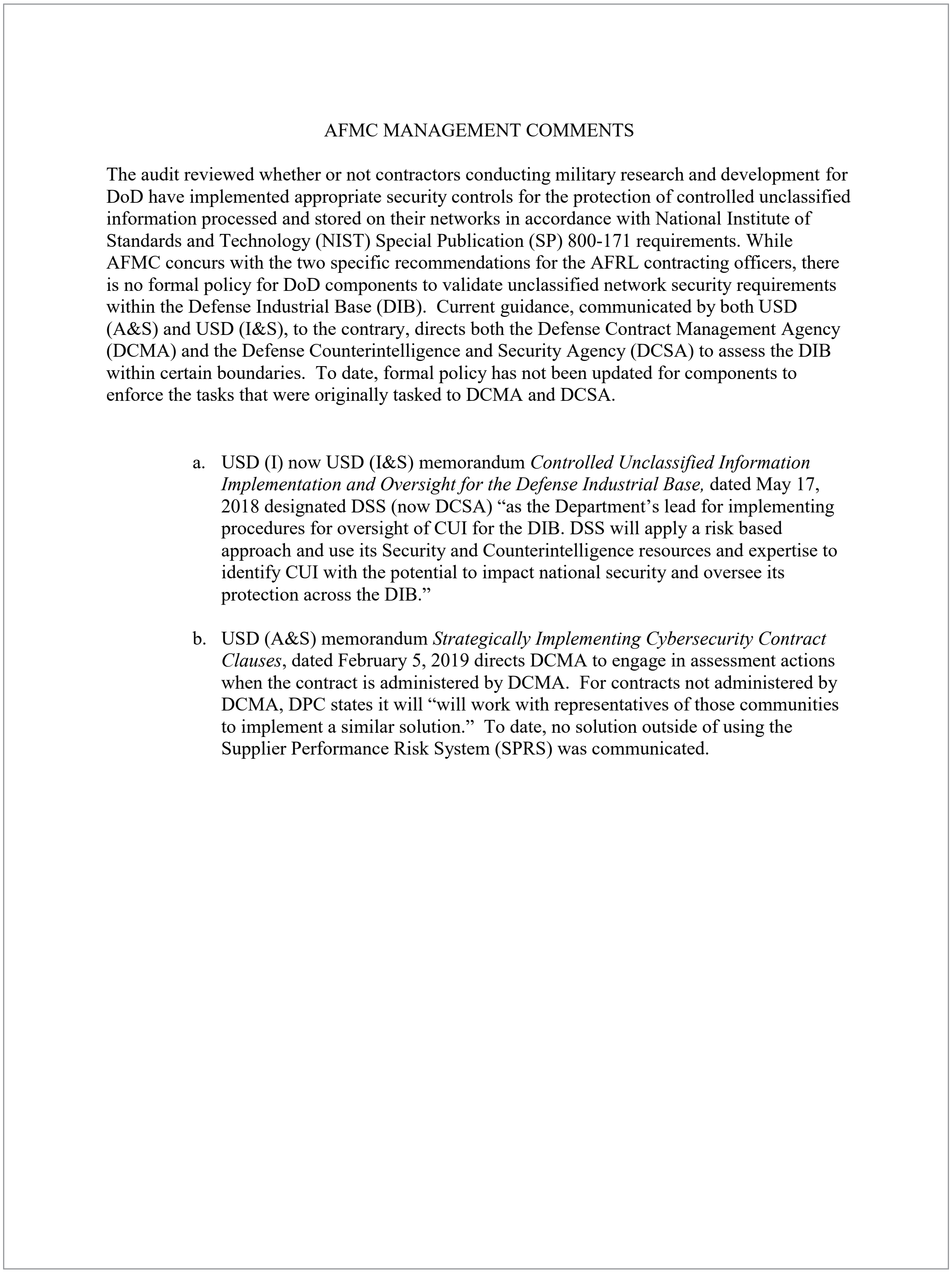
Attachment:
AFMC Management Comments

cc:
AFRL/CC

One AFMC … Powering the World's Greatest Air Force

(U) Air Force (cont’d)

(U) AFMC (cont’d)



