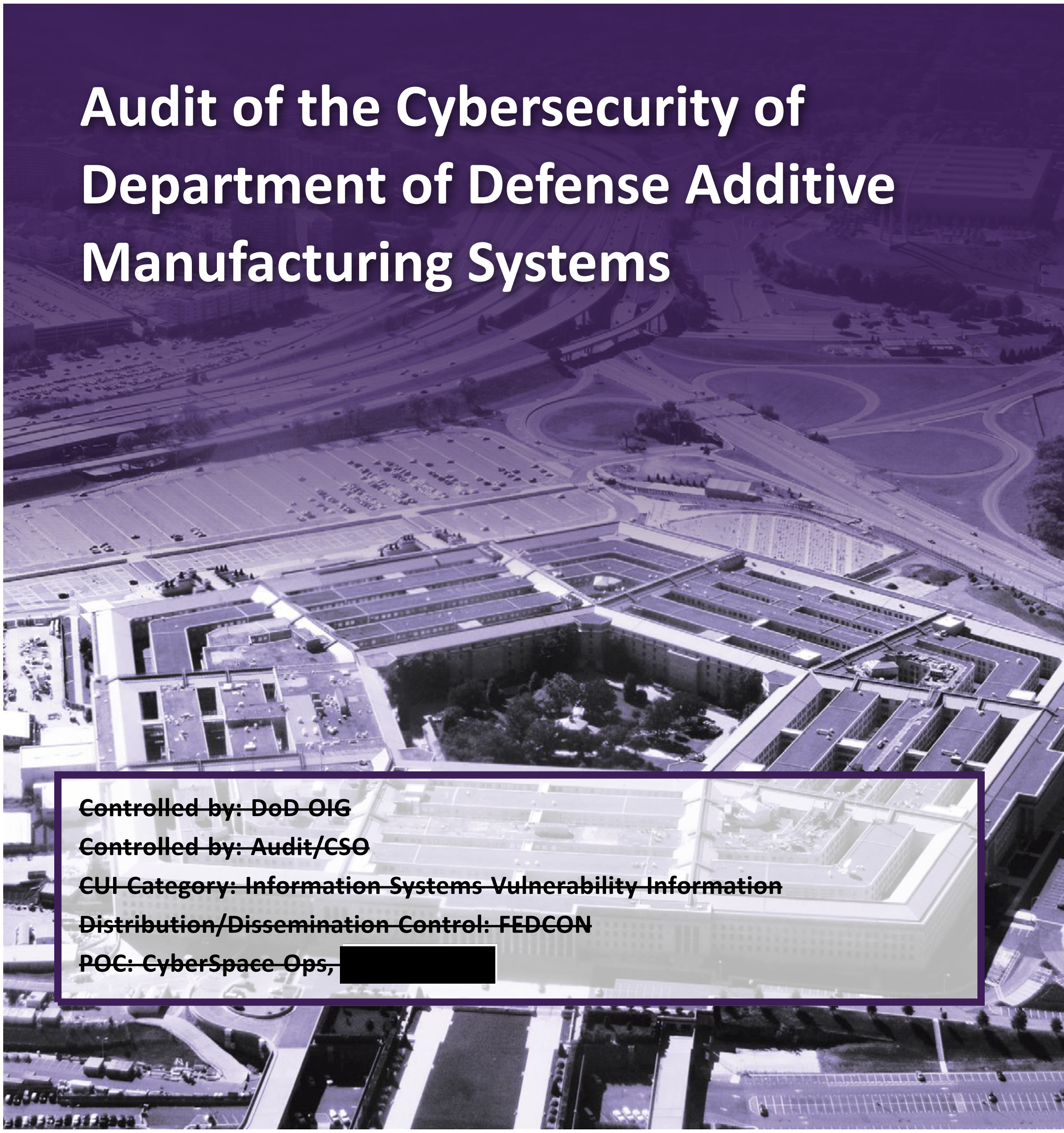
Report No. DODIG-2021-098

INSPECTOR GENERAL

U.S. Department of Defense

JULY 1, 2021



Audit of the Cybersecurity of Department of Defense Additive Manufacturing Systems

~~Controlled by: DoD OIG~~
~~Controlled by: Audit/CSO~~
~~CUI Category: Information Systems Vulnerability Information~~
~~Distribution/Dissemination Control: FEDCON~~
~~POC: CyberSpace Ops,~~ [redacted]

INTEGRITY ★ INDEPENDENCE★ EXCELLENCE

Results in Brief

Audit of the Cybersecurity of Department of Defense Additive Manufacturing Systems

July 1, 2021

Objective

The objective of this audit was to determine whether DoD Components secured additive manufacturing (AM) systems to prevent unauthorized changes and ensure the integrity of the design data. AM systems are printers and computer workstations used to develop three-dimensional (3-D) products.

Background

AM creates 3-D physical objects by adding layers of material from a digital description of the product's design. AM is used to build physical models, prototypes, patterns, and production parts in plastic, metal, ceramic, and glass. The DoD uses AM to improve its logistics support and increase materiel readiness. For example, the DoD uses AM to create molds for personal protection body armor, parts for tactical vehicles, brackets for weapons systems, and medical implants and prostheses (artificial body parts). The DoD also uses AM to create spare parts on demand, which reduces the need to store or maintain large on hand inventories, allowing units to relocate quickly if mission requirements change.

Findings

DoD Component officials at the five sites we reviewed did not consistently secure or manage their AM systems to prevent unauthorized changes and ensure the integrity of the design data. Officials at the five sites generally had controls in place or corrected the minor deficiencies we identified for managing user accounts, configuring authentication factors, accounting for AM assets, and implementing physical security controls. However, officials at:

- ~~(CUI)~~ [redacted]
- ~~(CUI)~~ [redacted]
- ~~(CUI)~~ [redacted]

The DoD Components did not consistently secure or manage their AM systems or design data because AM users considered the AM systems as "tools" to generate supply parts instead of information technology systems that required cybersecurity controls. In addition, the DoD Components incorrectly categorized the AM systems as stand-alone systems and erroneously concluded that the systems did not require an authority to operate.[1]

As a result, DoD Components were unaware of existing AM system vulnerabilities that exposed the DoD Information Network to unnecessary cybersecurity risks. Unless the DoD properly protects the confidentiality and integrity of its AM systems and design data, internal or external malicious actors could compromise AM systems to steal the design data or gain access to the DoD Information Network. The compromise of AM design data could allow an adversary to re-create and use DoD's technology to the adversary's advantage on the battlefield. In addition, if malicious actors change the AM design data, the changes could affect the end strength and utility of the 3D-printed products.

[1] To obtain an authority to operate, DoD Components must conduct a risk assessment, identify risks to the system, and implement security controls for identifying and mitigating those risks.

Results in Brief

Audit of the Cybersecurity of Department of Defense Additive Manufacturing Systems

Recommendations

We recommend that the DoD Chief Information Officer (CIO), in coordination with the Under Secretary of Defense for Research and Engineering (USD[R&E]), and the Under Secretary of Defense for Acquisition and Sustainment (USD[A&S]), include additive manufacturing systems in the information technology systems portfolio and establish and maintain cybersecurity controls in accordance with Federal and DoD guidance.

We recommend that the DoD Chief Information Officer require AM system owners to immediately identify and implement security controls to minimize risk until obtaining an authority to operate.

We recommend that the DoD Chief Information Officer and the DoD Component CIOs, in coordination with designated AM Leads, require all AM systems to obtain an authority to operate in accordance with DoD policy before their use.

Finally, we recommend that the DoD Component Commanders or Director update all AM computer operating systems to Windows 10, or obtain an approved waiver; scan all AM systems for vulnerabilities, or have exceptions to regularly scanning documented in an approved authority to operate; and label, secure, and scan, as applicable, all removable media devices connected to AM systems in accordance with DoD guidance.

Management Comments and Our Response

The DoD CIO disagreed that cybersecurity guidance should be established for AM systems, stating that DoD Instructions 8500.01 and 8510.01 require all systems, including AM systems, to apply cybersecurity controls and undergo a final risk determination and authorization decision. We agree with the DoD CIO that DoD Instructions 8500.01 and 8510.01 are applicable to all information systems; however, the AM system owners did not consider the AM systems as information systems and to reduce the risk of continued noncompliance, specific guidance is needed. Further, although the DoD CIO disagreed, the actions taken and planned by the USD(R&E), USD(A&S), and the DoD Components meet the intent of the recommendation. Therefore, we will close the recommendation once the USD(R&E) and USD(A&S) provide copies of guidance requiring AM systems to be included in the information technology portfolio and to be in compliance with Federal and DoD cybersecurity controls.

The DoD Component CIOs, in coordination with designated AM Leads, agreed to require all AM systems to obtain an authority to operate in accordance with DoD policy before use, unless a waiver is granted. We will close the recommendation once the DoD Component CIOs provide approved guidance requiring all AM systems to obtain an authority to operate.

The DoD Component Commanders or Director agreed to update all AM computer operating systems to Windows 10, or obtain a waiver; scan all AM systems for vulnerabilities or have an exception; and label, secure, and scan all applicable removable media devices connected to AM systems in accordance with DoD guidance. We will close the recommendations once the DoD Components Commanders or Director provide documentation showing that all AM computers are using the Windows 10 operating system; all AM systems have been scanned for vulnerabilities; and, removable media devices have been labelled, secured, and scanned in accordance with DoD guidance.

Please see the Recommendations Table on the next page for the status of the recommendations.

Recommendations Table

Management	Recommendations Unresolved	Recommendations Resolved	Recommendations Closed
Under Secretary of Defense for Research and Engineering		1	
Under Secretary of Defense for Acquisition and Sustainment		1	
DoD Chief Information Officer		1, 3	2
Department of the Navy, Chief Information Officer		3	
U.S. Marine Corps, Deputy Commandant for Information		3	
U.S. Air Force, Chief Information Officer		3	
U.S. Marine Corps 1st Marine Expeditionary Force, Commander		4.a, 4.b	
Navy Fleet Readiness Center Southwest, Commander		5.a, 5.b, 5.c	
Naval Information Warfare Center Pacific, Commander		6	
Air Force 60th Maintenance Group, Commander		7.a, 7.b, 7.c	
Defense Health Agency, Chief Information Officer		3	
Walter Reed National Military Medical Center, Director		8.a, 8.b	

Please provide Management Comments by September 30, 2021.

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

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

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

July 1, 2021

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Audit of the Cybersecurity of Department of Defense Additive Manufacturing Systems (Report No. DODIG-2021-098)

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. Those comments are included in the report.

This report contains 1 recommendation that is closed and 13 recommendations that are considered resolved. Therefore, as discussed in the Recommendations, Management Comments, and Our Response section of this report, the resolved recommendations will remain open until adequate documentation has been submitted showing that the agreed-upon actions have been completed. Once we verify that the actions are complete, the recommendations will be closed.

For the resolved recommendations, please provide us within 90 days documentation showing that the agreed-upon actions have been completed. Send your response to either [redacted] if unclassified or [redacted] if classified SECRET. Responses must have the actual signature of the authorizing official for your organization.

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

Carol N. Gorman

Carol N. Gorman
Assistant Inspector General for Audit
Cyberspace Operations

Distribution:

SECRETARY OF THE NAVY
SECRETARY OF THE AIR FORCE
UNDER SECRETARY OF DEFENSE FOR RESEARCH AND ENGINEERING
UNDER SECRETARY OF DEFENSE FOR ACQUISITION AND SUSTAINMENT
CHIEF INFORMATION OFFICER OF THE DEPARTMENT OF DEFENSE
DIRECTOR, DEFENSE HEALTH AGENCY
AUDITOR GENERAL, DEPARTMENT OF THE NAVY
AUDITOR GENERAL, DEPARMENT OF THE AIR FORCE

Contents

Introduction

Finding. The DoD Components Did Not Consistently Secure and Manage Additive Manufacturing Systems or Design Data 7

Appendixes

Management Comments

Contents (cont'd)

Introduction

Objective

The objective of this audit was to determine whether DoD Components secured additive manufacturing (AM) systems to prevent unauthorized changes and ensure the integrity of the design data.

We initially selected a nonstatistical sample of nine DoD Component sites that manage AM systems to review.[2] The DoD Component sites consisted of one Army, one Marine Corps, two Navy, two Air Force, two Special Operations Commands (Marine Corps and Navy), and one Defense Health Agency (DHA) sites. On March 13, 2020, the DoD Deputy Secretary of Defense issued a stop movement order for domestic travel due to the coronavirus disease–2019 (COVID-19) pandemic.[3] The stop movement order affected the execution phase of this audit and we were unable to conduct all initial and followup site visits, as planned. As a result, we reduced the sample size to five DoD Component sites—the 1st Marine Expeditionary Force (1st MEF), the Navy Fleet Readiness Center Southwest (FRC-SW), the Naval Information Warfare Center Pacific (NIWC-P), the Air Force 60th Maintenance Group (MXG), and the DHA Walter Reed National Military Medical Center (WRNMMC). See Appendix A for a discussion on the scope and methodology.

Background

AM creates three-dimensional (3-D) physical objects by adding layers of material from a digital description of the product's design. AM is used to build models, prototypes, patterns, and production parts in plastic, metal, ceramic, and glass. The DoD uses AM to improve its logistics support and increase materiel readiness. For example, the DoD uses AM to create molds for personal protection body armor, parts for tactical vehicles, brackets for weapons systems, and medical implants and prostheses (artificial body parts). The DoD also uses AM to create spare parts on demand, which reduces the need to store or maintain large on hand inventories, allowing units to relocate quickly if mission requirements change. Figures 1 and 2 are examples of 3-D parts printed by DoD Components.

[2] For purposes of this report, AM systems refer to AM printers and computer workstations used to control the printers and to develop three-dimensional products.

[3] Deputy Secretary of Defense Memorandum, "Stop Movement for all Domestic Travel for DoD Components in Response to Coronavirus Disease 2019," March 13, 2020.

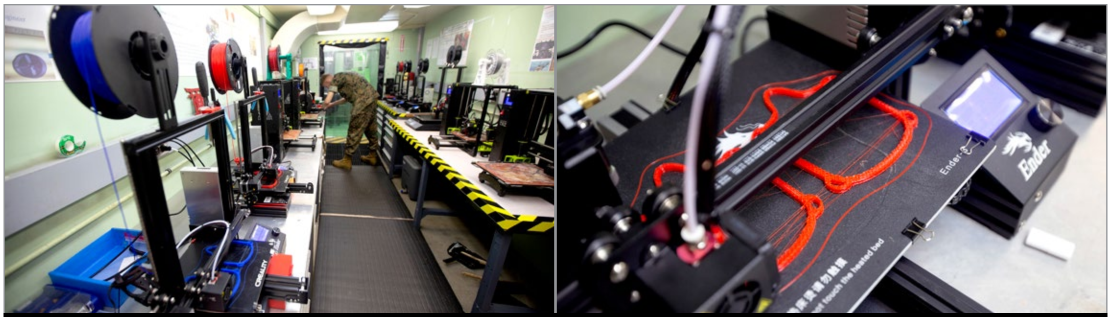


Figure 1. Marine Air Logistics Squadron Printing Mask Frames, Face Shields, and Surgical Masks in Support of the DoD Response to the COVID-19 Pandemic
Source: The Defense Logistics Agency.

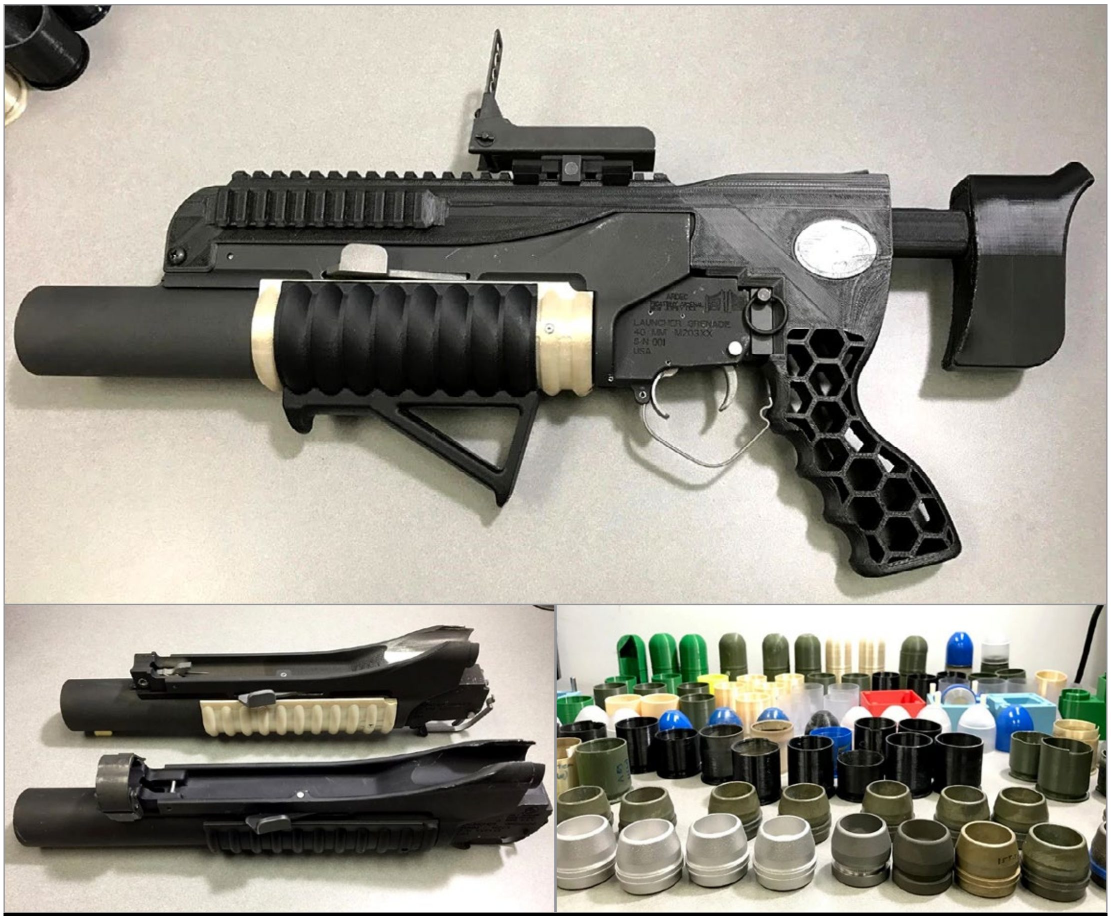
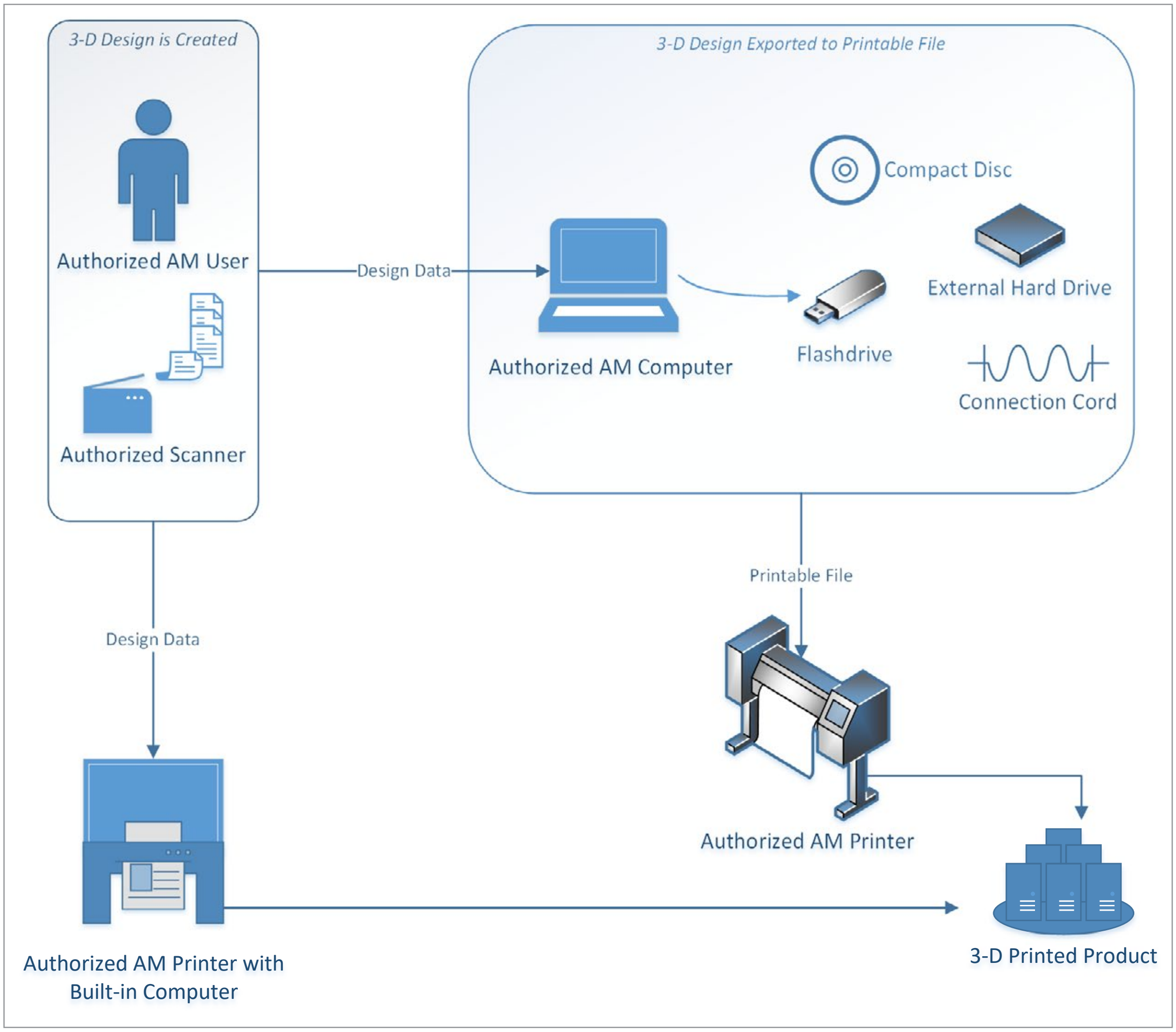


Figure 2. A 3-D Printed Grenade Launcher (Top), Grenade Launcher Parts (Bottom Left), and Miscellaneous Parts (Bottom Right)
Source: The U.S. Army Armament, Research, Development, and Engineering Center.

Additive Manufacturing Printing Process

AM system users print 3-D products in three phases.[4] During the first phase, the user creates a digital design on a computer for the 3-D product using computer-aided design software as an original design or based on output from a 3-D scanner.[5] In the second phase, the user exports the digital design to a 3-D compatible printable file and then imports the file to a slicing software that translates the file into instructions that the 3-D printer can understand.[6] In the third phase, the user sends the sliced file, including instructions on layering, to the AM system to print the 3-D product. Figure 3 shows the AM printing process.

Figure 3. The AM Printing Process



Source: The DoD OIG.

[4] The three-phase process is the description of the AM process based on our audit observations.

[5] Computer aided design software is used to develop and document design-drawings for manufacturing, which assists in developing parts through the 3-D printing process by eliminating hours of manual drawing.

[6] Slicing is the process of converting a 3-D model into a series of instructions for the printer to carry out.

As shown in Figure 3, AM printers can have a built-in computer that directly prints the 3-D product or the computer and AM printer can be separate devices. For the separate devices, a single computer may be connected to one or more AM printers or multiple computers can be connected to the printer via a network. AM system users can also download design data to removable media and transport the data to an AM printer.[7]

DoD Additive Manufacturing

On November 30, 2016, the DoD published an AM roadmap to coordinate AM activities across the DoD.[8] The roadmap sets goals and objectives to integrate AM into DoD doctrine and identifies the following cybersecurity goals for the use of AM.

- Secure the AM information technology infrastructure;
- Ensure that AM data are protected from internal and external threats; and,
- Develop techniques to safeguard design AM data throughout the production process.

In July 2017, the Under Secretary of Defense for Acquisition, Technology, and Logistics established the Joint AM Steering Group and the Joint AM Working Group.[9] The groups were tasked to develop a DoD AM vision, identify AM best practices, share information on AM efforts throughout the DoD, and provide recommendations for a joint AM investment strategy.

On March 21, 2019, the USD for Acquisition and Sustainment (A&S) issued Directive-Type Memorandum 19-006 to assign responsibilities to the USD Research and Engineering (R&E), USD(A&S), Military Departments, and Defense agencies to ensure the safe and effective use of AM in the DoD sustainment enterprise.[10] Specifically, the memorandum stated that the USD(R&E), in coordination with the USD(A&S), is responsible for overseeing the use of AM in the DoD. It also states that the USD(R&E) leads the Joint AM Steering Group and the Joint AM Working Group, aligns AM investments with DoD priorities, and develops policy for

[7] Removable media is a portable device that can be inserted into and removed from an information system or network to provide data storage.

[8] DoD, "DoD Additive Manufacturing Roadmap," November 30, 2016.

[9] During the 2018 reorganization of the Office of the Under Secretary of Defense For Acquisition, Technology, and Logistics, the office was split into the Under Secretary Of Defense (USD) for Research and Engineering (R&E) and the USD for Acquisition and Sustainment (A&S). USD R&E and A&S established the Joint Defense Manufacturing Council, which absorbed the Joint AM Steering Group and serves as the oversight organization for the Joint AM Working Group.

[10] Directive-Type Memorandum 19-006, "Interim Policy and Guidance for the Use of Additive Manufacturing in Support of Materiel Sustainment," March 21, 2019 (incorporating Change 1 June 26, 2020). The Directive-Type Memorandum expired on December 31, 2020.

AM research and engineering efforts. The memorandum required the USD(A&S) to review and develop AM acquisition policy to support the AM digital and cyber infrastructure for sustainment operations.

Cybersecurity Controls Assessed

At the five DoD Component sites visited, we reviewed cybersecurity controls over the AM systems used to print 3-D parts. The AM systems reviewed consisted of 73 AM printers and 46 computers, of which three of the computers were built into the AM printers. We reviewed security controls in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 and NIST Internal Report 8183 to identify baseline controls for protecting information systems.[11] We focused our review on the seven cybersecurity controls that, if not in place, we determined could present a higher-risk to DoD Components to protect AM systems from unauthorized changes and modification of the design data.[12] Table 1 identifies the cybersecurity controls assessed and their importance to AM systems.

Table 1. Cybersecurity Controls Assessed and Their Importance for AM Systems

Cybersecurity Control	Importance of Cybersecurity Control for AM Systems
Operating System Updates	An operating system is software that starts up a computer and keeps it running and responding to user commands. It also runs the applications and enables the user to interact with the applications. Updating the operating system is critical to mitigating threats because the updates provide security features that are not available in older versions of the software. If updates are not consistently and timely made, the risk that malicious actors could exploit the security weakness is increased, which could cause damage or disruption to systems or their associated network.
Use of Authentication Factors	Authentication is the process of verifying the identity of a user of a system by using authentication factors, such as a user name and password. Enabling and protecting authentication factors is important because they can protect an information system or network from unauthorized access. Authentication factors can also be used to limit the files and resources users can access and the system actions they can perform. If authentication factors are not in place, an unauthorized person could access a system and its data.

[11] NIST SP 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," Revision 4, April 2013, was superseded by NIST SP 800-53, "Security and Privacy Controls for Information Systems and Organizations," Revision 5, September 23, 2020. However, our findings and conclusions were based on NIST SP 800-53, Revision 4, because it was effective during the audits. NIST Internal Report 8183, "Cybersecurity Framework Manufacturing Profile," September 2017 (Including Updates as of May 20, 2019).

[12] See Appendix B for a list of Federal and DoD guidance that establishes cybersecurity controls for protecting information systems, including AM systems.

Table 1. Cybersecurity Controls Assessed and Their Importance for AM Systems (cont'd)

Cybersecurity Control	Importance of Cybersecurity Control for AM Systems
Unauthorized User Accounts	Unauthorized user accounts are those that can still be accessed by a user but the user no longer has a valid need to access the system. Once a user no longer has a valid need to access a system, the user's account should be disabled, suspended, or removed.
Vulnerability Identification	System vulnerabilities are weaknesses in an information system or system security procedures that can expose the system to adverse threats. Vulnerability identification includes efforts such as scanning to identify potential weaknesses that could be exploited on systems and networks. Identifying and mitigating vulnerabilities reduces a malicious actor's ability to gain access to systems and networks and insert spyware or other malware.
Protection of Removable Media	Removable media are portable devices such as compact discs or external hard drives that connect to information systems or networks to store and transfer data. Protecting removable media involves proper labeling, secure storage, and monitoring the use of the devices. Since removable media is portable, improper protection of the media presents an unsophisticated means to steal data or insert spyware or other malware.
Property Accountability	DoD Components establish property accountability upon receipt, delivery, or acceptance of an asset by maintaining a record of the property in a system or establishing a managerial record. Accountability of property allows DoD Components to accurately account for and manage all assets, including information technology equipment, and protect the assets against unauthorized use, disclosure, or loss.
Implementation of Physical Security	Physical security includes active and passive security measures designed to prevent unauthorized access to equipment, installations, information, and to safeguard them against damage and criminal activity. Physical security can include procedures such as physical barriers, facility hardening, and secure locking systems. If physical security measures are not implemented or enforced, malicious actors could potentially access an installation and damage or steal equipment and information.

Source: The DoD OIG.

Review of Internal Controls

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.[13] We identified internal control weaknesses related to performing regular or scheduled operating system updates, identifying network or system vulnerabilities, and tracking or securing removable media. We will provide a copy of the final report to the senior official responsible for internal controls in the Marine Corps, the Navy, the Air Force, OUSD(R&E), OUSD(A&S), U.S. Cyber Command, DoD Chief Information Officer, and the DHA.

[13] DoDI 5010.40, "Managers' Internal Control Program Procedures," May 30, 2013.

Finding

The DoD Components Did Not Consistently Secure and Manage Additive Manufacturing Systems or Design Data

DoD Component officials at the five sites we reviewed did not consistently secure or manage their AM systems to prevent unauthorized changes and ensure the integrity of the design data. Officials at the five sites generally had controls in place or corrected the minor deficiencies we identified for managing user accounts, configuring authentication factors, accounting for AM assets, and implementing physical security controls. However, officials at:

- ~~(CUI)~~ [redacted]
- ~~(CUI)~~ [redacted]
- ~~(CUI)~~ [redacted]

The DoD Components did not consistently secure or manage their AM systems or design data because AM users considered the AM systems as "tools" to generate supply parts instead of information technology systems that required cybersecurity controls. In addition, the DoD Components incorrectly categorized the AM systems as stand-alone systems and erroneously concluded that the systems did not require an authority to operate (ATO).[14]

As a result, DoD Components were unaware of existing AM system vulnerabilities that exposed the DoD Information Network (DODIN) to unnecessary cybersecurity risks.[15] Unless the DoD properly protects the confidentiality and integrity of its AM systems and design data, internal or external malicious actors could compromise AM systems to steal the design data or gain access to the DODIN. The compromise of AM design data could allow an adversary to re-create and use DoD's technology to the adversary's advantage on the battlefield. In addition, if malicious actors change the AM design data, the changes could affect the end strength and utility of the 3D-printed products.

[14] To obtain an ATO, DoD Components must conduct a risk assessment, identify risks to the system, and implement security controls for identifying and mitigating those risks.

[15] The DODIN is a globally interconnected, set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, including computing systems and services, software, data, security services, other associated services, and national security systems.

Cybersecurity Controls Were Generally Implemented

DoD Component officials at the five sites generally had controls in place to manage user accounts, configure authentication factors, account for AM assets, and implement physical security controls. Although we identified minor deficiencies concerning those controls, officials took action to correct the deficiencies after our site visit and; therefore, we do not make recommendations specific to managing user accounts, configuring authentication factors, accounting for AM assets, and implementing physical security controls in this report.

For example, we reviewed whether user accounts were disabled, suspended, or removed when users no longer required access to the AM systems. We identified two users at WRNMMC, whose accounts should have been disabled and we notified WRNMMC officials, who took immediate action to disable the accounts. Similarly, in our review of the use of authentication factors, we identified an AM computer at the Navy FRC-SW that could be accessed without a Common Access Card or a username and password, thereby making the computer accessible to anyone who simply touched the keyboard. After our site visit, Navy FRC-SW officials enabled the authentication factor for the noncompliant AM computer. The Command information systems security manager (ISSM) confirmed that the authentication factor was enabled.[16]

We also reviewed whether the 46 AM computers and 73 AM printers were properly accounted for on the site property books, and identified three printers that were not. Two of the three printers were located at the 60th MXG AM and one at WRNMMC. Once we notified officials at those sites of the discrepancies, they took action to add the AM printers to their respective property books. The officials provided copies of the revised property books and we verified that the corrective action was taken. Likewise, of the 46 AM computers and the 73 AM printers that we reviewed for physical security, only 1 AM computer at NIWC-P was stored in a space where a door did not close properly. NIWC-P officials took action to repair the door and sent us a copy of the maintenance report to verify that the corrective action was taken.

Cybersecurity Controls Were Not Implemented

DoD Component officials at the five sites did not have controls in place to update operating systems, scan for vulnerabilities, or control removable media. Table 2 summarizes the control deficiencies identified by cybersecurity control and site.

[16] An ISSM is the individual responsible for the information assurance of a program, organization, or system.

Table 2. Control Deficiencies DoD Component Site

~~(CUI)~~ Cybersecurity Controls	1st MEF	Navy FRC-SW	NIWC-P	60th MXG	WRNMMC
Operating systems not updated	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Vulnerability scans not conducted	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Removable media not properly controlled	[redacted]	[redacted]	[redacted]	[redacted]	[redacted] ~~(CUI)~~

Source: The DoD OIG.

Operating Systems Were Not Consistently Updated

~~(CUI)~~ DoD Component officials [redacted] did not perform regular or scheduled operating system updates on their AM systems. Specifically, 35 of the 46 AM computers did not have updated operating systems.[17] All 46 computers had Microsoft operating systems and should have been using Microsoft Windows 10, as required by a February 26, 2016, Deputy Secretary of Defense memorandum.[18] According to the memorandum, Microsoft Windows 10 provides security features that are not available in older versions of Windows.

To determine whether the DoD Component officials were operating the most current version of Microsoft Windows 10, we reviewed the Microsoft Windows version and the operating system update status in the Windows settings of the AM computers.

~~(CUI)~~ Table 3 identifies the operating system status for all 46 AM computers by site. Of the 35 AM computers that were not updated, [redacted] Although the Deputy Secretary of Defense memorandum allows DoD Components to use other Windows versions with an authorized waiver, none of the DoD Component officials had requested or obtained a waiver.

[17] The operating system upgrades are applicable to the AM computers, the printers do not use commercial operating systems.

[18] Deputy Secretary Of Defense Memorandum, "Implementation of Microsoft Windows 10 Secure Host Baseline," February 26, 2016.

Table 3. DoD Components Operating System Status During Audit

~~(CUI)~~ Sites	Total AM Computers	Operating Systems Not Updated
1st MEF	[redacted]	[redacted]
Navy FRC-SW	[redacted]	[redacted]
NIWC-P	[redacted]	[redacted]
60th MXG	[redacted]	[redacted]
WRNMMC	[redacted]	[redacted]
Total	**46**	**35** **~~(CUI)~~**

Source: The DoD OIG.

~~(CUI)~~ 1st MEF and [redacted] officials took action after our site visit to correct some of the operating system deficiencies.[19] For example, in October 2020, 1st MEF officials provided documentation indicating that they disposed of one AM computer that was using Microsoft Windows 7. In February 2021, a 1st MEF official provided confirmation that five of their AM computers were updated to the current version of Microsoft Windows 10. [redacted]

~~(CUI)~~ The need to update operating systems is critical to protecting the AM computers and the printers connected to them. For example, in 2019, Microsoft issued over 197 operating system updates to fix security vulnerabilities, one of which fixed a vulnerability that allowed attackers to gain unauthorized access to a single computer and then use that access to log into other computers. Therefore, we recommend that [redacted] update all AM computer operating systems to Windows 10, or obtain an approved waiver.

Vulnerability Scans Were Not Conducted

~~(FOUO)~~ DoD Component officials [redacted] did not identify network or system vulnerabilities on their AM systems. Specifically, 32 of the 46 AM computers were not periodically scanned for vulnerabilities. [redacted]

[19] The 1st MEF includes both the 1st MEF Additive Manufacturing and Training Center and the 1st Marine Logistics Group, 1st Maintenance Battalion.

~~(FOUO)~~ [redacted][20] In addition, Chairman of the Joint Chiefs of Staff Manual 6510.02 requires DoD Components to implement processes to proactively identify vulnerabilities that may impact their information systems and take corrective actions to mitigate detected vulnerabilities.[21] The NIST SP 800-53, Revision 4, requires agencies to define the frequency and process for conducting vulnerability scans on information systems and hosted applications. Finally, DoD Instruction 8531.01 requires DoD Components to manage and respond to vulnerabilities within DoD networks.[22]

To determine whether the DoD Component officials conducted vulnerability scans on the AM systems, we interviewed system administrators and users to identify the processes used to identify vulnerabilities. We also observed or obtained screen shots, as appropriate, showing the scan results for the AM systems that were scanned.

~~(FOUO)~~ Table 4 identifies the vulnerability scanning status for all 46 AM computers by site. [redacted]

Table 4. DoD Component Vulnerability Scanning Status During Audit

~~(CUI)~~ Site	Total AM Computers	AM Computers Not Scanned for Vulnerabilities
1st MEF	[redacted]	[redacted]
Navy FRC-SW	[redacted]	[redacted]
NIWC-P	[redacted]	[redacted]
60th MXG	[redacted]	[redacted]
WRNMMC	[redacted]	[redacted]
Total	**46**	**32** ~~(CUI)~~

[1] ~~(FOUO)~~ [redacted] As such, NIWC-P AM systems are not included.

[2] One computer used by the Navy Postgraduate Dental School belonged to the U.S. Navy Bureau of Medicine and Surgery and was not managed by the DHA. As of November 2020, the Navy Postgraduate Dental School located at WRNMMC no longer uses AM systems.

Source: The DoD OIG.

[20] ~~(FOUO)~~ [redacted] Joint Forces Headquarters-DODIN Task Order, "Assured Compliance Assessment Solution Operational Guidance," May 6, 2020. The Assured Compliance Assessment Solution is a software that allows for the scanning of information systems for vulnerabilities.

[21] Chairman of the Joint Chiefs of Staff Manual 6510.02, "Information Assurance Vulnerability Management Program," November 5, 2013.

[22] DoDI 8530.01, "DoD Vulnerability Management," September 15, 2020.

~~(CUI)~~ According to the Cybersecurity and Infrastructure Security Agency, with the increased use of complex, interconnected, and internet-accessible systems, it is important to rapidly remediate vulnerabilities, which could allow malicious actors access to networks. The Cybersecurity and Infrastructure Security Agency also states that according to government and industry partner reports that the average time between discovery and exploitation of a vulnerability is decreasing as malicious actors are more skilled, persistent, and able to use known vulnerabilities. Therefore, we recommend that [redacted] scan all AM systems for vulnerabilities in accordance with DoD guidance, or have exceptions documented in an approved authority to operate (ATO).[23]

Removable Media Was Not Properly Controlled

~~(CUI)~~ DoD Component officials [redacted] did not properly track or secure removable media used on their AM systems. Specifically, removable media used on 18 AM computers and 27 printers was not properly labeled, tracked, or secured. Chairman of the Joint Chiefs of Staff Manual 6510.01F requires DoD Components to implement a program to track, account for, and safeguard removable media.[24]

To determine whether DoD Component officials consistently protected removable media with design data, we interviewed system administrators and users to identify the processes and policies they followed for protecting and storing removable media used for AM systems. We also observed the process AM users followed for tracking and storing removable media.

~~(CUI)~~ Table 5 identifies the Components that did not label, secure, or scan removable media devices containing AM design data. Of the 18 AM computers and 27 AM printers that used removable media devices, [redacted]

[23] An authority to operate is the written authorization from a senior organizational official accepting risk to organizational operations, assets, individuals, other organizations, or the Nation and allowing operation of the information system.

[24] Chairman of the Joint Chiefs of Staff Instruction 6510.01F, "Information Assurance and Support to Computer Network Defense," February 9, 2011, Directive Current as of June 9, 2015.

Table 5. DoD Component AM Systems Using Noncompliant Removable Media

~~(CUI)~~ Site	Total AM Computers	AM Computers Using Noncompliant Removable Media Devices	AM Printers Using Noncompliant Removable Media Devices
1st MEF	[redacted]	[redacted]	[redacted]
Navy FRC-SW	[redacted]	[redacted]	[redacted]
NIWC-P	[redacted]	[redacted]	[redacted]
60th MXG	[redacted]	[redacted]	[redacted]
WRNMMC	[redacted]	[redacted]	[redacted]
Total	**46**	**18**	**27** ~~(CUI)~~

Note: One 60th MXG AM system had not been set up during the site visit and is not included in the totals.
Source: The DoD OIG.

~~(CUI)~~ According to the Cybersecurity and Infrastructure Security Agency, removable media is appealing to malicious actors because it can be small, readily available, inexpensive, and portable. Malicious actors can use removable media to infect computers so that when other removable media is used, the malware is automatically downloaded to the new removable media and then unknowingly spreads to other computers. Therefore, we recommend that [redacted] label, secure, and scan, as applicable, all removable media devices connected to additive manufacturing systems in accordance with DoD guidance.

Users Did Not Consider AM Systems as Information Technology Systems Needing Cybersecurity Controls

The AM system users did not consider the AM systems as information technology systems needing cybersecurity protection and instead considered the AM systems as "tools" used to generate supply parts. For example, Navy FRC-SW engineers stated that they treated the AM systems as other manufacturing machines, such as milling and welding machines that did not require consideration of cybersecurity. AM systems meet the definition of information technology as stated in the Committee on National Security Systems Instruction 4009, "Glossary." The glossary states that information technology includes:

> Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange,

> transmission, or reception of data or information by the executive agency. The term information technwology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

AM computers and printers store, manipulate, display, transmit, and receive AM design data. Therefore, AM computers and printers are information technology systems and subject to Federal and DoD cybersecurity guidance in accordance with DoD Instruction 8500.01. The Instruction requires that all DoD information technology be assigned to, and governed by, a DoD cybersecurity program that manages risk commensurate with the importance of the supported missions. Specifically, the Instruction states that cybersecurity requirements for DoD information technology will be managed through the Risk Management Framework (RMF) as directed by DoD Instruction 8510.01.

The RMF is a structured process used to secure DoD information technology systems by identifying the threats and risks to a system, defining and implementing security controls for eliminating or minimizing the impact of those threats and risks, and monitoring and evaluating the security controls for effectiveness. DoD information technology systems must go through the RMF process to be granted the authority to operate (ATO) which indicates the authorizing official has determined that the risk of operating the system is acceptable.[25]

None of the AM systems had an ATO at the time of our site visit, although officials had initiated the RMF process for 6 computers and 11 AM printers. DoDI 8510.01 requires the Component Heads to ensure that the information technology systems under their purview comply with DoD cybersecurity guidance, and Commanders and information technology system owners implement the guidance. Therefore, we recommend that the DoD Chief Information Officer, in coordination with the Under Secretary of Defense for Research and Engineering, and the Under Secretary of Defense for Acquisition and Sustainment, include additive manufacturing systems to the information technology systems portfolio and establish and maintain cybersecurity controls in accordance with Federal and DoD guidance.