AFMC MANAGEMENT COMMENTS

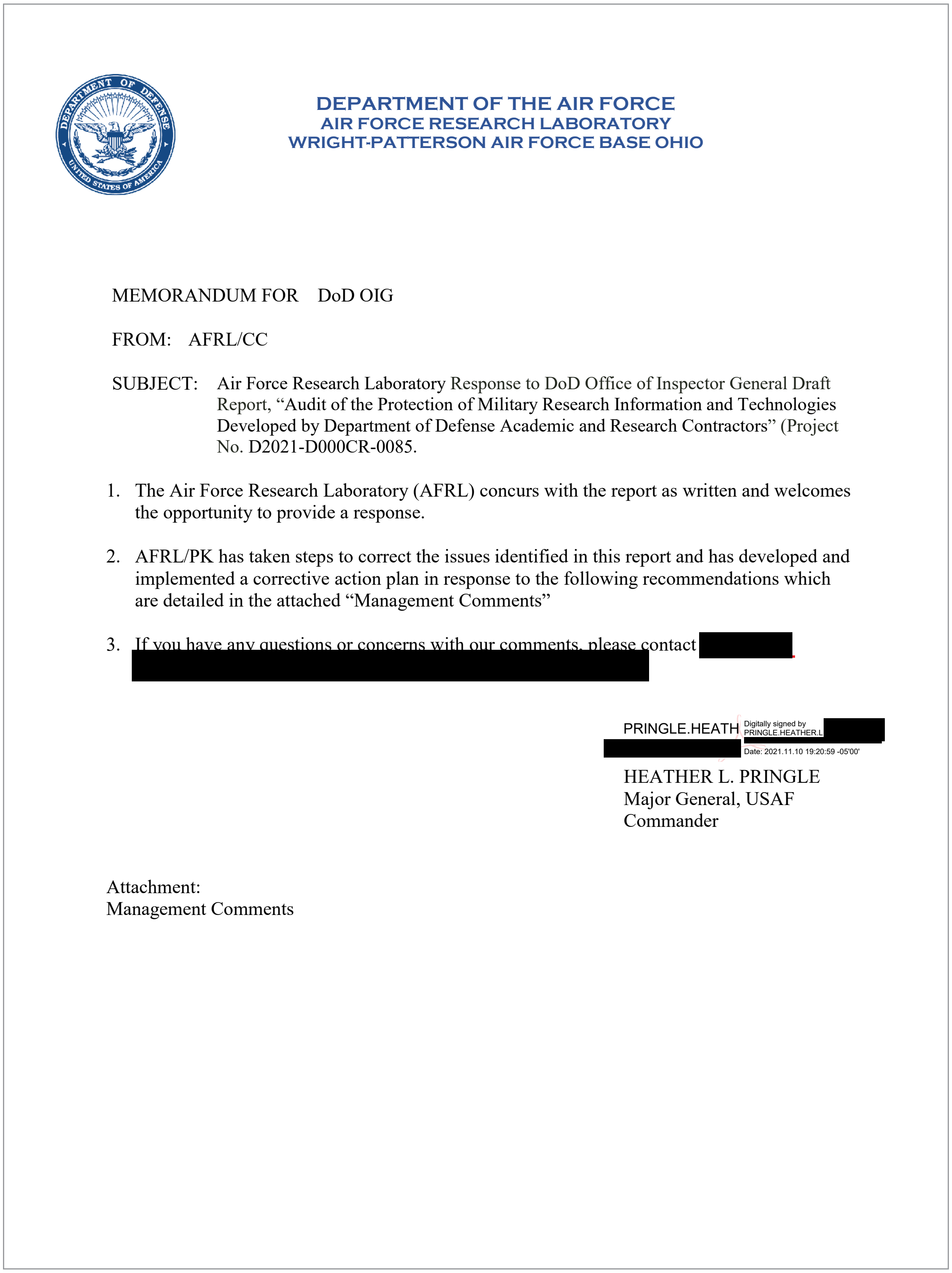
The audit reviewed whether or not contractors conducting military research and development for DoD have implemented appropriate security controls for the protection of controlled unclassified information processed and stored on their networks in accordance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 requirements. While AFMC concurs with the two specific recommendations for the AFRL contracting officers, there is no formal policy for DoD components to validate unclassified network security requirements within the Defense Industrial Base (DIB). Current guidance, communicated by both USD (A&S) and USD (I&S), to the contrary, directs both the Defense Contract Management Agency (DCMA) and the Defense Counterintelligence and Security Agency (DCSA) to assess the DIB within certain boundaries. To date, formal policy has not been updated for components to enforce the tasks that were originally tasked to DCMA and DCSA.

a. USD (I) now USD (I&S) memorandum *Controlled Unclassified Information Implementation and Oversight for the Defense Industrial Base,* dated May 17, 2018 designated DSS (now DCSA) “as the Department’s lead for implementing procedures for oversight of CUI for the DIB. DSS will apply a risk based approach and use its Security and Counterintelligence resources and expertise to identify CUI with the potential to impact national security and oversee its protection across the DIB.”

b. USD (A&S) memorandum *Strategically Implementing Cybersecurity Contract Clauses*, dated February 5, 2019 directs DCMA to engage in assessment actions when the contract is administered by DCMA. For contracts not administered by DCMA, DPC states it will “will work with representatives of those communities to implement a similar solution.” To date, no solution outside of using the Supplier Performance Risk System (SPRS) was communicated.

(U) Air Force (cont'd)

(U) AFRL



DEPARTMENT OF THE AIR FORCE
AIR FORCE RESEARCH LABORATORY
WRIGHT-PATTERSON AIR FORCE BASE OHIO

MEMORANDUM FOR DoD OIG

FROM: AFRL/CC

SUBJECT: Air Force Research Laboratory Response to DoD Office of Inspector General Draft Report, "Audit of the Protection of Military Research Information and Technologies Developed by Department of Defense Academic and Research Contractors" (Project No. D2021-D000CR-0085.

1. The Air Force Research Laboratory (AFRL) concurs with the report as written and welcomes the opportunity to provide a response.

2. AFRL/PK has taken steps to correct the issues identified in this report and has developed and implemented a corrective action plan in response to the following recommendations which are detailed in the attached "Management Comments"

3. If you have any questions or concerns with our comments, please contact [redacted] [redacted]

PRINGLE.HEATH [redacted] Digitally signed by PRINGLE.HEATHER.L [redacted]
Date: 2021.11.10 19:20:59 -05'00'

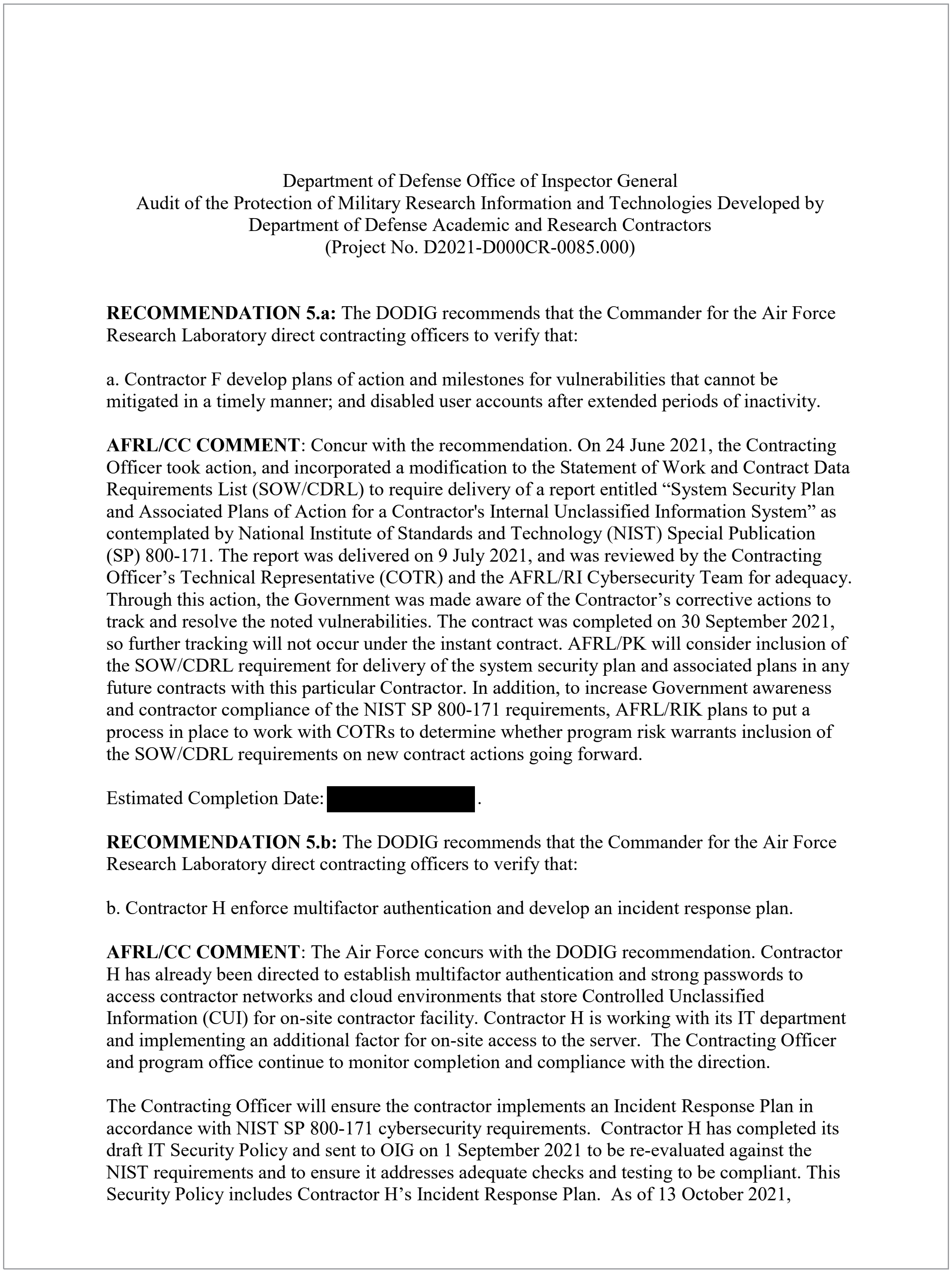
HEATHER L. PRINGLE
Major General, USAF
Commander

Attachment:
Management Comments

(U) Air Force (cont'd)

(U) AFRL (cont'd)

Final Report Reference



Department of Defense Office of Inspector General
Audit of the Protection of Military Research Information and Technologies Developed by Department of Defense Academic and Research Contractors
(Project No. D2021-D000CR-0085.000)

Renumbered as Recommendation 4.a

RECOMMENDATION 5.a: The DODIG recommends that the Commander for the Air Force Research Laboratory direct contracting officers to verify that:

a. Contractor F develop plans of action and milestones for vulnerabilities that cannot be mitigated in a timely manner; and disabled user accounts after extended periods of inactivity.

AFRL/CC COMMENT: Concur with the recommendation. On 24 June 2021, the Contracting Officer took action, and incorporated a modification to the Statement of Work and Contract Data Requirements List (SOW/CDRL) to require delivery of a report entitled "System Security Plan and Associated Plans of Action for a Contractor's Internal Unclassified Information System" as contemplated by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171. The report was delivered on 9 July 2021, and was reviewed by the Contracting Officer's Technical Representative (COTR) and the AFRL/RI Cybersecurity Team for adequacy. Through this action, the Government was made aware of the Contractor's corrective actions to track and resolve the noted vulnerabilities. The contract was completed on 30 September 2021, so further tracking will not occur under the instant contract. AFRL/PK will consider inclusion of the SOW/CDRL requirement for delivery of the system security plan and associated plans in any future contracts with this particular Contractor. In addition, to increase Government awareness and contractor compliance of the NIST SP 800-171 requirements, AFRL/RIK plans to put a process in place to work with COTRs to determine whether program risk warrants inclusion of the SOW/CDRL requirements on new contract actions going forward.

Estimated Completion Date: [redacted].

Renumbered as Recommendation 4.b

RECOMMENDATION 5.b: The DODIG recommends that the Commander for the Air Force Research Laboratory direct contracting officers to verify that:

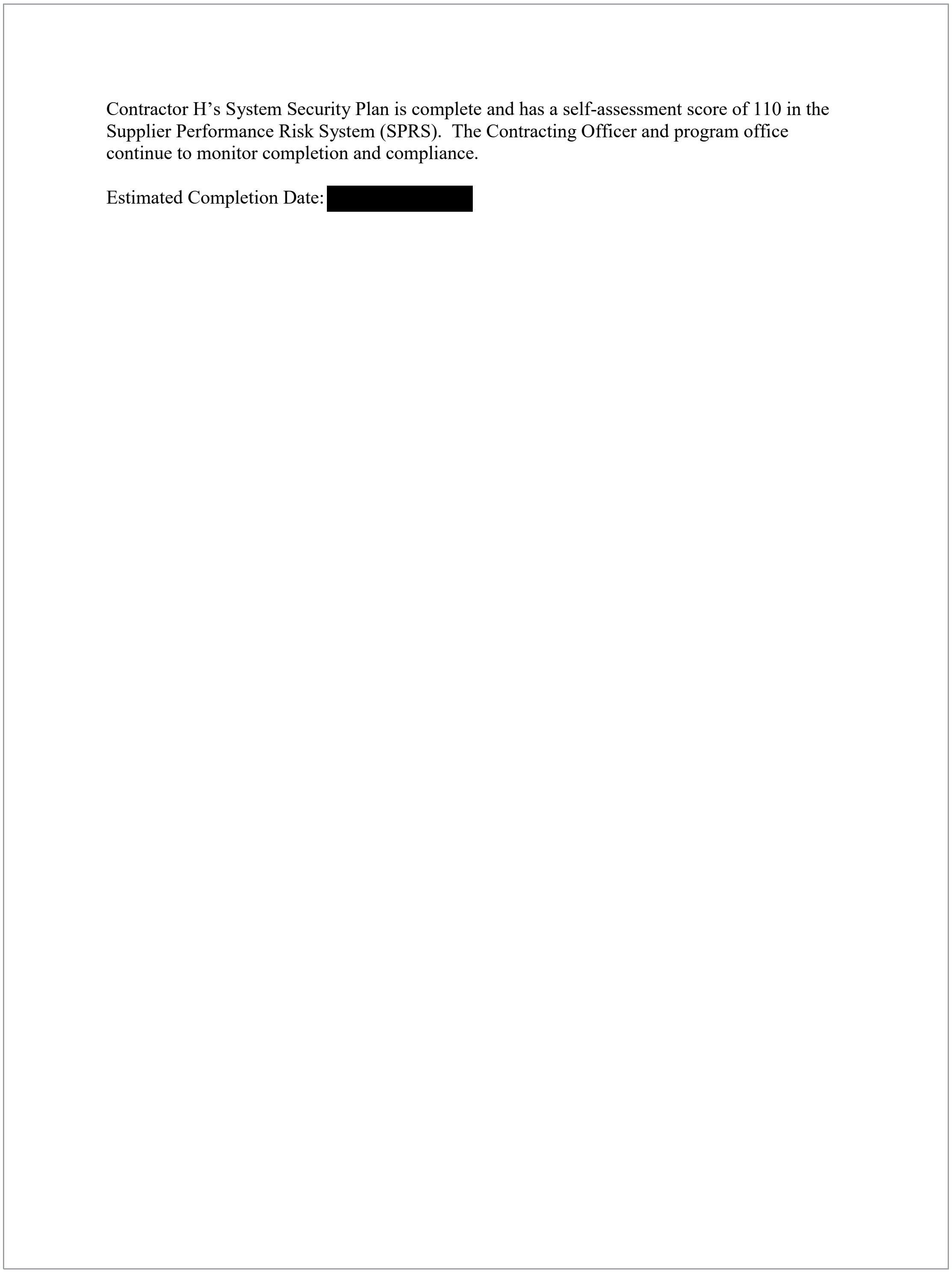
b. Contractor H enforce multifactor authentication and develop an incident response plan.