[25] Committee on National Security Systems 4009-2015 defines an Authorizing Official as “a senior (federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.” DoDI 8510.01 distinguishes between information technology that requires full assessment resulting in an ATO and information technology that only requires an assessment, referred to as “Assess Only.” The distinction is determined during the RMF process by the type of products, services, data flows, and the interaction with other information technology systems.

DoD Component Officials Miscategorized AM Systems and Did Not Obtain an ATO

DoD Component officials, including ISSMs, information system security officers, and AM system users, incorrectly categorized the AM systems as stand-alone systems and erroneously concluded that the systems did not require an ATO. DoD Instruction 8510.01 defines a stand-alone system as a system that is not connected to another network and does not transmit, receive, route, or exchange information outside of the system's authorization boundary. For the AM systems, the authorization boundary includes all networks and systems that are included in or connected to the system.

DoD Component officials stated that their AM systems were stand-alone, but none of the five sites had established an authorization boundary to support that statement. In addition, DoD Component AM officials were not aware that connecting the AM systems to local networks, the Internet, or using removable media disqualified the AM systems as stand-alone systems. Further, compliance with the RMF process and the requirement to obtain an ATO apply to all systems, stand-alone or not. Had the cybersecurity officials completed the RMF process and obtained an ATO to use the AM systems, they would have identified the cybersecurity controls needed to mitigate the identified risks.

During the site visits, we notified officials that AM users were operating the AM systems without an ATO. We confirmed that in April, 2019 1st MEF officials started the RMF process for seven AM systems. As of March 31, 2021, 1st MEF officials were still in the early stages of the process. We also confirmed that in October 2019, Navy FRC-SW officials started the RMF process to obtain ATOs for their AM systems. As of January 2021, Navy FRC-SW officials have completed about half of the RMF process. In addition, in May 2020, the NIWC-P Command-ISSM authorized the AM systems to operate through a limited integration test environment approval process. The limited integration test environment process helps Research, Development, Test, and Evaluation programs obtain an ATO while addressing associated cybersecurity risks. To ensure that DoD Component officials obtain ATOs for all AM systems, we recommend that the DoD Chief Information Officer (CIO), the Department of Navy CIO, the USMC Deputy Commandant for Information, the U.S. Air Force CIO, and the DHA CIO, in coordination with designated AM Leads, require all AM systems to obtain an ATO in accordance with DoD policy before their use. We also recommend that the DoD CIO require AM system owners to immediately identify and implement security controls to minimize risk until obtaining an ATO.

Securing Additive Manufacturing Systems and Data Prevent Unauthorized Access and Ensure Integrity of the Design Data

DoD Component officials did not take required actions to identify AM system vulnerabilities that exposed the DODIN to unnecessary internal or external cybersecurity risks. Protecting and securing AM systems and data against cybersecurity risks consists of implementing DoD cyber hygiene practices such as enabling authentication factors, regularly updating operating systems, and conducting periodic system vulnerabilities scans. Unless the DoD properly protects the confidentiality and integrity of its AM systems and design data, there is an increased risk that internal or external malicious actors could compromise AM systems to steal the design data or gain access to the DoD networks. The compromise of AM design data could allow an adversary to re-create and use DoD's technology to the adversary's advantage on the battlefield. In addition, if malicious actors change the AM design data, that action could affect the end strength and utility of the AM printed products.

For example, hackers may be able to introduce internal defects in the manufacturing process to cause products to be made to handle less strain, leading them to break apart over time. In 2016, a team of university researchers demonstrated the ease in which hackers could turn malicious code into real world damage with an AM system. The team hacked an AM system and altered a few lines of code (instructions) in the design files, causing a created drone propeller to fail and the drone to crash. In 2019, a DoD Component team hacked an AM system, tricking it into using its own fan controls to manipulate the ratio of materials being printed and also designed a custom auger and print head using the AM system to create those parts. The hack allowed the DoD Component to devise a method to create ceramic body armor, even though it was not in the AM system manufacturer's manual.

In the January 2021 DoD AM strategy, USD(R&E) stated that as the AM manufacturing base expands the cybersecurity risks increase, including potential for data theft, alteration of data, and machine tampering which could result in low quality parts.[26] DoD cybersecurity official lack of awareness of how the AM systems operated contributed to the improper application of the RMF and improper categorization of AM systems, which allowed the AM users to operate information systems with critical known vulnerabilities.

[26] Joint Defense Manufacturing Council, "DoD Additive Manufacturing Strategy," January 2021.

Recommendations, Management Comments, and Our Response

Recommendation 1

We recommend that the DoD Chief Information Officer, in coordination with the Under Secretary of Defense for Research and Engineering and the Under Secretary of Defense for Acquisition and Sustainment, include additive manufacturing systems to the information technology systems portfolio and establish and maintain cybersecurity controls in accordance with Federal and DoD guidance.

DoD Chief Information Officer Comments

The DoD CIO disagreed, stating that DoD Instructions 8500.01 and 8510.01 require all systems, including AM systems, to apply cybersecurity controls. The DoD CIO suggested restating the recommendation to clarify that system owners were not following policy.

Under Secretary of Defense for Research and Engineering Comments

The Acting Director of Defense Research and Engineering for Research and Technology, responding for the USD(R&E), agreed, stating that the USD(R&E) supported including AM systems in the information technology systems portfolio, recognizing that AM systems contain operational technology. The Acting Director also stated that current DoD policy allows for a waiver to some RMF requirements that could adversely impact AM operations; therefore, she suggested revising the recommendation to acknowledge that the AM systems contain operational technology, which should be considered when implementing guidance and policies. The Acting Director stated that the USD(R&E) has taken several steps to prioritize cybersecurity for AM systems including:

- establishing the Cyber-physical Working Group to facilitate AM cybersecurity efforts across the DoD in FY 2019;
- supporting the creation of the National Center for Cybersecurity in Manufacturing that conducts research and development to identify gaps in cybersecurity guidance for manufacturing and provides best practices for implementing cybersecurity controls in FY 2020; and
- publishing the DoD AM Strategy that specifically addresses securing the AM workflow as a cited goal in FY 2021.

The Acting Director stated that the USD(R&E) would issue DoD Instruction 5000.UK, “Use of Additive Manufacturing in the DoD,” by the third quarter of 2021 to establish policy, assign responsibilities, and detail procedures when using AM in the DoD. The procedures will include the cybersecurity processes and physical infrastructure required to secure and support the use of AM in the DoD. The Acting Director also stated that she would invite a DoD CIO representative to join the Joint Defense Manufacturing Council by fourth quarter of FY 2021.

Under Secretary of Defense for Acquisition and Sustainment Comments

The Deputy Assistant Secretary of Defense for Materiel Readiness, responding for the USD(A&S), agreed, stating that the USD(A&S) fully supported including AM systems in the information technology portfolio and establishing and maintaining cybersecurity controls for AM systems. The Deputy Assistant Secretary stated that the USD(A&S) has taken several steps to prioritize cybersecurity for AM systems including publishing a memorandum to ensure that appropriate policy and guidance include the digital and cyber infrastructure to support AM for sustainment operations; partnering with the USD(R&E) to organize AM cybersecurity workshops with DoD, industry, and academia subject matter experts; and, publishing the DoD Additive Manufacturing Strategy with USD(R&E).

The Deputy Assistant Secretary also stated that the USD(A&S) would work closely with the DoD CIO on implementation guidance for the acquisition and sustainment communities on including AM systems in the information technology portfolio and establishing and maintaining cybersecurity controls for AM systems. Furthermore, the Deputy Assistant Secretary stated that the USD(A&S) would continue to work collaboratively with the Joint Defense Manufacturing Council, the DoD senior leadership body responsible for manufacturing.

Our Response

Although the DoD CIO disagreed with the recommendation, actions taken and planned by the USD(R&E) and USD(A&S) to include AM systems in the information technology portfolio and establish cybersecurity control requirements for AM systems meet the intent of the recommendation. We agree with the DoD CIO that DoD Instructions 8500.01 and 8510.01 are applicable to all information systems; however, the AM system owners did not consider the AM systems as information systems and to reduce the risk of continued noncompliance, specific guidance is needed. We did not make the Acting Director of Defense Research and Engineering for Research and Technology’s suggested revision to the recommendation because including AM systems in the information technology portfolio achieves that result. Because the actions taken and planned by the USD(R&E) and USD(A&S) address the specifics of the recommendation, the recommendation is resolved but will remain open. We will close the recommendation once the USD(R&E) and USD(A&S) provide copies of guidance requiring AM systems to be included in the information technology portfolio and in compliance with Federal and DoD cybersecurity controls.

Recommendation 2

We recommend that the DoD Chief Information Officer require additive manufacturing system owners to immediately identify and implement security controls to minimize risk until obtaining an authority to operate.

DoD Chief Information Officer Comments

The DoD CIO disagreed, stating that all systems containing DoD information were already required to implement cybersecurity controls and subject to DoD Cybersecurity Program requirements in DoD Instruction 8510.01 for managing cybersecurity risk. The DoD CIO suggested revising the recommendation to direct system owners to implement existing policy and security controls.

Our Response

Although the DoD CIO disagreed, actions taken and planned by the Department of the Navy CIO, U.S. Marine Corps Deputy Commandant for Information, Department of the Air Force CIO; and Defense Health Agency CIO (the DoD Component CIOs) in response to Recommendation 3 meet the intent of the recommendation. Specifically, the DoD Component CIOs agreed to require all AM systems to obtain an authority to operate, which will require the AM system owners to identify and implement security controls. We agree with the DoD CIO that DoD Instruction 8510.01 is applicable to all information systems; however, the AM system owners did not consider the AM systems as information systems and to reduce the risk of continued noncompliance, specific guidance is needed. We did not make the DoD CIO’s suggested revision to the recommendation because the resulting recommendation would be duplicative to recommendations already made to system owners to obtain an authority to operate; conduct vulnerability scans; label, scan, and secure removable media; and, update operating systems in accordance with DoD policies. We consider the recommendation closed because no further action is needed from the DoD CIO.

Recommendation 3

We recommend that the DoD Chief Information Officer, the Department of the Navy Chief Information Officer, U.S. Marine Corps Deputy Commandant for Information, U.S. Air Force Chief Information Officer, and Defense Health Agency Chief Information Officer, in coordination with designated Additive Manufacturing Leads, require all additive manufacturing systems to obtain an authority to operate in accordance with DoD policy before their use.

DoD Chief Information Officer Comments

The DoD CIO disagreed, stating that DoD Instruction 8510.01 already requires all systems containing DoD technology to undergo a final risk determination and authorization decision. The DoD CIO also stated that system owners of all systems, including AM systems, are subject to DoD Cybersecurity program requirements.

Our Response

Although the DoD CIO disagreed, actions taken and planned by the DoD Component CIOs meet the intent of the recommendation. Specifically, the DoD Component CIOs agreed to require all AM systems to obtain an authority to operate, which will require the AM system owners to identify and implement security controls. We agree with the DoD CIO that DoD Instruction 8510.01 already requires all systems containing DoD technology to undergo a final risk determination and authorization decision. We also agree that AM systems are subject to all DoD Cybersecurity program requirements; however, the AM system owners did not consider the AM systems as information systems and to reduce the risk of continued noncompliance, specific guidance is needed. Because the actions taken and planned by the DoD Component CIOs address the specifics of the recommendation, the recommendation is resolved but will remain open. We will close the recommendation once the DoD Component CIOs provide guidance stating that all AM systems are required to obtain an authority to operate.

Department of the Navy Chief Information Officer Comments

The Department of the Navy Senior Information Security Officer, responding for the Department of the Navy CIO, agreed, stating that DoD Instruction 8500.01 and Secretary of the Navy Instruction 5239.3C, “Department of the Navy Cybersecurity Policy” require that Department of the Navy organizations obtain and maintain authorization for all information technology in accordance with DoD Instruction 8510.01. The Senior Information Security Officer stated that he would task the Deputy Senior Information Security Officer to work with the responsible Command Information Officers and Authorizing Officials to ensure all additive manufacturing systems comply with DoD Instructions 8500.01, 8510.01, and Secretary of the Navy Instruction 5239.3C by June 1, 2022.

Our Response

Comments from the Department of the Navy Senior Information Security Officer addressed the specifics of the recommendation; therefore, the recommendation is resolved but will remain open. We will close the recommendation once the Department of the Navy CIO provides implementation procedures for AM systems authorizations and documentation, such as screenshots of RMF packages, showing that AM systems have initiated the RMF process.

U.S. Marine Corps Deputy Commandant for Information Comments

The Headquarters Marine Corps Director for Information Command, Control, Communications, and Computers responding for the Deputy Commandant for Information agreed, stating that the Marine Corps has directed all AM system owners and ISSMs to update and complete their current RMF authorization packages in the Marine Corps Compliance and Authorization Support Tool. In addition, the Director stated that failure to complete and upload annual security review assessments into the Marine Corps Compliance and Authorization Support Tool would result in automated reminders to the system owners and ISSMs; reports to the appropriate chain-of-command for action; and status reports to the Deputy Commandant for Information leadership.

Our Response

Comments from the Director addressed the specifics of the recommendation; therefore, the recommendation is resolved but will remain open. We will close the recommendation once the U.S. Marine Corps Deputy Commandant for Information provides approved guidance requiring all AM systems to obtain an authority to operate.

Department of the Air Force Chief Information Officer Comments

The Department of the Air Force Deputy CIO, responding for the Department of the Air Force CIO, agreed, stating that the Department will correct the issues identified in the report. The Deputy CIO stated that the Department of the Air Force Chief Information Security Officer would issue a guidance memorandum by May 30, 2021, directing Authorizing Officials to issue an authority to operate for all AM systems within their boundaries. The Authorizing Officials must comply with the guidance memorandum by April 30, 2022.

Our Response

Comments from the Deputy CIO addressed the specifics of the recommendation; therefore, the recommendation is resolved but will remain open. We will close the recommendation once the Department of the Air Force CIO provides a copy of the associated memorandum directing authorizing officials to issue an authority to operate for all AM systems within their respective boundaries.

Defense Health Agency Chief Information Officer Comments

The DHA Director, responding for the DHA CIO, agreed, stating that the DHA Interim RMF policy requires all information systems to obtain an authority to operate; therefore, no new policy is required. The Director stated that, based on findings in this report, some sites may not be fully aware that AM systems are considered information systems and are subject to the Interim RMF policy. The Director also stated that to reduce the risk of future noncompliance, DHA would present a DHA CIO Working Group information briefing on the subject to the DHA site CIOs.

Our Response

Comments from the Director addressed the specifics of the recommendation; therefore, the recommendation is resolved but will remain open. We will close the recommendation once the DHA Chief Information Officer provides a copy of the associated briefing to include the date the briefing was conducted and a list of the attendees.

Naval Facilities Engineering Systems Commander Comments

Although not required to respond, the Naval Facilities Engineering Systems Command (NAVFAC) Commander stated that NAVFAC Headquarters Command Information Officer agreed and will require all AM systems to obtain an authority to operate in accordance with DoD Policy before their use. The Commander also stated that the Command Information Officer would ensure that all AM systems currently in use are immediately registered to satisfy the first step of the RMF within 90 days and will obtain an authority to operate by December 31, 2022.

Recommendation 4

We recommend that the 1st Marine Expeditionary Force Commander, in coordination with designated Additive Manufacturing Leads:

a. **~~(CUI)~~** [redacted]

1st Marine Expeditionary Force Commander Comments

~~(CUI)~~ The Deputy Assistant Chief of Staff, Information Environment Division, Marine Forces Pacific, responding for the 1st MEF Commander, agreed, stating that the 1st MEF [redacted]

Our Response

~~(CUI)~~ Comments from the Deputy Assistant Chief of Staff addressed the specifics of the recommendation; therefore, the recommendation is resolved but will remain open. We will close the recommendation once the 1st MEF Commander provides documentation, [redacted]

b. **~~(CUI)~~** [redacted]

1st Marine Expeditionary Force Commander Comments

~~(CUI)~~ The Deputy Assistant Chief of Staff, Information Environment Division, Marine Forces Pacific, responding for the 1st MEF Commander, agreed, stating that the 1st MEF [redacted]

Our Response

~~(CUI)~~ Comments from the Deputy Assistant Chief of Staff addressed the specifics of the recommendation; therefore, the recommendation is resolved but will remain open. We will close the recommendation once the 1st MEF Commander provides documentation, [redacted]

Recommendation 5

We recommend that the Navy Fleet Readiness Center Southwest Commander, in coordination with designated Additive Manufacturing Leads:

a. **~~(CUI)~~** [redacted]

Navy Fleet Readiness Center Southwest Commander Comments

~~(CUI)~~ The Navy FRC-SW Commanding Officer agreed, stating that the FRC-SW would complete a detailed inventory of all AM systems [redacted]

The Commanding Officer also stated that the FRC-SW would [redacted] and incorporate RMF requirements as part of the process for obtaining an authority to operate. In addition, the Commander stated that FRC-SW [redacted]

Our Response

~~(CUI)~~ Comments from the Commanding Officer addressed the specifics of the recommendation; therefore, the recommendation is resolved but will remain open. We will close the recommendation once the Commanding Officer provides the inventory results and documentation, such as work orders or screenshots, [redacted]

b. **~~(CUI)~~** [redacted]

Navy Fleet Readiness Center Southwest Commander Comments

~~(CUI)~~ The Navy FRC-SW Commanding Officer agreed, stating that [redacted]

Our Response

~~(CUI)~~ Comments from the Commanding Officer addressed the specifics of the recommendation; therefore, the recommendation is resolved but will remain open. We will close the recommendation once the Commanding Officer provides documentation, [redacted]

c. ~~(CUI)~~ [redacted]

Navy Fleet Readiness Center Southwest Commander Comments

~~(CUI)~~ The Navy FRC-SW Commanding Officer agreed, stating that the FRC-SW would publish an instruction or guidance requiring the FRC-SW [redacted] In addition, the Commanding Officer stated that the FRC-SW [redacted]

Our Response

~~(CUI)~~ Comments from the Commanding Officer addressed the specifics of the recommendation; therefore, the recommendation is resolved but will remain open. We will close the recommendation once the Commanding Officer provides [redacted]

Deputy Chief of Naval Operations for Fleet Readiness and Logistics Comments

Although not required to respond, the Deputy Chief of Naval Operations for Fleet Readiness and Logistics, agreed, stating that the Naval Air Systems Command would ensure that the FRC-SW completed all recommended actions.

Recommendation 6

~~(CUI)~~ We recommend that the Naval Information Warfare Center Pacific Commander, in coordination with designated Additive Manufacturing Leads [redacted]

Naval Information Warfare Center Pacific Commander Comments

~~(CUI)~~ The Commanding Officer, NIWC-P, agreed, stating that he would remind the NIWC-P Information System Security Officers/Tech Codes of command policy [redacted] The Commanding Officer also stated that NIWC-P would conduct followup testing to validate compliance with policy.

Our Response

~~(CUI)~~ Comments from the Commanding Officer addressed the specifics of the recommendation; therefore, the recommendation is resolved but will remain open. We will close the recommendation once the Commanding Officer provides documentation [redacted]

Recommendation 7

We recommend that the Air Force 60th Maintenance Group Commander, in coordination with designated Additive Manufacturing Leads:

a. **~~(CUI)~~** [redacted]

Air Force 60th Maintenance Group Commander Comments

~~(CUI)~~ The Deputy Director of Communications, Headquarters Air Mobility Command, responding for the 60th MXG Commander, agreed, stating that [redacted]

Our Response

~~(CUI)~~ Comments from the Deputy Director addressed the specifics of the recommendation; therefore, the recommendation is resolved but will remain open. We will close the recommendation once the 60th MXG Commander provides documentation, [redacted]

b. **~~(CUI)~~** [redacted]

Air Force 60th Maintenance Group Commander Comments

~~(CUI)~~ The Deputy Director of Communications, Headquarters Air Mobility Command, responding for the 60th MXG Commander, agreed, stating that the 60th Air Mobility Wing Cybersecurity office [redacted]

Our Response

~~(CUI)~~ Comments from the Deputy Director addressed the specifics of the recommendation; therefore, the recommendation is resolved, but will remain open. We will close the recommendation once the 60th MXG Commander provides documentation, [redacted]

c. **~~(CUI)~~** [redacted]

Air Force 60th Maintenance Group Commander Comments

~~(CUI)~~ The Deputy Director of Communications, Headquarters Air Mobility Command, responding for the 60th MXG Commander, agreed, stating that [redacted] In addition, the Deputy Director stated that the 60th MXS would [redacted]

[27] Reimaging is the process of restoring a computer hard disk drive from a disk image, a virtual copy of the entire hard disk drive including the file structure and all files and folders.

~~(CUI)~~ [redacted]

Our Response

~~(CUI)~~ Comments from the Deputy Director addressed the specifics of the recommendation; therefore, the recommendation is resolved but will remain open. We will close the recommendation once the 60th MXG Commander provides documentation, [redacted]

Recommendation 8

We recommend that the Walter Reed National Military Medical Center Director, in coordination with designated Additive Manufacturing Leads:

a. ~~(CUI)~~ [redacted]

Walter Reed National Military Medical Center Director Comments

~~(CUI)~~ The DHA Director, responding for the WRNMMC Director, agreed, stating that [redacted]

Our Response

~~(CUI)~~ Comments from the DHA Director addressed the specifics of the recommendation; therefore, the recommendation is resolved but will remain open. We will close the recommendation once the DHA Director provides documentation, [redacted]

b. ~~**(CUI)**~~ [redacted]

Walter Reed National Military Medical Center Director Comments

~~(CUI)~~ The DHA Director, responding for the WRNMMC Director, agreed, stating that the WRNMMC CIO started the process to obtain an authority to operate the restricted WRNMMC network on which the AM systems operate. The DHA Director also stated [redacted]

Our Response

~~(CUI)~~ Comments from the DHA Director addressed the specifics of the recommendation; therefore, the recommendation is resolved but will remain open. We will close the recommendation once the WRNMMC Director provides documentation, [redacted]

Appendix A

Scope and Methodology

We conducted this performance audit from April 2019 through March 2021 in accordance with generally accepted government auditing standards.[28] The generally accepted government auditing 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.

We interviewed officials from the Army, Marine Corps, Navy, Air Force, Marine Corps and Navy Special Operations Commands, Defense Logistics Agency, and DHA to determine their AM processes and identify information systems and physical security controls and procedures implemented at each site. We reviewed applicable Federal, DoD, and Component-level policies and guidance for using and protecting AM systems, storing data, and maintaining asset accountability records. In addition, we reviewed strategic documents related to the implementation of AM across the DoD, including Military Services roadmaps and the DoD roadmap.

We obtained the universe of AM systems from the Army, Marine Corps, Navy, Air Force, and DHA. We nonstatistically selected and planned to visit the following sites based on our review of the AM printers' usage and functionality.

- Army – Joint Manufacturing and Technology Center, Rock Island, Illinois
- Marine Corps – 1st MEF, Camp Pendleton, California
    - 1st Marine Logistics Group, 1st Maintenance Battalion
    - 1st MEF Additive Manufacturing and Training Center
- Navy – NIWC-P, San Diego, California
- Navy – FRC-SW, Coronado, California
- Air Force – 60th MXG, Travis Air Force Base, San Diego, California
- Air Force – Air Force Life Cycle Management Center, Dayton, Ohio
- DHA – WRNMMC, Bethesda, Maryland
- Special Operations Command – Naval Special Warfare Command, San Diego, California
- Special Operations Command – Marine Corps Forces Special Operations Command, San Diego, California

[28] Due to the COVID-19 pandemic and other DoD OIG priorities, the audit was suspended at different times for a total of eight months.

On March 13, 2020, the Deputy Secretary of Defense issued a stop movement order for domestic travel. The stop movement order affected the execution phase of the audit and we were not able to conduct all planned initial and follow-up site visits. As a result, we reduced the sample size to five DoD Component sites: one Marine Corps, two Navy, one Air Force, and one DHA. We reviewed the cybersecurity and physical security controls for AM systems operated at those five sites. Table 6 shows the Component sites included in the audit and the number of AM printers and computers associated with them.

Table 6. Sites Visited and Number of AM Systems Reviewed at Each Site

Sites		Number of AM Printers	Number of AM Computers
Marine Corps	1st MEF	21	15
U.S. Navy	Navy FRC-SW	5	4
	NIWC-P	28	14
U.S. Air Force	60th MXG	2	2
DHA	WRNMMC	17	11
Total		**73**	**46**

Note: We also identified three inoperable AM printers at NIWC-P and one at Navy FRC-SW that the Navy accounted for that were not included in our review.

Source: The DoD OIG.

To determine whether DoD Components were securing AM data and systems to prevent unauthorized changes and ensure integrity of the design data, we reviewed NIST guidance for Federal information systems to determine the baseline cybersecurity and physical controls included in our review. We selected controls that would increase security of the AM systems and reduce the risk that systems or data could be compromised, altered, or stolen. We reviewed and tested whether the following cybersecurity and physical security controls were implemented and operating in accordance with Federal and DoD guidance.

- Updating Operating Systems (Configuration Management)
- Using Authentication Factors (Logical Access)
- Removing User Access (Unauthorized System Access)
- Identifying Vulnerabilities (Vulnerability Management)
- Protecting Removal Media (Media Protection)
- Maintaining Accountability of AM Assets (Information Technology Asset Management)
- Implementing Security Controls (Physical Security)

We also reviewed information system maintenance logs, vulnerability scan reports, and physical security logs. We conducted walk-throughs at each site and observed AM and physical security processes and controls in place.

Internal Control Assessment and Compliance

We assessed internal controls and compliance with laws and regulations necessary to satisfy the audit objective. In particular, we assessed seven cybersecurity controls related to operating system updates, authentication factors, vulnerability identification, removable media, property accountability, and physical security. 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.

Use of Computer-Processed Data

We used computer-processed data that we received from the DoD Components' property management systems and manually compiled lists provided by property managers to develop a master list of all AM printers currently in use and tracked by the DoD Components. We used the master list to select a nonstatistical sample for possible site visits and as a baseline to identify the total number of printers by DoD Component. Once we selected the sites, we compared the master list data to the data provided by the site points of contact. We determined that the data were reliable enough to select site visits but did not rely on the data to form findings, recommendations, or conclusions.

Use of Technical Assistance

We received assistance from the DoD OIG Quantitative Methods Division to select a nonstatistical sample of AM systems from the Military Services and Defense agencies for review. We requested the OUSD(R&E) and OUSD(A&S) to provide an inventory of AM systems throughout the DoD enterprise; however, they did not have this information. Between July and September 2019, we requested the AM system's inventories directly from the Military Services and Defense agencies. Based on the information received, we identified 188 Army, 172 Marine Corps, 553 Navy, 99 Air Force, 18 Special Operations Command, and 17 DHA AM systems. We selected a nonstatistical sample of 151 of the 1,047 AM systems for review. Due to the COVID-19 pandemic, we reduced the scope of the audit from the 151 AM systems originally selected to the 73 AM systems that we had already visited at the time of the stop movement order. The 73 AM systems include 33 Navy, 2 Air Force, 21 Marine Corps, and 17 DHA.

Prior Coverage

During the last 5 years, the Government Accountability Office (GAO) and the DoD Office of Inspector General (DoD OIG) have issued three reports discussing AM systems. Unrestricted GAO reports can be accessed at http://www.gao.gov and unrestricted OIG reports can be accessed at http://www.dodig.mil/reports.html/.

GAO

Report No. GAO-16-56, "DoD Needs to Systematically Track Department-wide 3D Printing Efforts," October 14, 2015

> The GAO determined that the DoD had taken steps to implement AM to improve performance and combat capability, and to achieve cost saving. The DoD also used various mechanisms to coordinate AM efforts. However, the DoD did not systematically track Organizations' efforts to include all activities performed and resources expanded by the DoD and the results of these activities, including actual and potential performance and combat capability improvements, cost savings, and lesson learned.

Report No. GAO-15-505SP, "Highlights of a Forum presented to the Chairman, Committee on Science, Space, and Technology, House of Representatives, "3D Printing: Opportunities, Challenges, and Policy Implications of AM," June 24, 2015

> The GAO determined that the DoD was looking at ways to use AM in supply chain management, including repairing equipment and producing parts in the field, to reduce the need to store parts, to produce discontinued parts or temporary parts to use until a permanent part can be obtained, and to quickly build parts to meet mission requirements.

DoD OIG

Report No. DODIG-2020-003, "Audit of the DoD's Use of Additive Manufacturing for Sustainment Parts," October 17, 2019

> The DoD OIG determined that the DoD had not identified data to be reported for AM equipment purchased, parts produced, and funds spent on AM. In addition, the DoD had not standardized the requirements for tracking AM equipment purchased by the Military Services.

Appendix B

Security Controls for Protecting Additive Manufacturing Systems and Data

The following Federal and DoD guidance establish security controls for protecting information systems and data, to include AM systems and data.

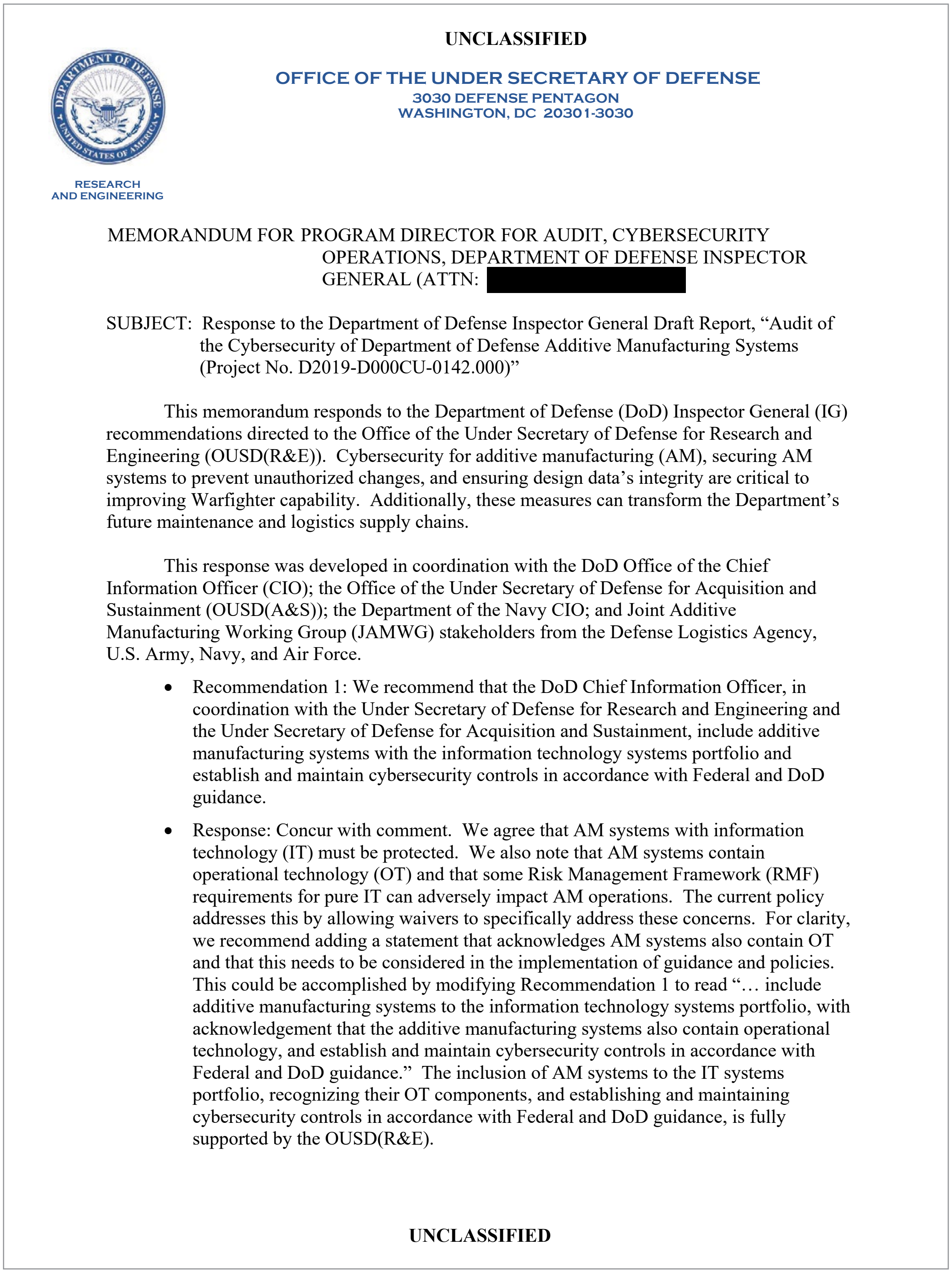
- **NIST SP 800-53 Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations," April 2013 (Including Updates as of January 1, 2015)**, provides a catalog of security and privacy controls for Federal information systems, and a glossary of terms applicable to security and privacy.
- **NIST Internal Report 8183, "Cybersecurity Framework Manufacturing Profile," September 2017 (Including Updates as of May 20, 2019)**, provides a roadmap using a risk-based approach for reducing cybersecurity risk for the manufacturing sector by enhancing current cybersecurity standards.
- **DoD Instruction 5200.08-R, "Physical Security Program," April 9, 2007 (Incorporating Change 1, May 27, 2009)**, requires DoD Components to implement physical security controls, such as physical barriers and access control devices, to safeguard DoD facilities.
- **DoD Instruction 8510.01, "Risk Management Framework for DoD Information Technology," March 12, 2014 (Incorporating Change 2, July 28, 2017)**, requires DoD Components to implement proper risk management procedures and perform regular risk assessments for DoD information systems. The Risk Management Framework establishes the process that risk management officials must follow to receive an authority to operate a system on the DoDIN or in a DoD environment.
- **DoD Instruction 8500.01 "Cybersecurity," March 14, 2014 (Incorporating Change 1, October 7, 2019)**, requires DoD Components to implement strong identification and authentication methods to secure access to DoD information systems.
- **DoD Instruction 8530.01, "Cybersecurity Activities Support to DODIN Operations," March 7, 2016**, requires DoD Components to perform vulnerability scans and mitigate known system vulnerabilities in order to safeguard secured data more effectively.[29]

[29] The DODIN is globally interconnected, set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, including computing systems and services, software, data, security services, other associated services, and national security systems.

- ~~(FOUO)~~ **Joint Force Headquarters-DODIN, "Task Order 20-0020 Assured Compliance Assessment Solution (ACAS) Operational Guidance," May 2020**, [redacted]
- **DoD CIO Memorandum, "Interim Digital Authentication Guidelines for Unclassified and Secret Classified DoD Networks and Information Systems," August 20, 2018**, explains the DoD approved identity authentication solutions and outlines when using a username and password is acceptable.

Management Comments

Office of the Under Secretary of Defense for Research and Engineering



UNCLASSIFIED

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

RESEARCH
AND ENGINEERING

MEMORANDUM FOR PROGRAM DIRECTOR FOR AUDIT, CYBERSECURITY OPERATIONS, DEPARTMENT OF DEFENSE INSPECTOR GENERAL (ATTN: [redacted]

SUBJECT: Response to the Department of Defense Inspector General Draft Report, "Audit of the Cybersecurity of Department of Defense Additive Manufacturing Systems (Project No. D2019-D000CU-0142.000)"

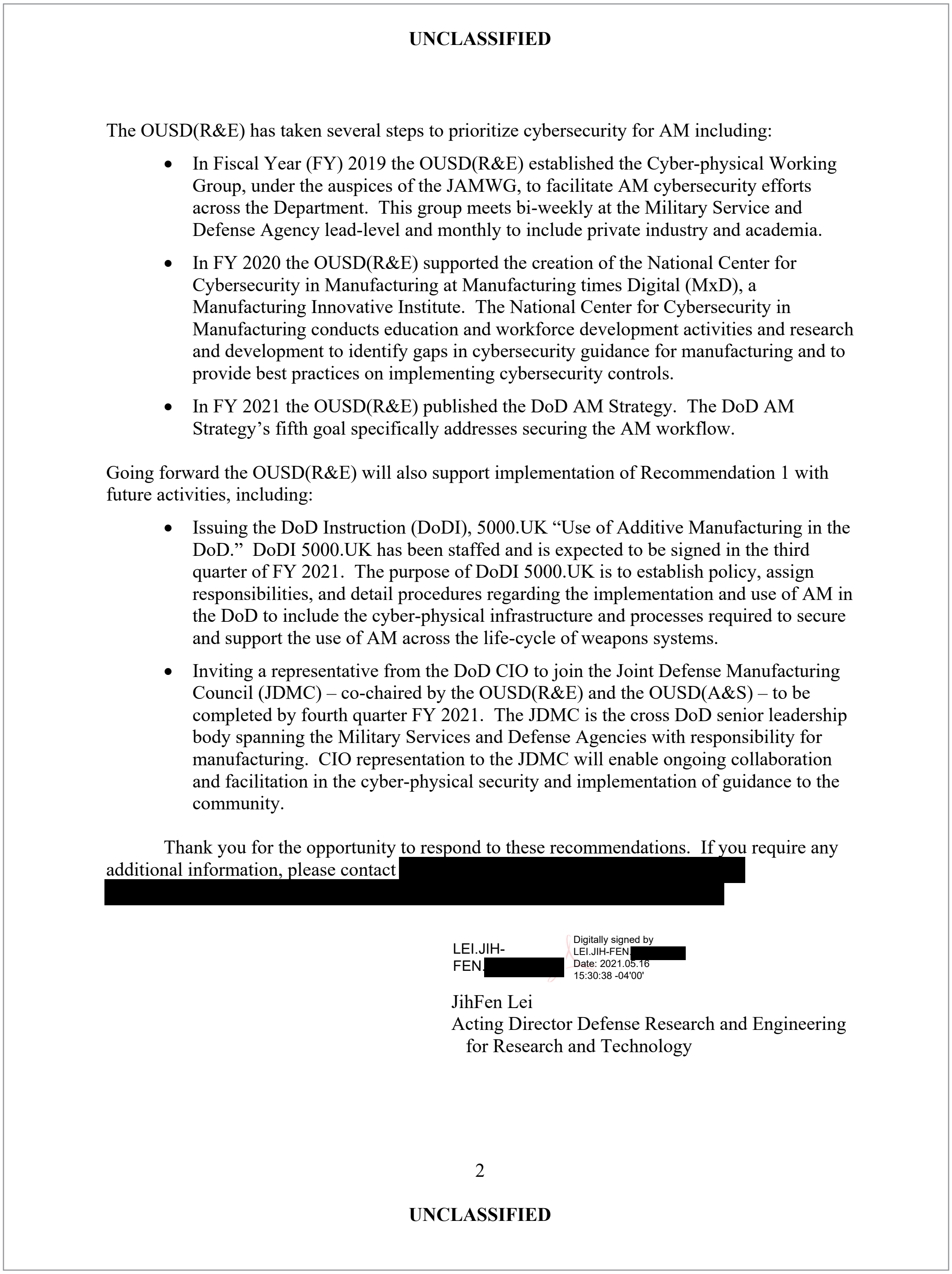
This memorandum responds to the Department of Defense (DoD) Inspector General (IG) recommendations directed to the Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&E)). Cybersecurity for additive manufacturing (AM), securing AM systems to prevent unauthorized changes, and ensuring design data's integrity are critical to improving Warfighter capability. Additionally, these measures can transform the Department's future maintenance and logistics supply chains.

This response was developed in coordination with the DoD Office of the Chief Information Officer (CIO); the Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)); the Department of the Navy CIO; and Joint Additive Manufacturing Working Group (JAMWG) stakeholders from the Defense Logistics Agency, U.S. Army, Navy, and Air Force.

- Recommendation 1: We recommend that the DoD Chief Information Officer, in coordination with the Under Secretary of Defense for Research and Engineering and the Under Secretary of Defense for Acquisition and Sustainment, include additive manufacturing systems with the information technology systems portfolio and establish and maintain cybersecurity controls in accordance with Federal and DoD guidance.
- Response: Concur with comment. We agree that AM systems with information technology (IT) must be protected. We also note that AM systems contain operational technology (OT) and that some Risk Management Framework (RMF) requirements for pure IT can adversely impact AM operations. The current policy addresses this by allowing waivers to specifically address these concerns. For clarity, we recommend adding a statement that acknowledges AM systems also contain OT and that this needs to be considered in the implementation of guidance and policies. This could be accomplished by modifying Recommendation 1 to read "… include additive manufacturing systems to the information technology systems portfolio, with acknowledgement that the additive manufacturing systems also contain operational technology, and establish and maintain cybersecurity controls in accordance with Federal and DoD guidance." The inclusion of AM systems to the IT systems portfolio, recognizing their OT components, and establishing and maintaining cybersecurity controls in accordance with Federal and DoD guidance, is fully supported by the OUSD(R&E).

UNCLASSIFIED

Office of the Under Secretary of Defense for Research and Engineering (cont'd)



UNCLASSIFIED

The OUSD(R&E) has taken several steps to prioritize cybersecurity for AM including:

- In Fiscal Year (FY) 2019 the OUSD(R&E) established the Cyber-physical Working Group, under the auspices of the JAMWG, to facilitate AM cybersecurity efforts across the Department. This group meets bi-weekly at the Military Service and Defense Agency lead-level and monthly to include private industry and academia.
- In FY 2020 the OUSD(R&E) supported the creation of the National Center for Cybersecurity in Manufacturing at Manufacturing times Digital (MxD), a Manufacturing Innovative Institute. The National Center for Cybersecurity in Manufacturing conducts education and workforce development activities and research and development to identify gaps in cybersecurity guidance for manufacturing and to provide best practices on implementing cybersecurity controls.
- In FY 2021 the OUSD(R&E) published the DoD AM Strategy. The DoD AM Strategy's fifth goal specifically addresses securing the AM workflow.

Going forward the OUSD(R&E) will also support implementation of Recommendation 1 with future activities, including:

- Issuing the DoD Instruction (DoDI), 5000.UK "Use of Additive Manufacturing in the DoD." DoDI 5000.UK has been staffed and is expected to be signed in the third quarter of FY 2021. The purpose of DoDI 5000.UK is to establish policy, assign responsibilities, and detail procedures regarding the implementation and use of AM in the DoD to include the cyber-physical infrastructure and processes required to secure and support the use of AM across the life-cycle of weapons systems.
- Inviting a representative from the DoD CIO to join the Joint Defense Manufacturing Council (JDMC) – co-chaired by the OUSD(R&E) and the OUSD(A&S) – to be completed by fourth quarter FY 2021. The JDMC is the cross DoD senior leadership body spanning the Military Services and Defense Agencies with responsibility for manufacturing. CIO representation to the JDMC will enable ongoing collaboration and facilitation in the cyber-physical security and implementation of guidance to the community.