AFRL/CC COMMENT: The Air Force concurs with the DODIG recommendation. Contractor H has already been directed to establish multifactor authentication and strong passwords to access contractor networks and cloud environments that store Controlled Unclassified Information (CUI) for on-site contractor facility. Contractor H is working with its IT department and implementing an additional factor for on-site access to the server. The Contracting Officer and program office continue to monitor completion and compliance with the direction.

The Contracting Officer will ensure the contractor implements an Incident Response Plan in accordance with NIST SP 800-171 cybersecurity requirements. Contractor H has completed its draft IT Security Policy and sent to OIG on 1 September 2021 to be re-evaluated against the NIST requirements and to ensure it addresses adequate checks and testing to be compliant. This Security Policy includes Contractor H's Incident Response Plan. As of 13 October 2021,

(U) Air Force (cont'd)

(U) AFRL (cont'd)

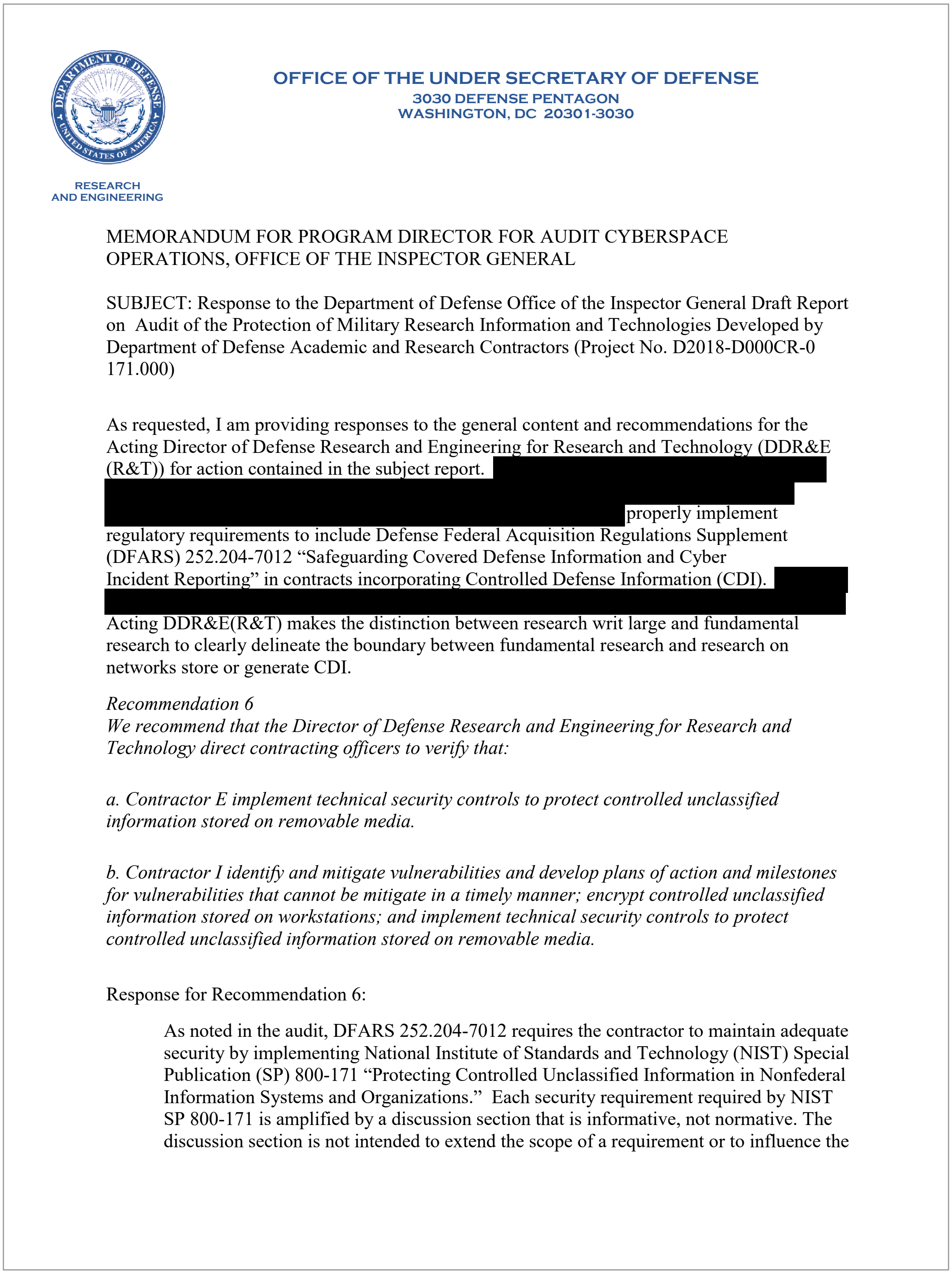


Contractor H's System Security Plan is complete and has a self-assessment score of 110 in the Supplier Performance Risk System (SPRS). The Contracting Officer and program office continue to monitor completion and compliance.

Estimated Completion Date: [redacted]

(U) Defense Research and Engineering for Research and Technology

Final Report Reference



OFFICE OF THE UNDER SECRETARY OF DEFENSE
3030 DEFENSE PENTAGON
WASHINGTON, DC 20301-3030

RESEARCH
AND ENGINEERING

MEMORANDUM FOR PROGRAM DIRECTOR FOR AUDIT CYBERSPACE OPERATIONS, OFFICE OF THE INSPECTOR GENERAL

SUBJECT: Response to the Department of Defense Office of the Inspector General Draft Report on Audit of the Protection of Military Research Information and Technologies Developed by Department of Defense Academic and Research Contractors (Project No. D2018-D000CR-0 171.000)

As requested, I am providing responses to the general content and recommendations for the Acting Director of Defense Research and Engineering for Research and Technology (DDR&E (R&T)) for action contained in the subject report. [redacted] properly implement regulatory requirements to include Defense Federal Acquisition Regulations Supplement (DFARS) 252.204-7012 "Safeguarding Covered Defense Information and Cyber Incident Reporting" in contracts incorporating Controlled Defense Information (CDI). [redacted] Acting DDR&E(R&T) makes the distinction between research writ large and fundamental research to clearly delineate the boundary between fundamental research and research on networks store or generate CDI.

Renumbered as Recommendation 5

Recommendation 6
We recommend that the Director of Defense Research and Engineering for Research and Technology direct contracting officers to verify that:

a. Contractor E implement technical security controls to protect controlled unclassified information stored on removable media.

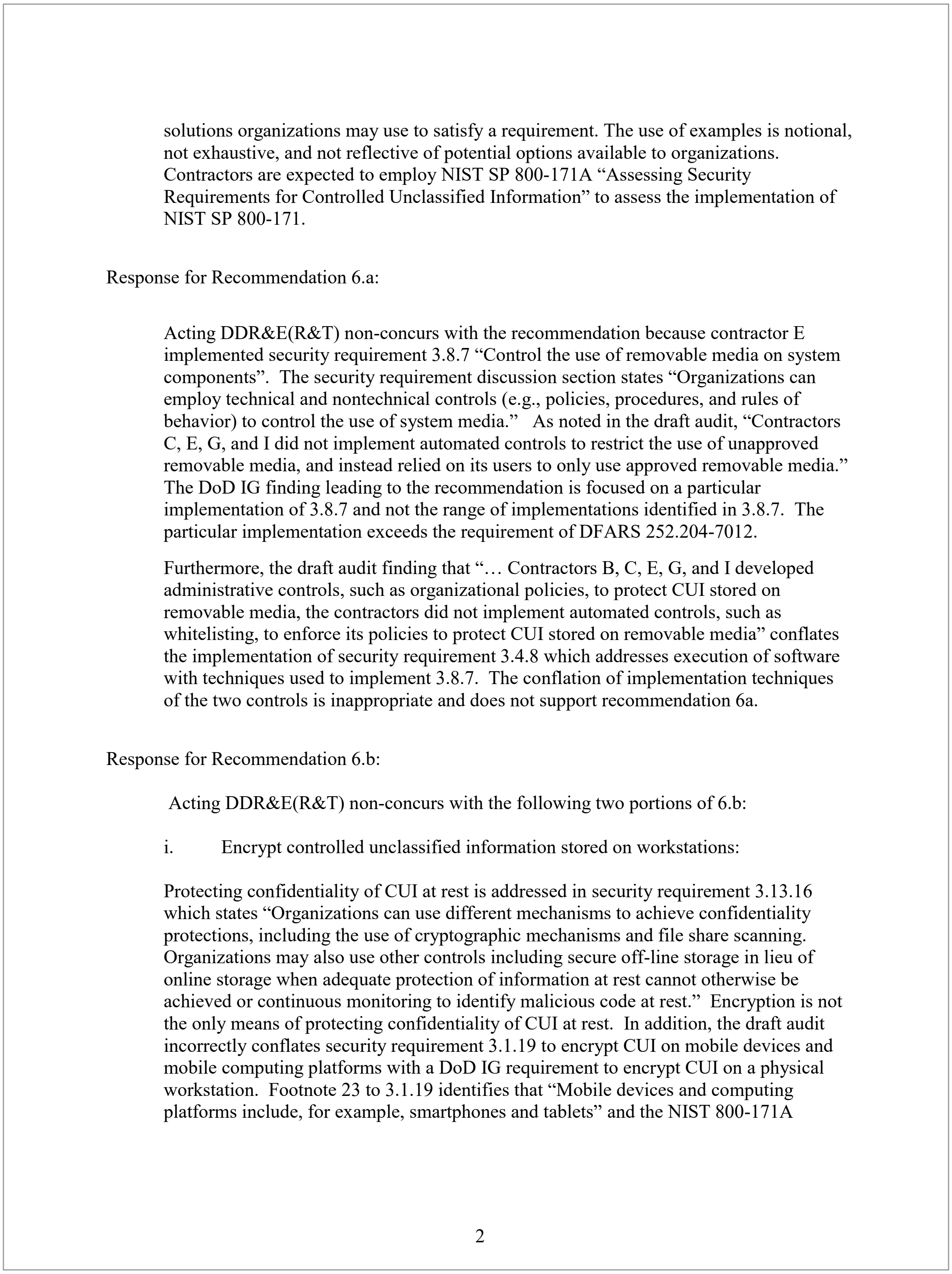
b. Contractor I identify and mitigate vulnerabilities and develop plans of action and milestones for vulnerabilities that cannot be mitigate in a timely manner; encrypt controlled unclassified information stored on workstations; and implement technical security controls to protect controlled unclassified information stored on removable media.