Thank you for the opportunity to respond to these recommendations. If you require any additional information, please contact [redacted]

LEI.JIH-FEN.[redacted]

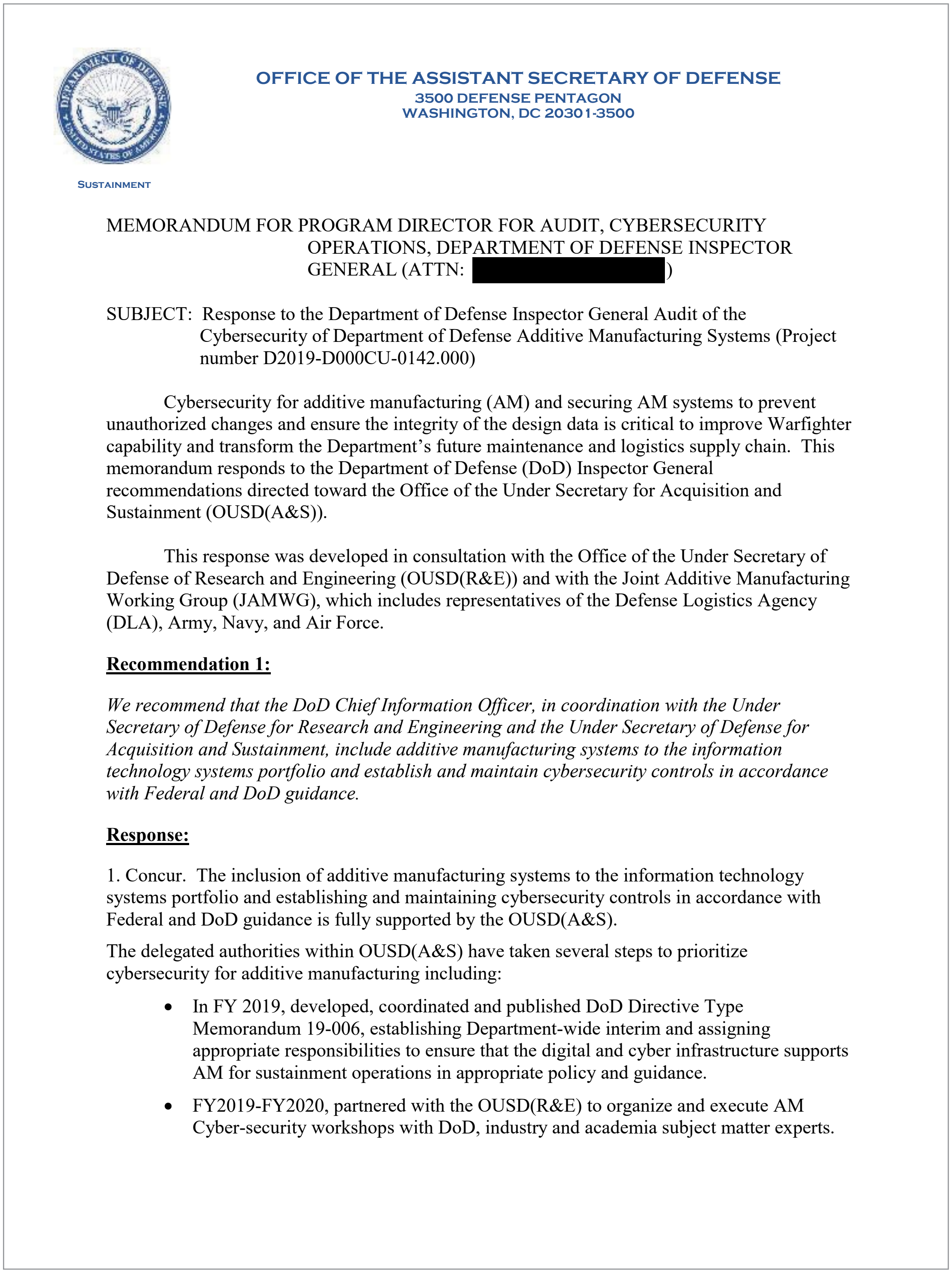
Digitally signed by LEI.JIH-FEN[redacted]
Date: 2021.05.16 15:30:38 -04'00'

JihFen Lei
Acting Director Defense Research and Engineering
for Research and Technology

2

UNCLASSIFIED

Office of the Under Secretary of Defense for Acquisition and Sustainment



OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
3500 DEFENSE PENTAGON
WASHINGTON, DC 20301-3500

SUSTAINMENT

MEMORANDUM FOR PROGRAM DIRECTOR FOR AUDIT, CYBERSECURITY OPERATIONS, DEPARTMENT OF DEFENSE INSPECTOR GENERAL (ATTN: [redacted])

SUBJECT: Response to the Department of Defense Inspector General Audit of the Cybersecurity of Department of Defense Additive Manufacturing Systems (Project number D2019-D000CU-0142.000)

Cybersecurity for additive manufacturing (AM) and securing AM systems to prevent unauthorized changes and ensure the integrity of the design data is critical to improve Warfighter capability and transform the Department's future maintenance and logistics supply chain. This memorandum responds to the Department of Defense (DoD) Inspector General recommendations directed toward the Office of the Under Secretary for Acquisition and Sustainment (OUSD(A&S)).

This response was developed in consultation with the Office of the Under Secretary of Defense of Research and Engineering (OUSD(R&E)) and with the Joint Additive Manufacturing Working Group (JAMWG), which includes representatives of the Defense Logistics Agency (DLA), Army, Navy, and Air Force.

Recommendation 1:

We recommend that the DoD Chief Information Officer, in coordination with the Under Secretary of Defense for Research and Engineering and the Under Secretary of Defense for Acquisition and Sustainment, include additive manufacturing systems to the information technology systems portfolio and establish and maintain cybersecurity controls in accordance with Federal and DoD guidance.

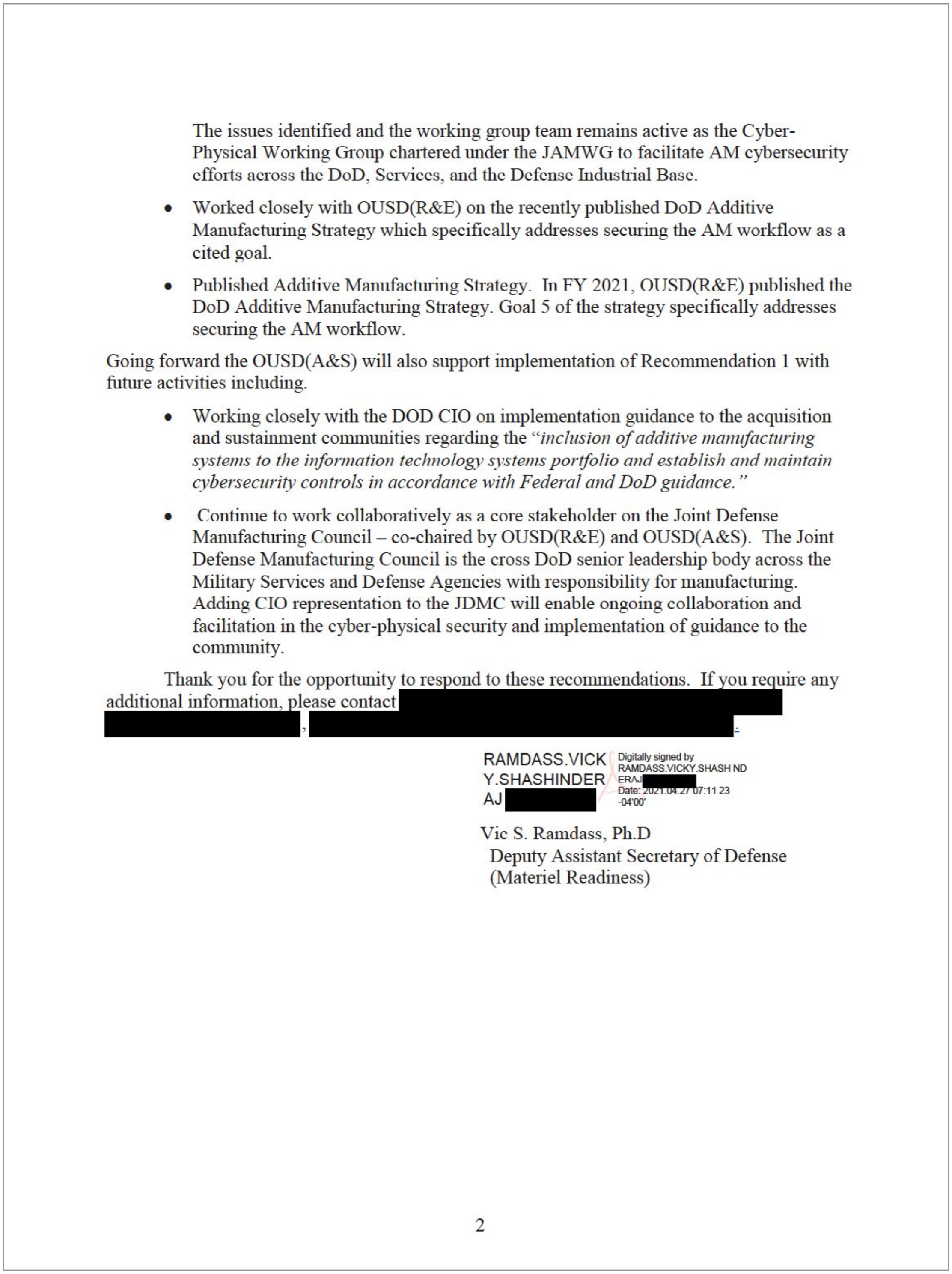
Response:

1. Concur. The inclusion of additive manufacturing systems to the information technology systems portfolio and establishing and maintaining cybersecurity controls in accordance with Federal and DoD guidance is fully supported by the OUSD(A&S).

The delegated authorities within OUSD(A&S) have taken several steps to prioritize cybersecurity for additive manufacturing including:

- In FY 2019, developed, coordinated and published DoD Directive Type Memorandum 19-006, establishing Department-wide interim and assigning appropriate responsibilities to ensure that the digital and cyber infrastructure supports AM for sustainment operations in appropriate policy and guidance.
- FY2019-FY2020, partnered with the OUSD(R&E) to organize and execute AM Cyber-security workshops with DoD, industry and academia subject matter experts.

Office of the Under Secretary of Defense for Acquisition and Sustainment (cont'd)



The issues identified and the working group team remains active as the Cyber-Physical Working Group chartered under the JAMWG to facilitate AM cybersecurity efforts across the DoD, Services, and the Defense Industrial Base.

- Worked closely with OUSD(R&E) on the recently published DoD Additive Manufacturing Strategy which specifically addresses securing the AM workflow as a cited goal.
- Published Additive Manufacturing Strategy. In FY 2021, OUSD(R&E) published the DoD Additive Manufacturing Strategy. Goal 5 of the strategy specifically addresses securing the AM workflow.

Going forward the OUSD(A&S) will also support implementation of Recommendation 1 with future activities including.

- Working closely with the DOD CIO on implementation guidance to the acquisition and sustainment communities regarding the "*inclusion of additive manufacturing systems to the information technology systems portfolio and establish and maintain cybersecurity controls in accordance with Federal and DoD guidance.*"
- Continue to work collaboratively as a core stakeholder on the Joint Defense Manufacturing Council – co-chaired by OUSD(R&E) and OUSD(A&S). The Joint Defense Manufacturing Council is the cross DoD senior leadership body across the Military Services and Defense Agencies with responsibility for manufacturing. Adding CIO representation to the JDMC will enable ongoing collaboration and facilitation in the cyber-physical security and implementation of guidance to the community.

Thank you for the opportunity to respond to these recommendations. If you require any additional information, please contact [redacted], [redacted].

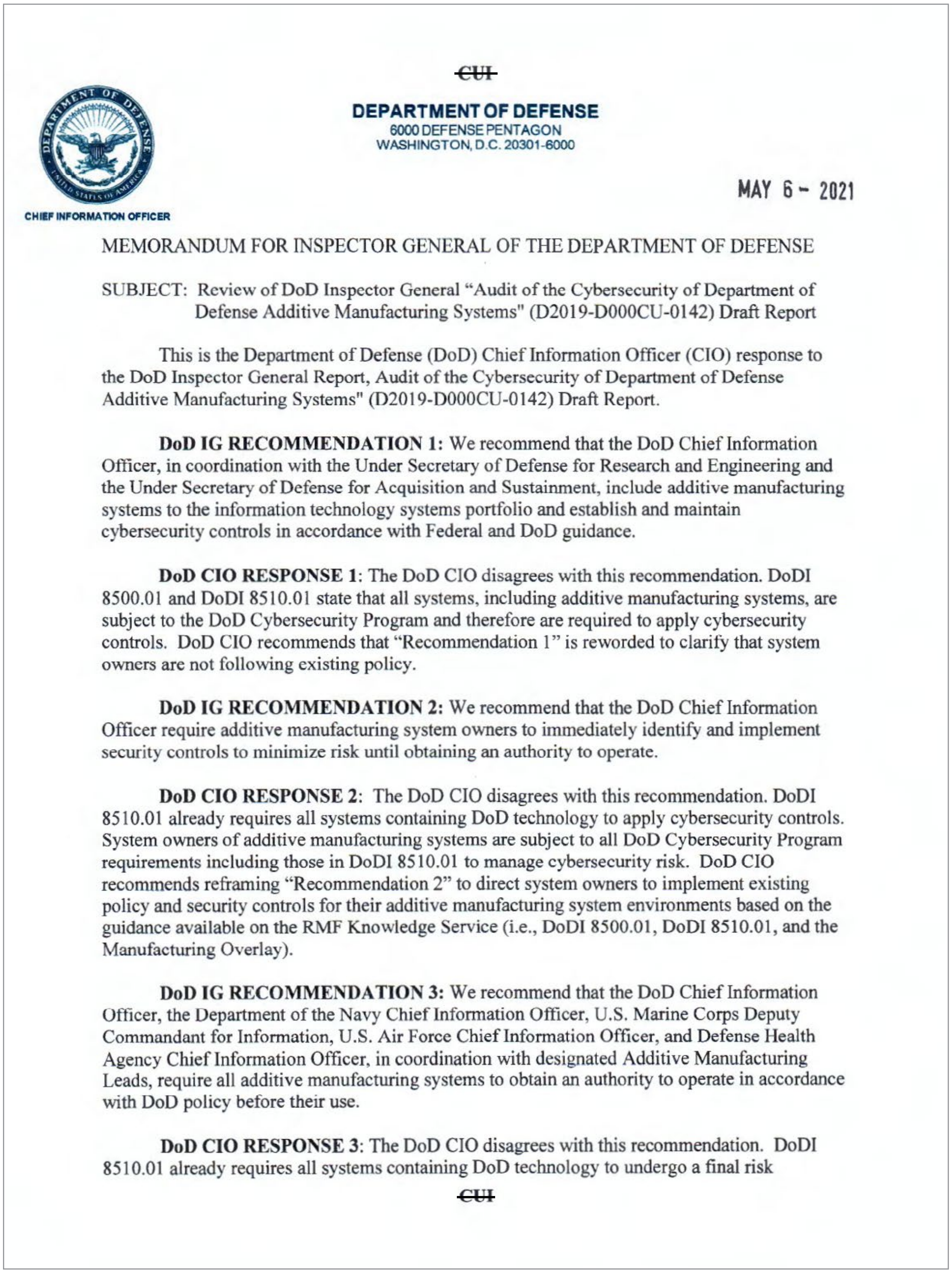
RAMDASS.VICK
Y.SHASHINDER
AJ [redacted]

Digitally signed by
RAMDASS.VICKY.SHASH ND
ERAJ [redacted]
Date: 2021.04.27 07:11 23
-04'00'

Vic S. Ramdass, Ph.D
Deputy Assistant Secretary of Defense
(Materiel Readiness)

2

Office of the DoD Chief Information Officer



~~CUI~~

DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

CHIEF INFORMATION OFFICER

MAY 6 - 2021

MEMORANDUM FOR INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE

SUBJECT: Review of DoD Inspector General "Audit of the Cybersecurity of Department of Defense Additive Manufacturing Systems" (D2019-D000CU-0142) Draft Report

This is the Department of Defense (DoD) Chief Information Officer (CIO) response to the DoD Inspector General Report, Audit of the Cybersecurity of Department of Defense Additive Manufacturing Systems" (D2019-D000CU-0142) Draft Report.

DoD IG RECOMMENDATION 1: We recommend that the DoD Chief Information Officer, in coordination with the Under Secretary of Defense for Research and Engineering and the Under Secretary of Defense for Acquisition and Sustainment, include additive manufacturing systems to the information technology systems portfolio and establish and maintain cybersecurity controls in accordance with Federal and DoD guidance.

DoD CIO RESPONSE 1: The DoD CIO disagrees with this recommendation. DoDI 8500.01 and DoDI 8510.01 state that all systems, including additive manufacturing systems, are subject to the DoD Cybersecurity Program and therefore are required to apply cybersecurity controls. DoD CIO recommends that "Recommendation 1" is reworded to clarify that system owners are not following existing policy.

DoD IG RECOMMENDATION 2: We recommend that the DoD Chief Information Officer require additive manufacturing system owners to immediately identify and implement security controls to minimize risk until obtaining an authority to operate.

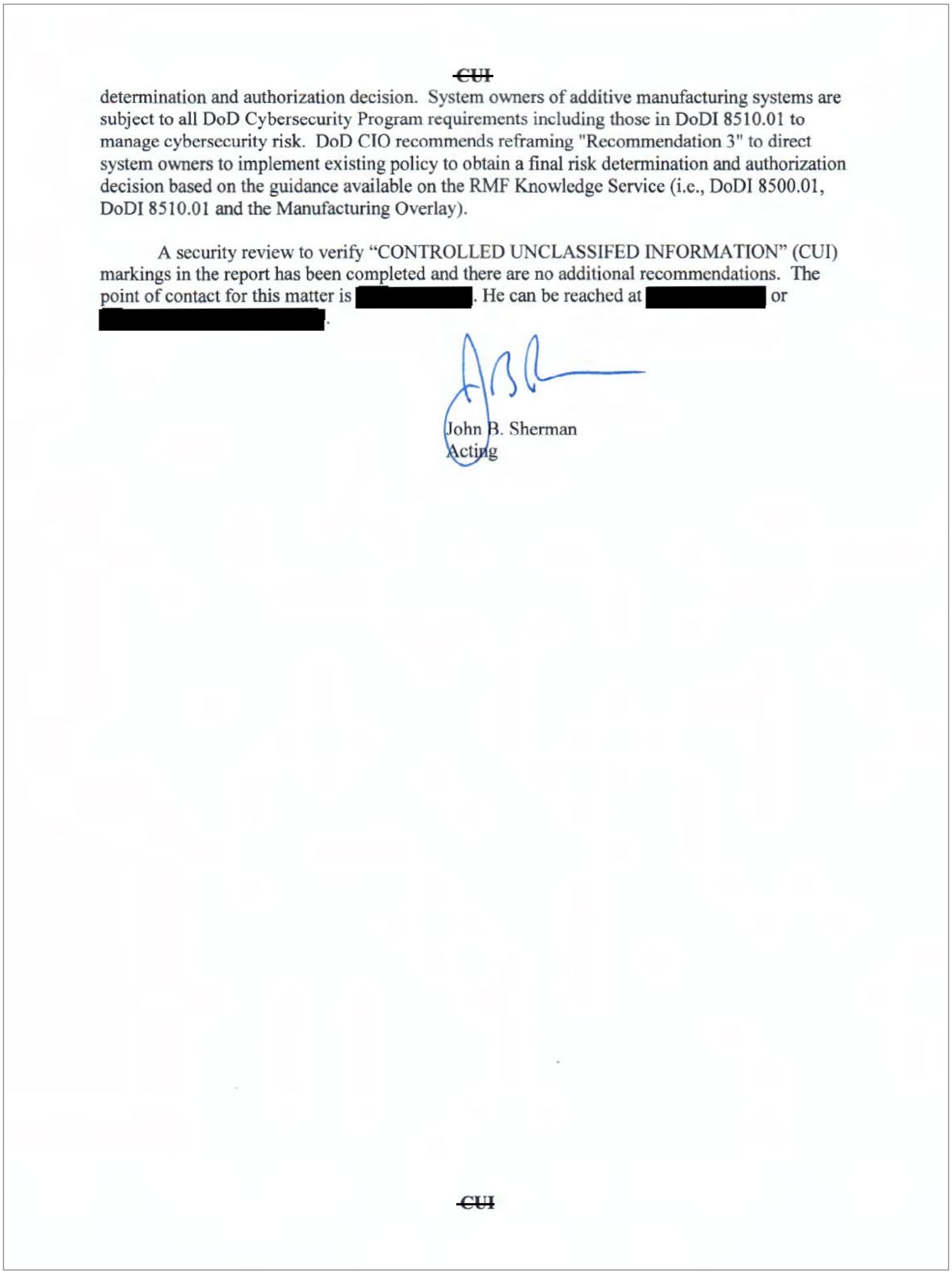
DoD CIO RESPONSE 2: The DoD CIO disagrees with this recommendation. DoDI 8510.01 already requires all systems containing DoD technology to apply cybersecurity controls. System owners of additive manufacturing systems are subject to all DoD Cybersecurity Program requirements including those in DoDI 8510.01 to manage cybersecurity risk. DoD CIO recommends reframing "Recommendation 2" to direct system owners to implement existing policy and security controls for their additive manufacturing system environments based on the guidance available on the RMF Knowledge Service (i.e., DoDI 8500.01, DoDI 8510.01, and the Manufacturing Overlay).

DoD IG RECOMMENDATION 3: We recommend that the DoD Chief Information Officer, the Department of the Navy Chief Information Officer, U.S. Marine Corps Deputy Commandant for Information, U.S. Air Force Chief Information Officer, and Defense Health Agency Chief Information Officer, in coordination with designated Additive Manufacturing Leads, require all additive manufacturing systems to obtain an authority to operate in accordance with DoD policy before their use.