Response for Recommendation 6:

> As noted in the audit, DFARS 252.204-7012 requires the contractor to maintain adequate security by implementing National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations." Each security requirement required by NIST SP 800-171 is amplified by a discussion section that is informative, not normative. The discussion section is not intended to extend the scope of a requirement or to influence the

(U) Defense Research and Engineering for Research and Technology (cont'd)

Final Report Reference



solutions organizations may use to satisfy a requirement. The use of examples is notional, not exhaustive, and not reflective of potential options available to organizations. Contractors are expected to employ NIST SP 800-171A "Assessing Security Requirements for Controlled Unclassified Information" to assess the implementation of NIST SP 800-171.

Response for Recommendation 6.a:

Revised as Recommendation 5.a

Acting DDR&E(R&T) non-concurs with the recommendation because contractor E implemented security requirement 3.8.7 "Control the use of removable media on system components". The security requirement discussion section states "Organizations can employ technical and nontechnical controls (e.g., policies, procedures, and rules of behavior) to control the use of system media." As noted in the draft audit, "Contractors C, E, G, and I did not implement automated controls to restrict the use of unapproved removable media, and instead relied on its users to only use approved removable media." The DoD IG finding leading to the recommendation is focused on a particular implementation of 3.8.7 and not the range of implementations identified in 3.8.7. The particular implementation exceeds the requirement of DFARS 252.204-7012.

Furthermore, the draft audit finding that "… Contractors B, C, E, G, and I developed administrative controls, such as organizational policies, to protect CUI stored on removable media, the contractors did not implement automated controls, such as whitelisting, to enforce its policies to protect CUI stored on removable media" conflates the implementation of security requirement 3.4.8 which addresses execution of software with techniques used to implement 3.8.7. The conflation of implementation techniques of the two controls is inappropriate and does not support recommendation 6a.

Response for Recommendation 6.b:

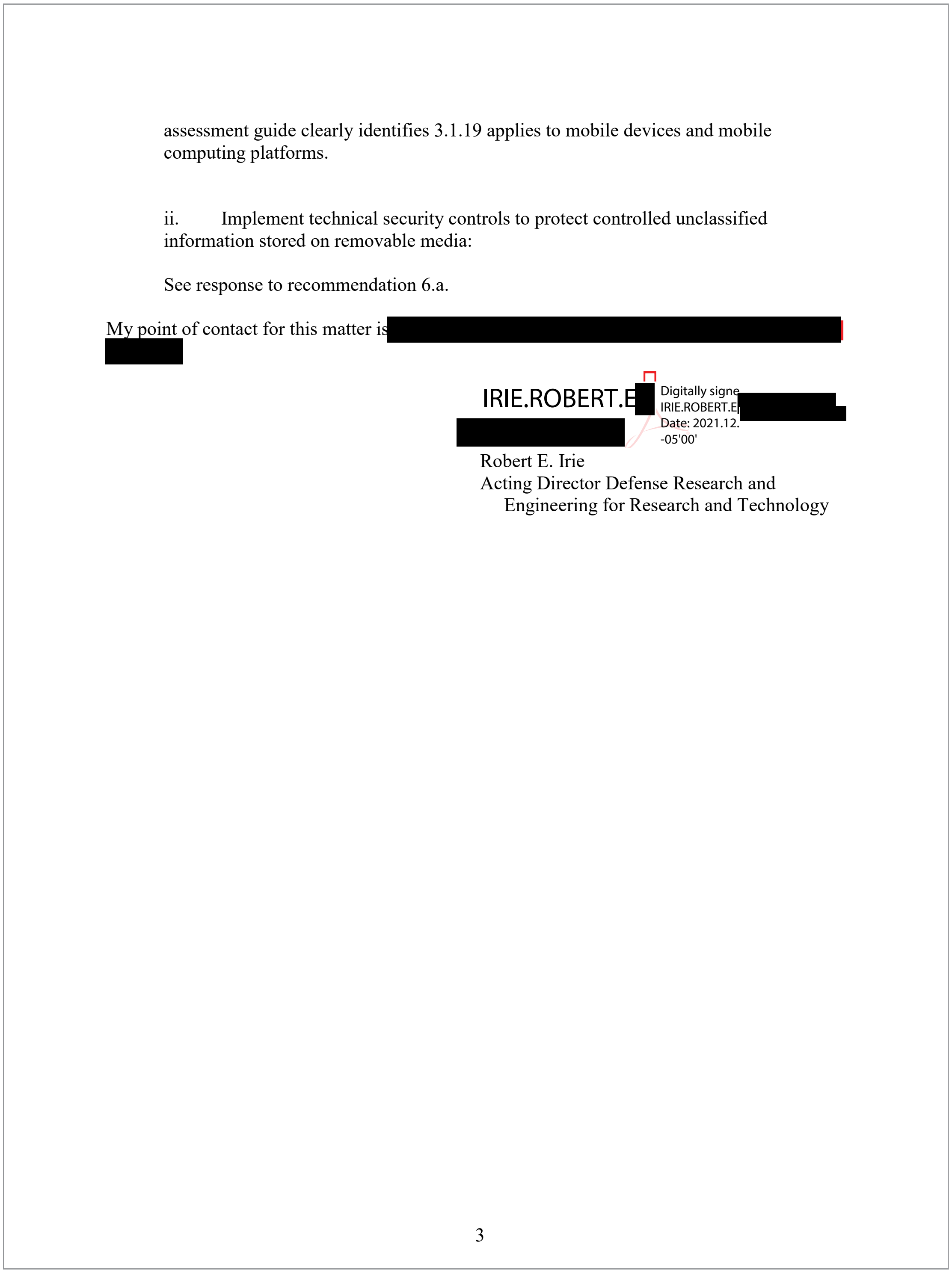
Revised as Recommendation 5.b

Acting DDR&E(R&T) non-concurs with the following two portions of 6.b:

i. Encrypt controlled unclassified information stored on workstations:

Protecting confidentiality of CUI at rest is addressed in security requirement 3.13.16 which states "Organizations can use different mechanisms to achieve confidentiality protections, including the use of cryptographic mechanisms and file share scanning. Organizations may also use other controls including secure off-line storage in lieu of online storage when adequate protection of information at rest cannot otherwise be achieved or continuous monitoring to identify malicious code at rest." Encryption is not the only means of protecting confidentiality of CUI at rest. In addition, the draft audit incorrectly conflates security requirement 3.1.19 to encrypt CUI on mobile devices and mobile computing platforms with a DoD IG requirement to encrypt CUI on a physical workstation. Footnote 23 to 3.1.19 identifies that "Mobile devices and computing platforms include, for example, smartphones and tablets" and the NIST 800-171A

(U) Defense Research and Engineering for Research and Technology (cont'd)



assessment guide clearly identifies 3.1.19 applies to mobile devices and mobile computing platforms.

ii. Implement technical security controls to protect controlled unclassified information stored on removable media:

See response to recommendation 6.a.