DoD CIO RESPONSE 3: The DoD CIO disagrees with this recommendation. DoDI 8510.01 already requires all systems containing DoD technology to undergo a final risk

~~CUI~~

Office of the DoD Chief Information Officer (cont’d)



~~CUI~~

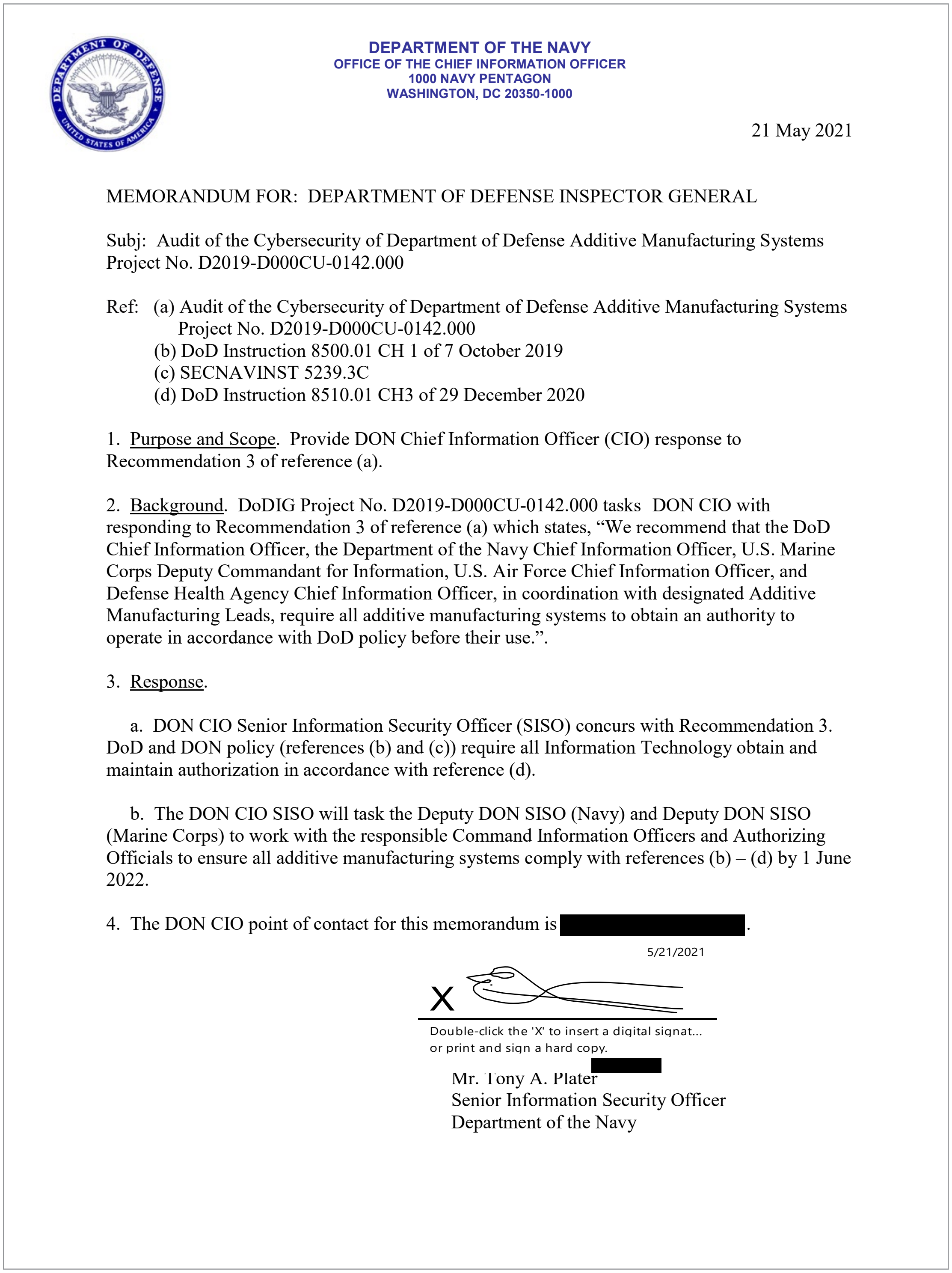
determination and authorization decision. System owners of additive manufacturing systems are subject to all DoD Cybersecurity Program requirements including those in DoDI 8510.01 to manage cybersecurity risk. DoD CIO recommends reframing "Recommendation 3" to direct system owners to implement existing policy to obtain a final risk determination and authorization decision based on the guidance available on the RMF Knowledge Service (i.e., DoDI 8500.01, DoDI 8510.01 and the Manufacturing Overlay).

A security review to verify “CONTROLLED UNCLASSIFED INFORMATION” (CUI) markings in the report has been completed and there are no additional recommendations. The point of contact for this matter is [redacted]. He can be reached at [redacted] or [redacted].

John B. Sherman
Acting

~~CUI~~

Office of the Department of the Navy Chief Information Officer



DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF INFORMATION OFFICER
1000 NAVY PENTAGON
WASHINGTON, DC 20350-1000

21 May 2021

MEMORANDUM FOR: DEPARTMENT OF DEFENSE INSPECTOR GENERAL

Subj: Audit of the Cybersecurity of Department of Defense Additive Manufacturing Systems
Project No. D2019-D000CU-0142.000

Ref: (a) Audit of the Cybersecurity of Department of Defense Additive Manufacturing Systems
Project No. D2019-D000CU-0142.000
(b) DoD Instruction 8500.01 CH 1 of 7 October 2019
(c) SECNAVINST 5239.3C
(d) DoD Instruction 8510.01 CH3 of 29 December 2020

1. Purpose and Scope. Provide DON Chief Information Officer (CIO) response to Recommendation 3 of reference (a).

2. Background. DoDIG Project No. D2019-D000CU-0142.000 tasks DON CIO with responding to Recommendation 3 of reference (a) which states, “We recommend that the DoD Chief Information Officer, the Department of the Navy Chief Information Officer, U.S. Marine Corps Deputy Commandant for Information, U.S. Air Force Chief Information Officer, and Defense Health Agency Chief Information Officer, in coordination with designated Additive Manufacturing Leads, require all additive manufacturing systems to obtain an authority to operate in accordance with DoD policy before their use.”.

3. Response.

a. DON CIO Senior Information Security Officer (SISO) concurs with Recommendation 3. DoD and DON policy (references (b) and (c)) require all Information Technology obtain and maintain authorization in accordance with reference (d).

b. The DON CIO SISO will task the Deputy DON SISO (Navy) and Deputy DON SISO (Marine Corps) to work with the responsible Command Information Officers and Authorizing Officials to ensure all additive manufacturing systems comply with references (b) – (d) by 1 June 2022.

4. The DON CIO point of contact for this memorandum is [redacted].

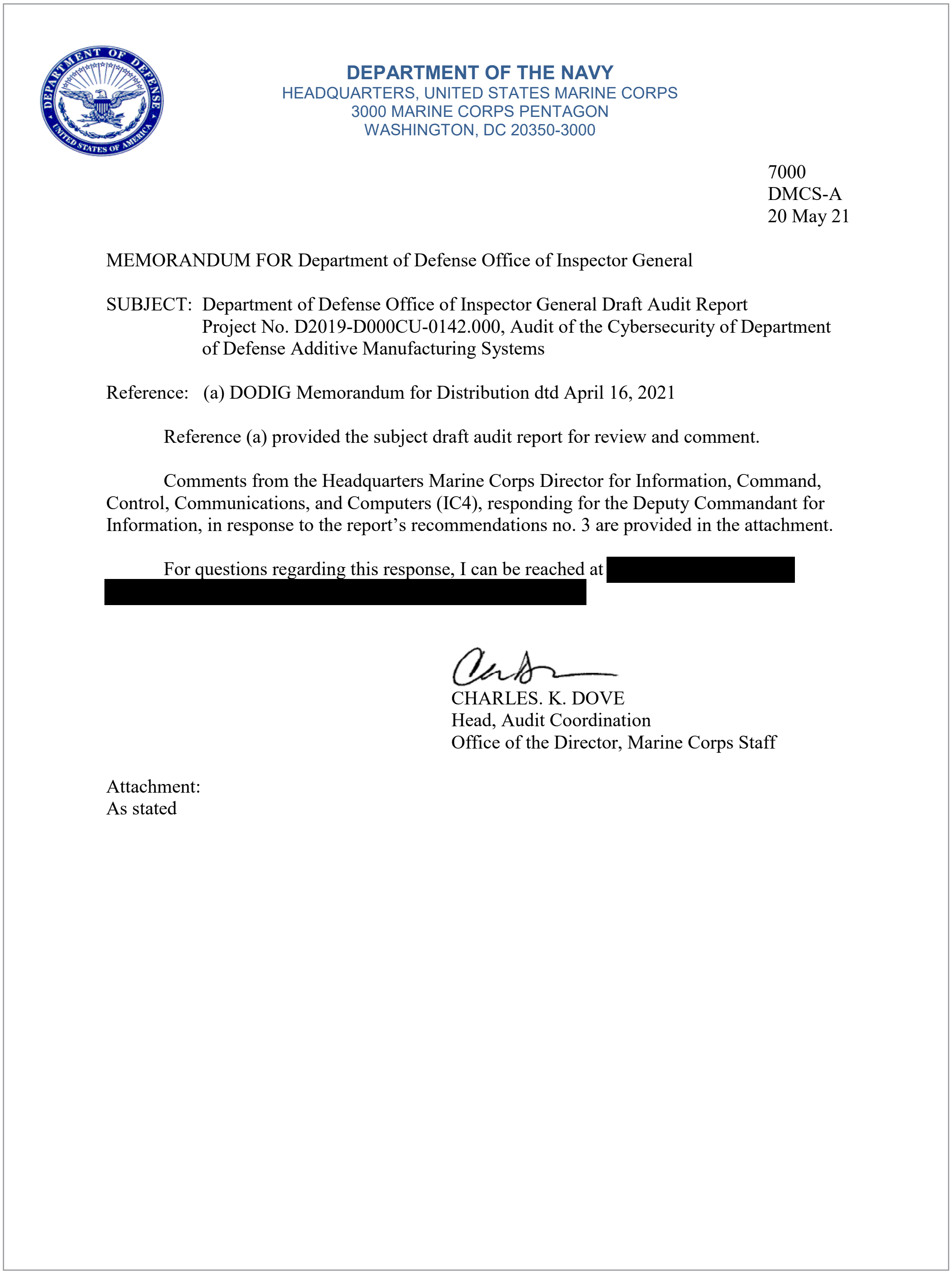
5/21/2021

X

Double-click the 'X' to insert a digital signat...
or print and sign a hard copy.

Mr. Tony A. Plater [redacted]
Senior Information Security Officer
Department of the Navy

Office of the U.S. Marine Corps Deputy Commandant for Information



DEPARTMENT OF THE NAVY
HEADQUARTERS, UNITED STATES MARINE CORPS
3000 MARINE CORPS PENTAGON
WASHINGTON, DC 20350-3000

7000
DMCS-A
20 May 21

MEMORANDUM FOR Department of Defense Office of Inspector General

SUBJECT: Department of Defense Office of Inspector General Draft Audit Report Project No. D2019-D000CU-0142.000, Audit of the Cybersecurity of Department of Defense Additive Manufacturing Systems

Reference: (a) DODIG Memorandum for Distribution dtd April 16, 2021

Reference (a) provided the subject draft audit report for review and comment.

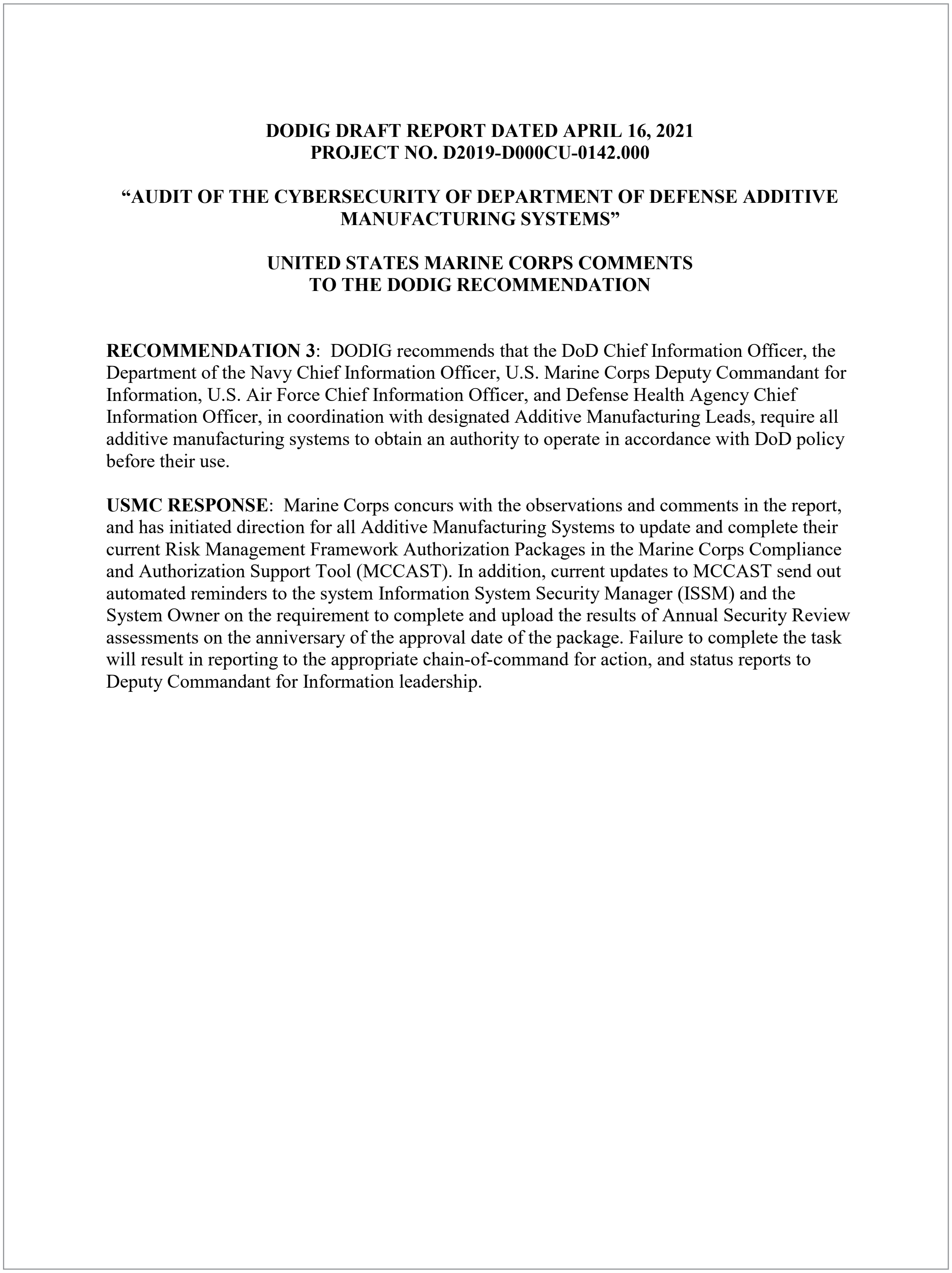
Comments from the Headquarters Marine Corps Director for Information, Command, Control, Communications, and Computers (IC4), responding for the Deputy Commandant for Information, in response to the report's recommendations no. 3 are provided in the attachment.

For questions regarding this response, I can be reached at [redacted]

CHARLES. K. DOVE
Head, Audit Coordination
Office of the Director, Marine Corps Staff

Attachment:
As stated

Office of the U.S. Marine Corps Deputy Commandant for Information (cont'd)



DODIG DRAFT REPORT DATED APRIL 16, 2021
PROJECT NO. D2019-D000CU-0142.000

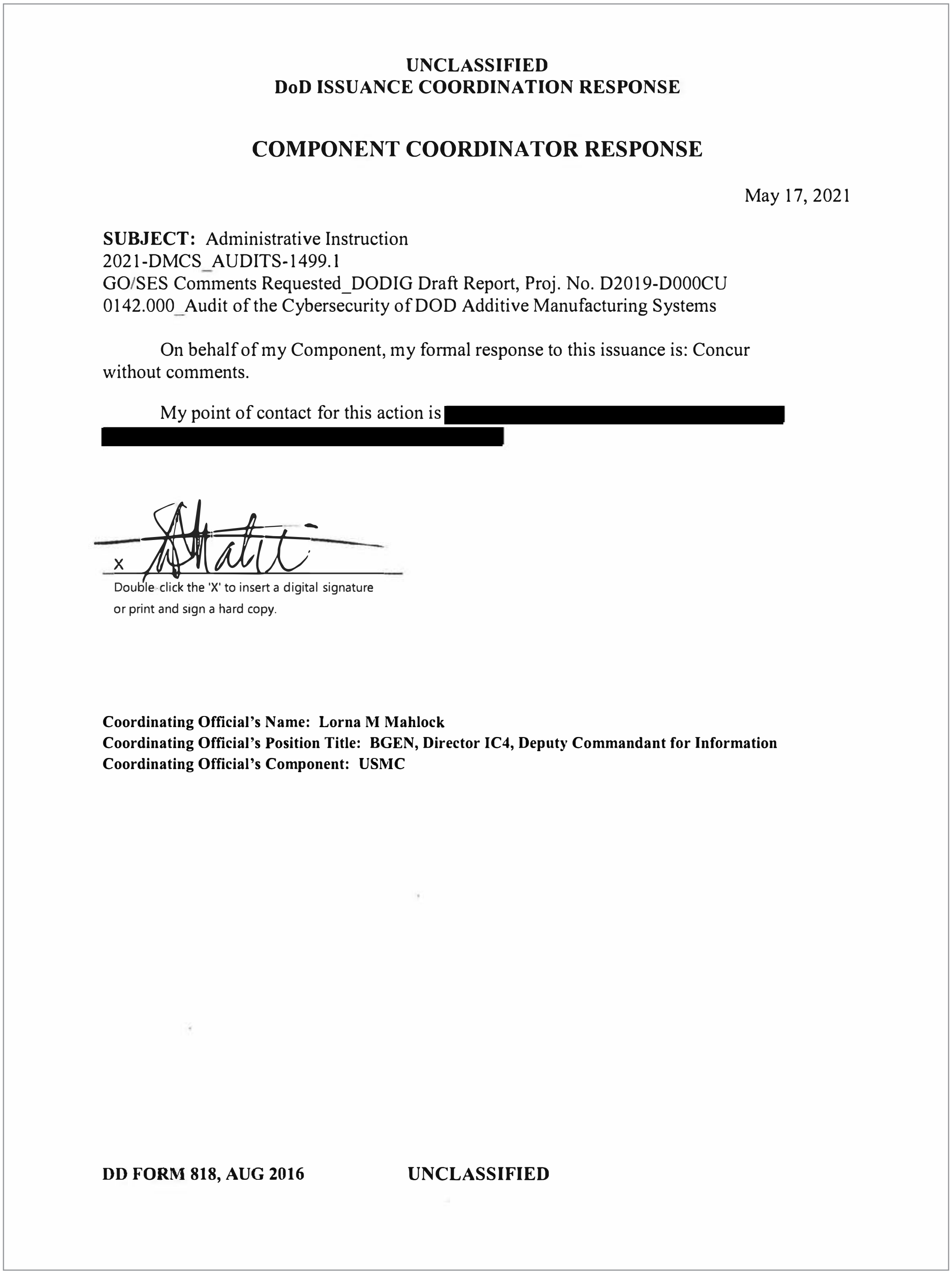
"AUDIT OF THE CYBERSECURITY OF DEPARTMENT OF DEFENSE ADDITIVE MANUFACTURING SYSTEMS"

UNITED STATES MARINE CORPS COMMENTS
TO THE DODIG RECOMMENDATION

RECOMMENDATION 3: DODIG recommends that the DoD Chief Information Officer, the Department of the Navy Chief Information Officer, U.S. Marine Corps Deputy Commandant for Information, U.S. Air Force Chief Information Officer, and Defense Health Agency Chief Information Officer, in coordination with designated Additive Manufacturing Leads, require all additive manufacturing systems to obtain an authority to operate in accordance with DoD policy before their use.

USMC RESPONSE: Marine Corps concurs with the observations and comments in the report, and has initiated direction for all Additive Manufacturing Systems to update and complete their current Risk Management Framework Authorization Packages in the Marine Corps Compliance and Authorization Support Tool (MCCAST). In addition, current updates to MCCAST send out automated reminders to the system Information System Security Manager (ISSM) and the System Owner on the requirement to complete and upload the results of Annual Security Review assessments on the anniversary of the approval date of the package. Failure to complete the task will result in reporting to the appropriate chain-of-command for action, and status reports to Deputy Commandant for Information leadership.

Office of the U.S. Marine Corps Deputy Commandant for Information (cont'd)



UNCLASSIFIED
DoD ISSUANCE COORDINATION RESPONSE

COMPONENT COORDINATOR RESPONSE

May 17, 2021

SUBJECT: Administrative Instruction
2021-DMCS_AUDITS-1499.1
GO/SES Comments Requested_DODIG Draft Report, Proj. No. D2019-D000CU
0142.000_Audit of the Cybersecurity of DOD Additive Manufacturing Systems

On behalf of my Component, my formal response to this issuance is: Concur without comments.