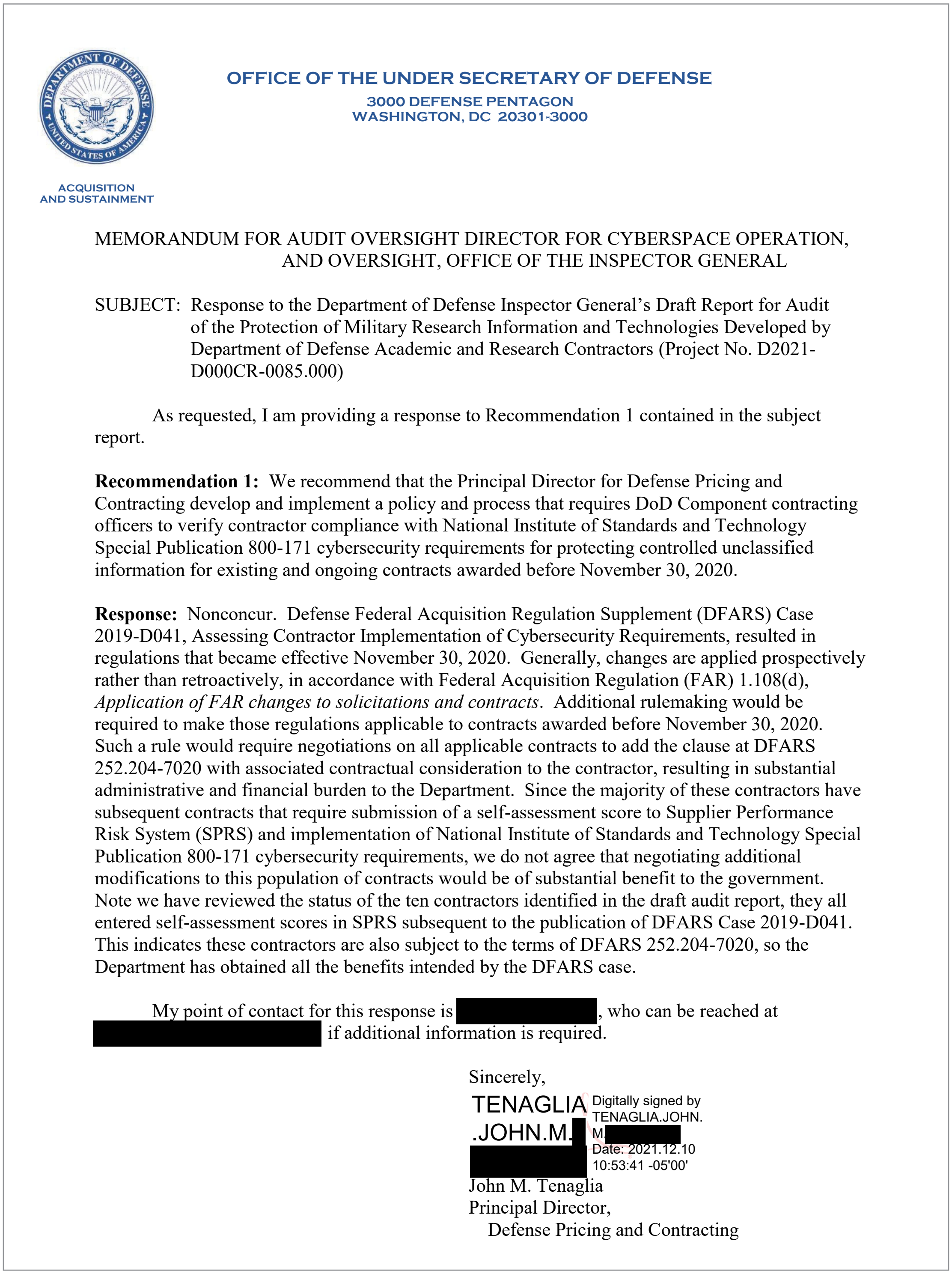
My point of contact for this matter is [redacted]

IRIE.ROBERT.E[redacted]
[redacted]
Digitally signe[redacted]
IRIE.ROBERT.E[redacted]
Date: 2021.12.
-05'00'

Robert E. Irie
Acting Director Defense Research and
Engineering for Research and Technology

(U) Defense Pricing and Contracting

Final Report Reference



OFFICE OF THE UNDER SECRETARY OF DEFENSE
3000 DEFENSE PENTAGON
WASHINGTON, DC 20301-3000

ACQUISITION
AND SUSTAINMENT

MEMORANDUM FOR AUDIT OVERSIGHT DIRECTOR FOR CYBERSPACE OPERATION, AND OVERSIGHT, OFFICE OF THE INSPECTOR GENERAL

SUBJECT: Response to the Department of Defense Inspector General's Draft Report for Audit of the Protection of Military Research Information and Technologies Developed by Department of Defense Academic and Research Contractors (Project No. D2021-D000CR-0085.000)

As requested, I am providing a response to Recommendation 1 contained in the subject report.

Recommendation 1: We recommend that the Principal Director for Defense Pricing and Contracting develop and implement a policy and process that requires DoD Component contracting officers to verify contractor compliance with National Institute of Standards and Technology Special Publication 800-171 cybersecurity requirements for protecting controlled unclassified information for existing and ongoing contracts awarded before November 30, 2020.