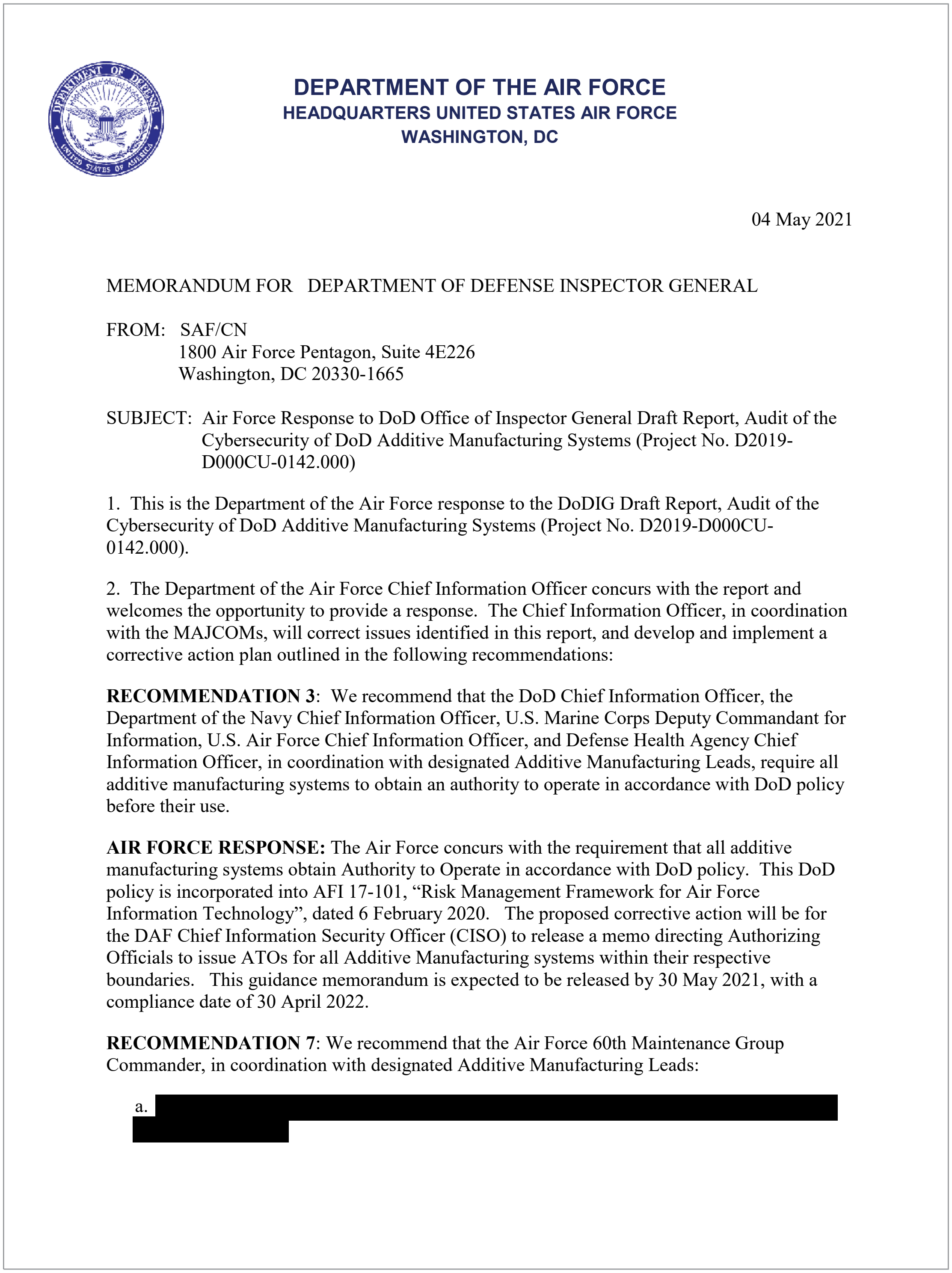
My point of contact for this action is [redacted]

X
Double click the 'X' to insert a digital signature or print and sign a hard copy.

Coordinating Official's Name: Lorna M Mahlock
Coordinating Official's Position Title: BGEN, Director IC4, Deputy Commandant for Information
Coordinating Official's Component: USMC

DD FORM 818, AUG 2016 **UNCLASSIFIED**

Office of Department of the Air Force Chief Information Officer



DEPARTMENT OF THE AIR FORCE
HEADQUARTERS UNITED STATES AIR FORCE
WASHINGTON, DC

04 May 2021

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL

FROM: SAF/CN
1800 Air Force Pentagon, Suite 4E226
Washington, DC 20330-1665

SUBJECT: Air Force Response to DoD Office of Inspector General Draft Report, Audit of the Cybersecurity of DoD Additive Manufacturing Systems (Project No. D2019-D000CU-0142.000)

1. This is the Department of the Air Force response to the DoDIG Draft Report, Audit of the Cybersecurity of DoD Additive Manufacturing Systems (Project No. D2019-D000CU-0142.000).

2. The Department of the Air Force Chief Information Officer concurs with the report and welcomes the opportunity to provide a response. The Chief Information Officer, in coordination with the MAJCOMs, will correct issues identified in this report, and develop and implement a corrective action plan outlined in the following recommendations:

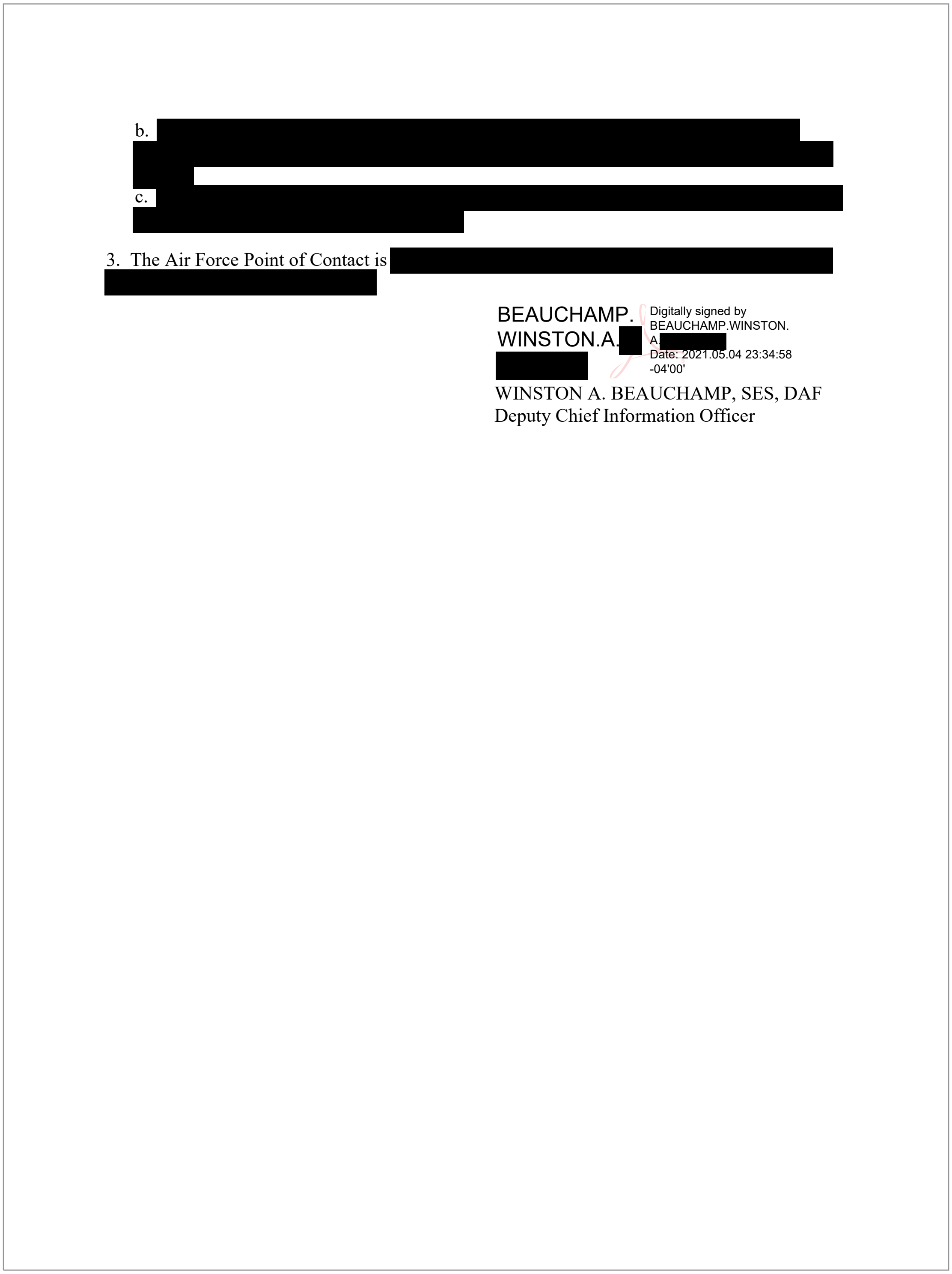
RECOMMENDATION 3: We recommend that the DoD Chief Information Officer, the Department of the Navy Chief Information Officer, U.S. Marine Corps Deputy Commandant for Information, U.S. Air Force Chief Information Officer, and Defense Health Agency Chief Information Officer, in coordination with designated Additive Manufacturing Leads, require all additive manufacturing systems to obtain an authority to operate in accordance with DoD policy before their use.

AIR FORCE RESPONSE: The Air Force concurs with the requirement that all additive manufacturing systems obtain Authority to Operate in accordance with DoD policy. This DoD policy is incorporated into AFI 17-101, "Risk Management Framework for Air Force Information Technology", dated 6 February 2020. The proposed corrective action will be for the DAF Chief Information Security Officer (CISO) to release a memo directing Authorizing Officials to issue ATOs for all Additive Manufacturing systems within their respective boundaries. This guidance memorandum is expected to be released by 30 May 2021, with a compliance date of 30 April 2022.

RECOMMENDATION 7: We recommend that the Air Force 60th Maintenance Group Commander, in coordination with designated Additive Manufacturing Leads:

a. [redacted]

Office of the Department of the Air Force Chief Information Officer (cont'd)



b. [redacted]

c. [redacted]

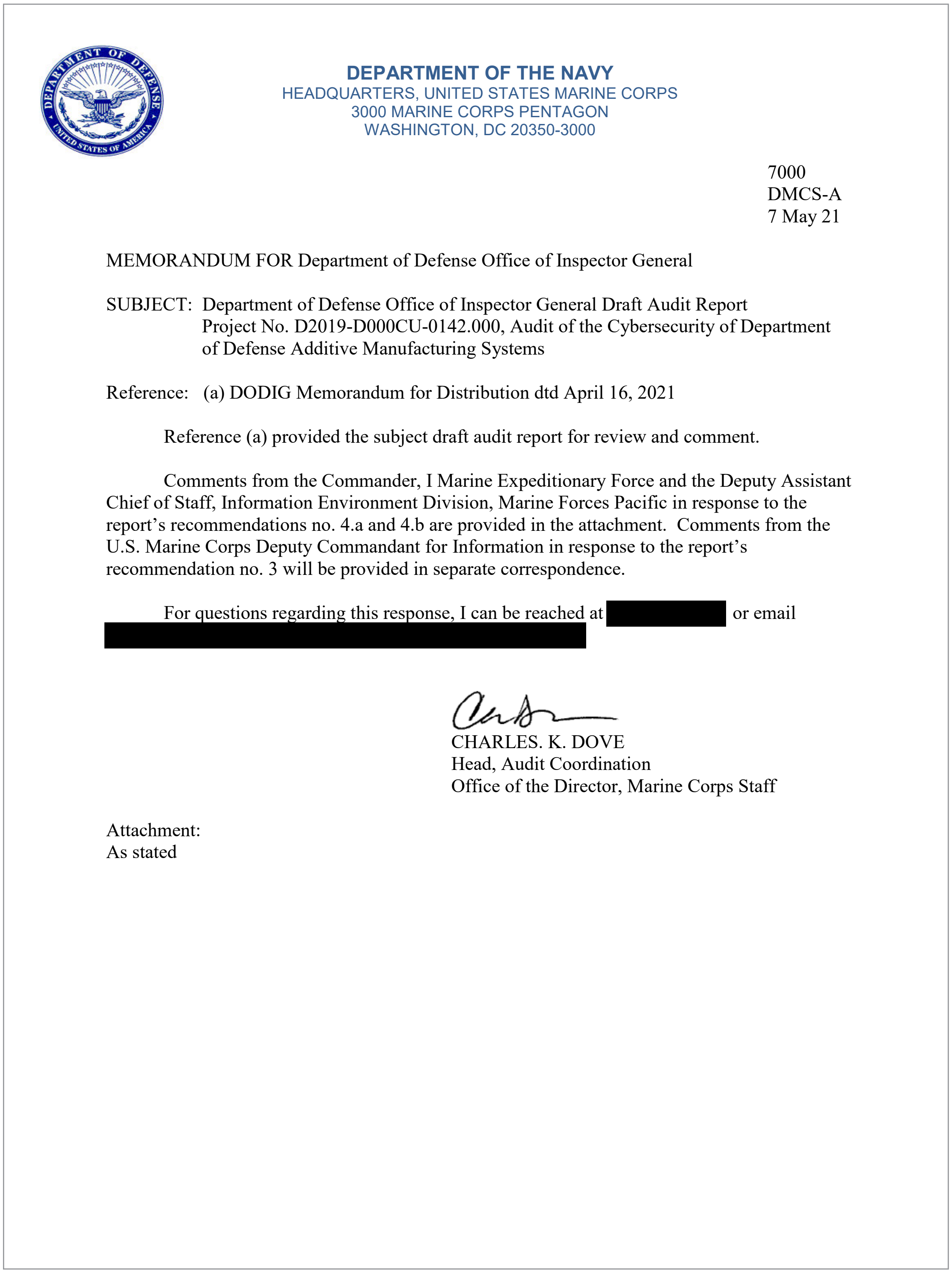
3. The Air Force Point of Contact is [redacted]

BEAUCHAMP.
WINSTON.A.[redacted]
[redacted]

Digitally signed by
BEAUCHAMP.WINSTON.
A.[redacted]
Date: 2021.05.04 23:34:58
-04'00'

WINSTON A. BEAUCHAMP, SES, DAF
Deputy Chief Information Officer

1st Marine Expeditionary Force



DEPARTMENT OF THE NAVY
HEADQUARTERS, UNITED STATES MARINE CORPS
3000 MARINE CORPS PENTAGON
WASHINGTON, DC 20350-3000

7000
DMCS-A
7 May 21

MEMORANDUM FOR Department of Defense Office of Inspector General

SUBJECT: Department of Defense Office of Inspector General Draft Audit Report Project No. D2019-D000CU-0142.000, Audit of the Cybersecurity of Department of Defense Additive Manufacturing Systems

Reference: (a) DODIG Memorandum for Distribution dtd April 16, 2021

Reference (a) provided the subject draft audit report for review and comment.

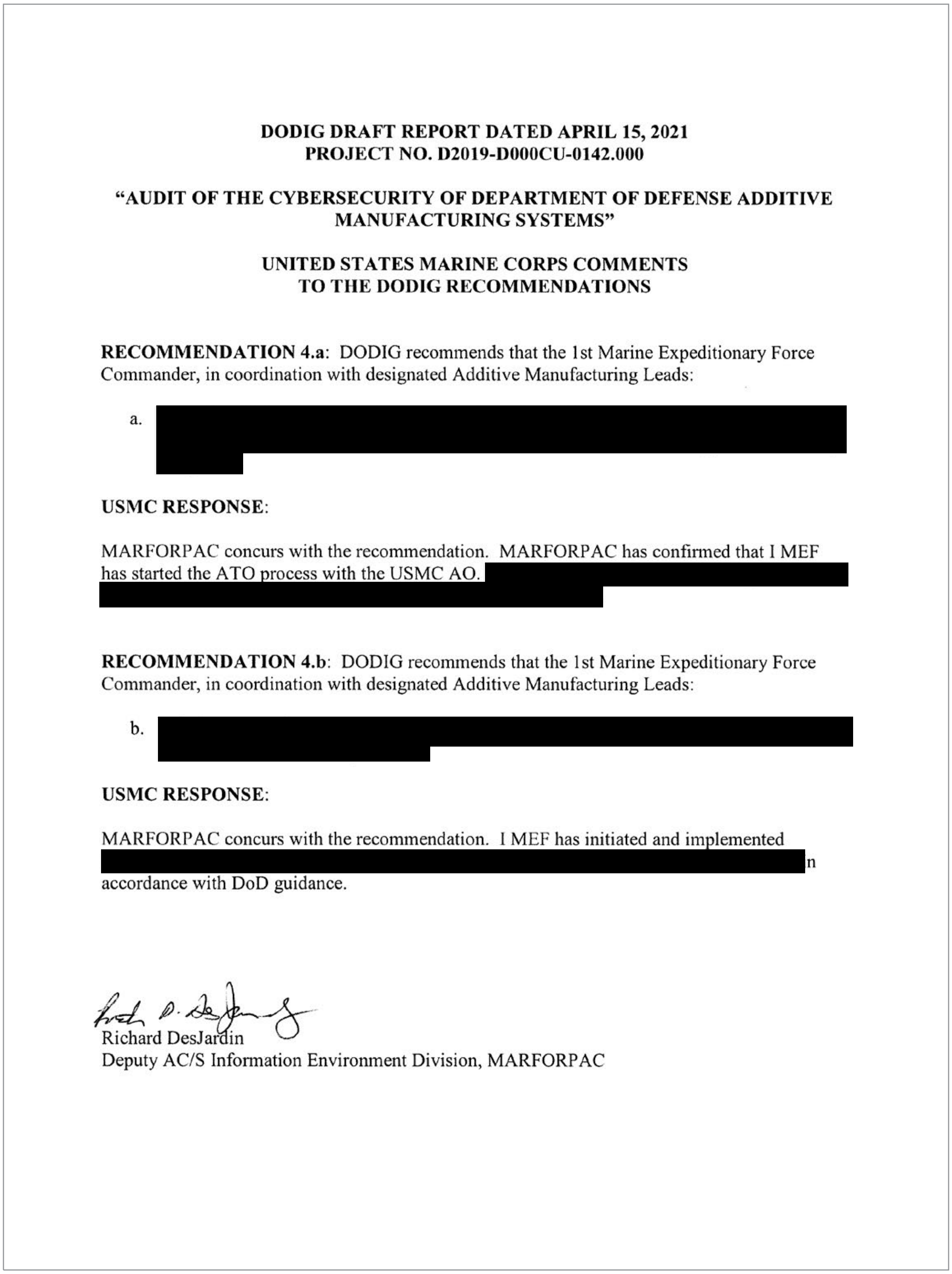
Comments from the Commander, I Marine Expeditionary Force and the Deputy Assistant Chief of Staff, Information Environment Division, Marine Forces Pacific in response to the report's recommendations no. 4.a and 4.b are provided in the attachment. Comments from the U.S. Marine Corps Deputy Commandant for Information in response to the report's recommendation no. 3 will be provided in separate correspondence.

For questions regarding this response, I can be reached at [redacted] or email [redacted]

CHARLES. K. DOVE
Head, Audit Coordination
Office of the Director, Marine Corps Staff

Attachment:
As stated

1st Marine Expeditionary Force (cont'd)



DODIG DRAFT REPORT DATED APRIL 15, 2021
PROJECT NO. D2019-D000CU-0142.000

"AUDIT OF THE CYBERSECURITY OF DEPARTMENT OF DEFENSE ADDITIVE MANUFACTURING SYSTEMS"

UNITED STATES MARINE CORPS COMMENTS
TO THE DODIG RECOMMENDATIONS

RECOMMENDATION 4.a: DODIG recommends that the 1st Marine Expeditionary Force Commander, in coordination with designated Additive Manufacturing Leads:

a. [redacted]

USMC RESPONSE:

MARFORPAC concurs with the recommendation. MARFORPAC has confirmed that I MEF has started the ATO process with the USMC AO. [redacted]

RECOMMENDATION 4.b: DODIG recommends that the 1st Marine Expeditionary Force Commander, in coordination with designated Additive Manufacturing Leads:

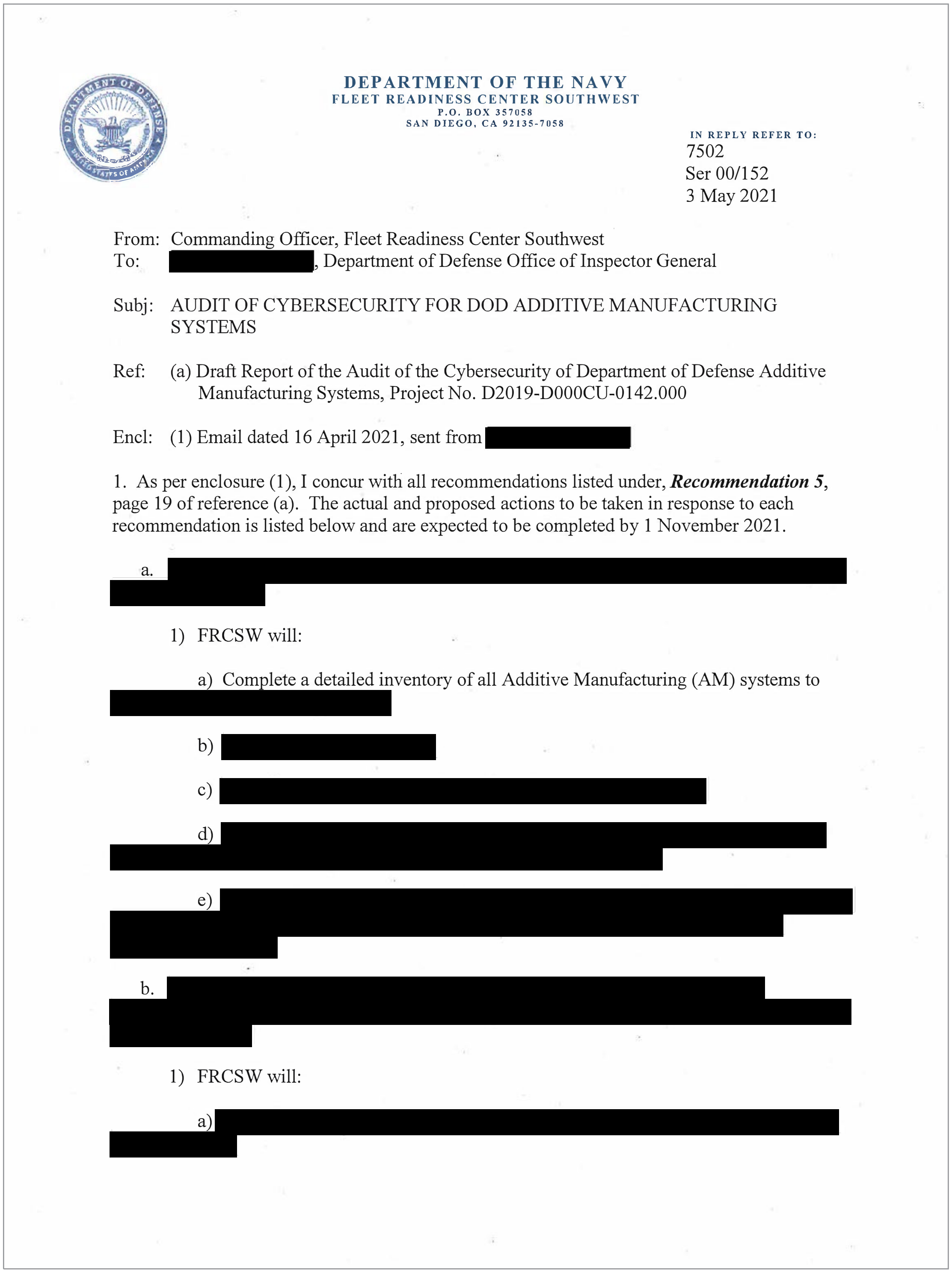
b. [redacted]

USMC RESPONSE:

MARFORPAC concurs with the recommendation. I MEF has initiated and implemented [redacted] n accordance with DoD guidance.