Revised Recommendation 1

Response: Nonconcur. Defense Federal Acquisition Regulation Supplement (DFARS) Case 2019-D041, Assessing Contractor Implementation of Cybersecurity Requirements, resulted in regulations that became effective November 30, 2020. Generally, changes are applied prospectively rather than retroactively, in accordance with Federal Acquisition Regulation (FAR) 1.108(d), *Application of FAR changes to solicitations and contracts*. Additional rulemaking would be required to make those regulations applicable to contracts awarded before November 30, 2020. Such a rule would require negotiations on all applicable contracts to add the clause at DFARS 252.204-7020 with associated contractual consideration to the contractor, resulting in substantial administrative and financial burden to the Department. Since the majority of these contractors have subsequent contracts that require submission of a self-assessment score to Supplier Performance Risk System (SPRS) and implementation of National Institute of Standards and Technology Special Publication 800-171 cybersecurity requirements, we do not agree that negotiating additional modifications to this population of contracts would be of substantial benefit to the government. Note we have reviewed the status of the ten contractors identified in the draft audit report, they all entered self-assessment scores in SPRS subsequent to the publication of DFARS Case 2019-D041. This indicates these contractors are also subject to the terms of DFARS 252.204-7020, so the Department has obtained all the benefits intended by the DFARS case.

My point of contact for this response is [redacted], who can be reached at [redacted] if additional information is required.

Sincerely,

TENAGLIA.JOHN.M.[redacted] Digitally signed by TENAGLIA.JOHN.M.[redacted] Date: 2021.12.10 10:53:41 -05'00'

John M. Tenaglia
Principal Director,
Defense Pricing and Contracting

(U) Acronyms and Abbreviations

(U) AFRL	Air Force Research Laboratory
(U) CUI	Controlled Unclassified Information
(U) DDR&E	Director of Defense Research and Engineering
(U) DFARS	Defense Federal Acquisition Regulation Supplement
(U) DPC	Defense Pricing and Contracting
~~(CUI)~~ [redacted]	[redacted]
(U) FPDS	Federal Procurement Data System
(U) GAO	Government Accountability Office
(U) NAVSEA	Naval Sea Systems Command
(U) NIST	National Institute of Standards and Technology
(U) POA&M	Plan of Action and Milestones
(U) R&T	Research and Technology
(U) SP	Special Publication
~~(CUI)~~ [redacted]	[redacted]

(U) Glossary

(U) Access Control. The process of granting or denying specific requests for obtaining and using information-processing services to enter specific physical facilities.

(U) Active Directory. A Microsoft technology used to manage computers and other devices on a network that allows network administrators to create and manage groups of computers, users, and computer interaction within a network.

(U) Authentication. Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system.

(U) Availability. Ensuring timely and reliable access to, and the use of, information.

(U) Boundary Protection. Monitoring and control of communications at the external boundary of a network or an information system to prevent and detect malicious and other unauthorized communications using boundary protection devices (such as proxies, gateways, routers, firewalls, and encrypted tunnels).

(U) Brute Force Password Attack. A method of accessing a device by attempting multiple combinations of passwords.

(U) Confidentiality. The property that information is not disclosed to system entities (users, processes, or devices) unless they have been authorized to access the information.

(U) Configuration Settings. The set of parameters that can be changed in hardware, software, or firmware that affect the security posture or functionality of the system.

(U) Controlled Unclassified Information (CUI). Information created or possessed on behalf of the Government that requires safeguarding or dissemination controls according to applicable laws, regulations, and Government-wide policies.

(U) Critical Vulnerabilities. If exploited, would likely result in unauthorized privileged access to servers and information systems and, therefore, require immediate patches.

(U) Cyberattack. An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment or infrastructure, destroying the integrity of the data, or stealing controlled information.

(U) Data-at-Rest. Information that resides in a stationary location such as on a server or workstation.

(U) Enclave. An isolated network that is protected by the security controls in place around the overall organizational network.

(U) Encryption. The process of changing plain text to an unreadable format for the purpose of security or privacy.

(U) Full-disk Scan. Checks all files on the hard disk and all running programs.

(U) High Vulnerabilities. If exploited, could result in obtaining unauthorized elevated privileges, significant data loss, and network downtime.

(U) Incident Response. Procedures to detect, respond to, and mitigate the consequences of malicious cyberattacks against an organization's information systems.

(U) Integrity. The property whereby an entity has not been modified in an unauthorized manner.

(U) Malicious Actions. Activities that seek to compromise or impair the confidentiality, integrity, or availability of computers, information or communications systems, networks, physical or virtual infrastructure controlled by computers or information systems, or information residing on any of these systems.

(U) Malicious Code. Software that has an adverse impact on the confidentiality, integrity, or availability of an information system, such as a virus.

(U) Multifactor Authentication. Authentication using two or more different factors to achieve authentication. Factors include something known to the user (for example, a personal identification number or password), something in the user's possession (for example, a cryptographic identification device or token), or a physical aspect of the user (such as biometric information).

(U) Network. A system of interconnected components including routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.

(U) Network Access. Access to a system by a user (or a process acting on behalf of a user) communicating through a network (for example, the Internet) or an internal network.

(U) Non-privileged Accounts. Accounts not authorized to perform security-related functions.

(U) Plan of Action and Milestones (POA&M). A document that identifies the resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

(U) Removable Media. Portable electronic storage devices that can be inserted into and removed from a computer. Examples include hard disks, floppy disks, Zip drives, compact discs, thumb drives, and similar Universal Serial Bus (USB) storage devices.

(U) Safeguards. Protective measures prescribed to meet the security requirements (confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices.

(U) Security Control. A safeguard or countermeasure prescribed for a system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.

(U) Single-Factor Authentication. A less stringent authentication method, such as the use of a username and password, which presents a greater risk of malicious actors compromising networks and systems.

(U) Token. Used to authenticate a user's identity.

(U) Trusted Platform Module Chip. A tamper-resistant circuit that is built into a computer to encrypt and protect sensitive information.

(U) Vulnerability. A weakness in a system, application, or network that could be exploited by a threat.

(U) Whitelisting. A list of devices, such as removable media, approved for use on an organization's systems and network.

(U) Workstation. A desktop computer terminal, which is normally connected to a network and more powerful than a personal computer.

INSPECTOR GENERAL

INTEGRITY EFFICIENCY

DEPARTMENT OF DEFENSE

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 http://www.dodig.mil/Components/Administrative-Investigations/Whistleblower-Reprisal-Investigations/Whisteblower-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

DoD OIG Mailing Lists
www.dodig.mil/Mailing-Lists/

Twitter
www.twitter.com/DoD_IG

DoD Hotline
www.dodig.mil/hotline

DEPARTMENT OF DEFENSE | OFFICE OF INSPECTOR GENERAL

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