Richard DesJardin
Deputy AC/S Information Environment Division, MARFORPAC

Navy Fleet Readiness Center Southwest



DEPARTMENT OF THE NAVY
FLEET READINESS CENTER SOUTHWEST
P.O. BOX 357058
SAN DIEGO, CA 92135-7058

IN REPLY REFER TO:
7502
Ser 00/152
3 May 2021

From: Commanding Officer, Fleet Readiness Center Southwest
To: [redacted], Department of Defense Office of Inspector General

Subj: AUDIT OF CYBERSECURITY FOR DOD ADDITIVE MANUFACTURING SYSTEMS

Ref: (a) Draft Report of the Audit of the Cybersecurity of Department of Defense Additive Manufacturing Systems, Project No. D2019-D000CU-0142.000

Encl: (1) Email dated 16 April 2021, sent from [redacted]

1. As per enclosure (1), I concur with all recommendations listed under, ***Recommendation 5***, page 19 of reference (a). The actual and proposed actions to be taken in response to each recommendation is listed below and are expected to be completed by 1 November 2021.

a. [redacted]

1) FRCSW will:

a) Complete a detailed inventory of all Additive Manufacturing (AM) systems to [redacted]

b) [redacted]

c) [redacted]

d) [redacted]

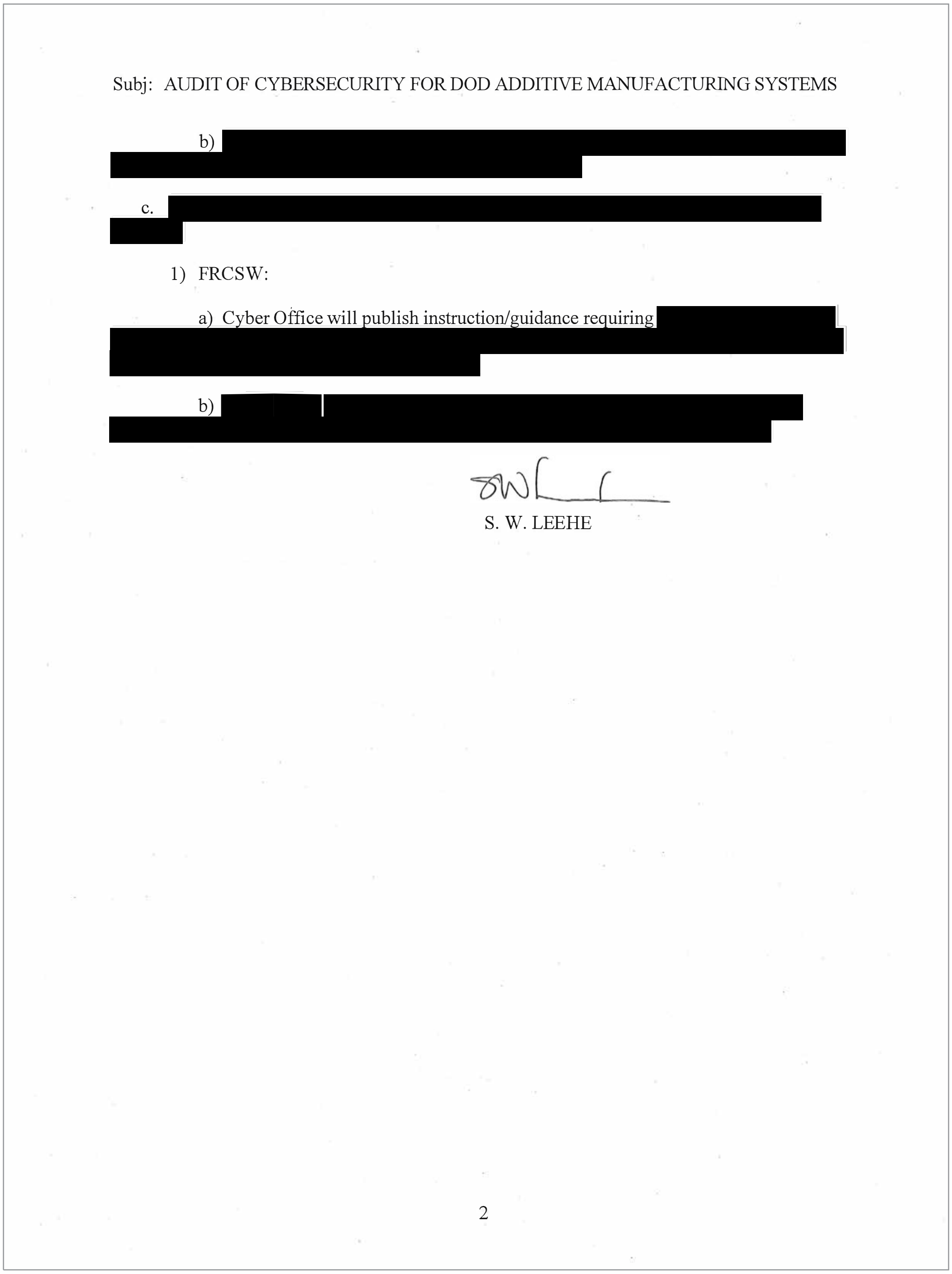
e) [redacted]

b. [redacted]

1) FRCSW will:

a) [redacted]

Navy Fleet Readiness Center Southwest (cont’d)



Subj: AUDIT OF CYBERSECURITY FOR DOD ADDITIVE MANUFACTURING SYSTEMS

b) [redacted]

c. [redacted]

1) FRCSW:

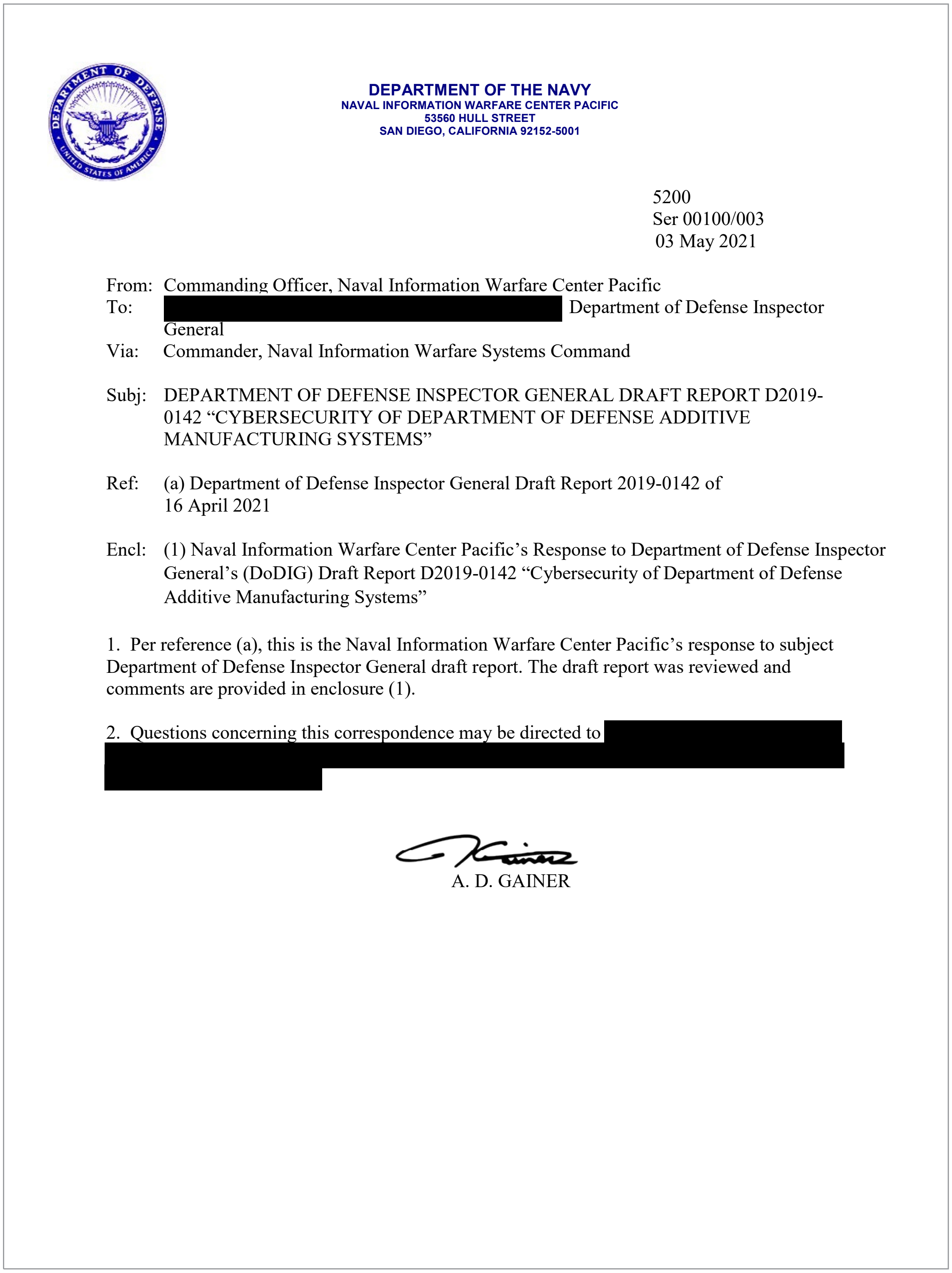
a) Cyber Office will publish instruction/guidance requiring [redacted]

b) [redacted]

S. W. LEEHE

2

Naval Information Warfare Center Pacific



DEPARTMENT OF THE NAVY
NAVAL INFORMATION WARFARE CENTER PACIFIC
53560 HULL STREET
SAN DIEGO, CALIFORNIA 92152-5001

5200
Ser 00100/003
03 May 2021

From: Commanding Officer, Naval Information Warfare Center Pacific
To: [redacted] Department of Defense Inspector General
Via: Commander, Naval Information Warfare Systems Command

Subj: DEPARTMENT OF DEFENSE INSPECTOR GENERAL DRAFT REPORT D2019-0142 "CYBERSECURITY OF DEPARTMENT OF DEFENSE ADDITIVE MANUFACTURING SYSTEMS"

Ref: (a) Department of Defense Inspector General Draft Report 2019-0142 of 16 April 2021

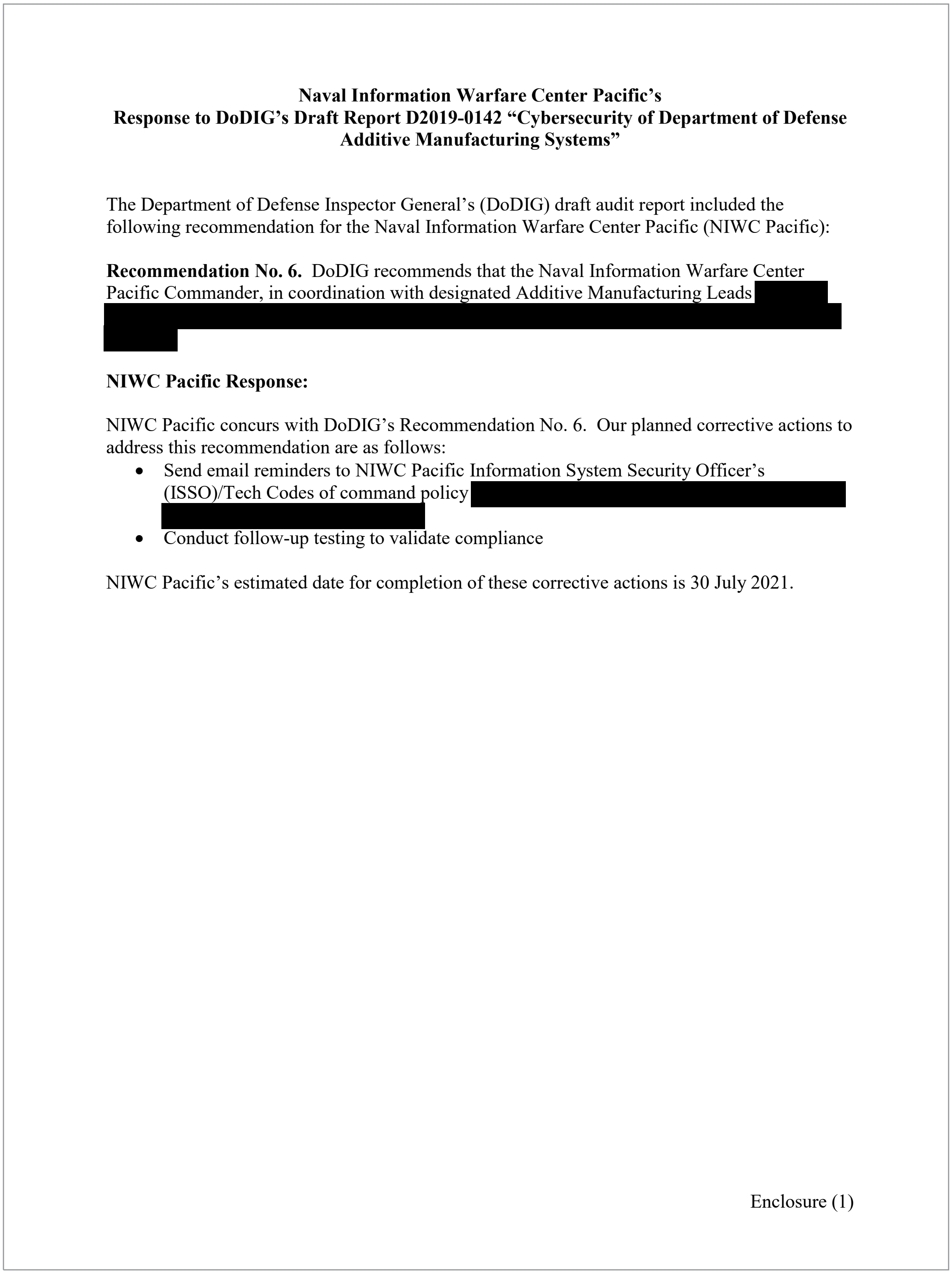
Encl: (1) Naval Information Warfare Center Pacific's Response to Department of Defense Inspector General's (DoDIG) Draft Report D2019-0142 "Cybersecurity of Department of Defense Additive Manufacturing Systems"

1. Per reference (a), this is the Naval Information Warfare Center Pacific's response to subject Department of Defense Inspector General draft report. The draft report was reviewed and comments are provided in enclosure (1).

2. Questions concerning this correspondence may be directed to [redacted]

A. D. GAINER

Naval Information Warfare Center Pacific (cont'd)



Naval Information Warfare Center Pacific's
Response to DoDIG's Draft Report D2019-0142 "Cybersecurity of Department of Defense Additive Manufacturing Systems"

The Department of Defense Inspector General's (DoDIG) draft audit report included the following recommendation for the Naval Information Warfare Center Pacific (NIWC Pacific):

Recommendation No. 6. DoDIG recommends that the Naval Information Warfare Center Pacific Commander, in coordination with designated Additive Manufacturing Leads [redacted]

NIWC Pacific Response:

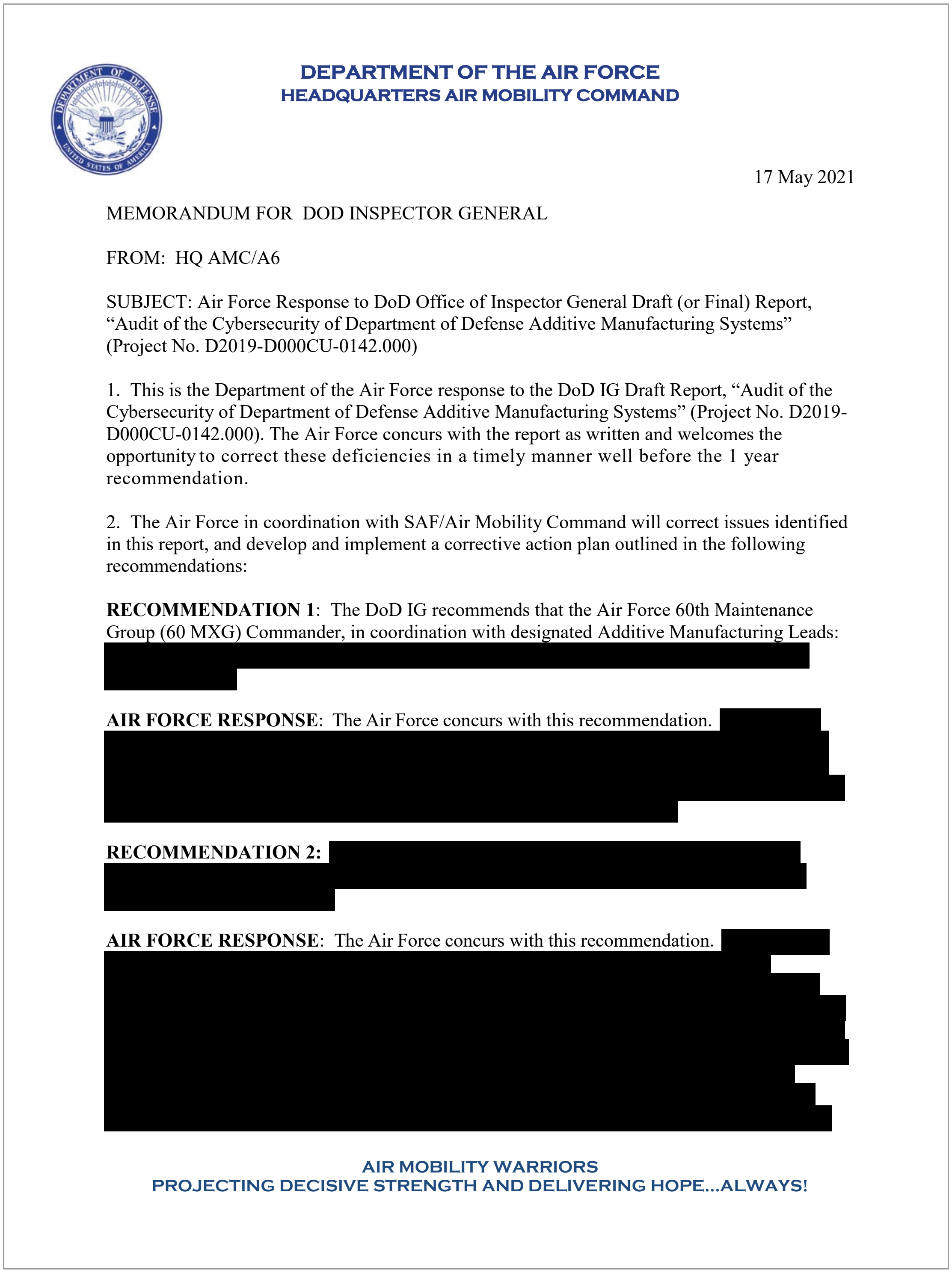
NIWC Pacific concurs with DoDIG's Recommendation No. 6. Our planned corrective actions to address this recommendation are as follows:

- Send email reminders to NIWC Pacific Information System Security Officer's (ISSO)/Tech Codes of command policy [redacted]
- Conduct follow-up testing to validate compliance

NIWC Pacific's estimated date for completion of these corrective actions is 30 July 2021.

Enclosure (1)

Air Force 60th Maintenance Group



DEPARTMENT OF THE AIR FORCE
HEADQUARTERS AIR MOBILITY COMMAND

17 May 2021

MEMORANDUM FOR DOD INSPECTOR GENERAL

FROM: HQ AMC/A6

SUBJECT: Air Force Response to DoD Office of Inspector General Draft (or Final) Report, "Audit of the Cybersecurity of Department of Defense Additive Manufacturing Systems" (Project No. D2019-D000CU-0142.000)

1. This is the Department of the Air Force response to the DoD IG Draft Report, "Audit of the Cybersecurity of Department of Defense Additive Manufacturing Systems" (Project No. D2019-D000CU-0142.000). The Air Force concurs with the report as written and welcomes the opportunity to correct these deficiencies in a timely manner well before the 1 year recommendation.

2. The Air Force in coordination with SAF/Air Mobility Command will correct issues identified in this report, and develop and implement a corrective action plan outlined in the following recommendations:

RECOMMENDATION 1: The DoD IG recommends that the Air Force 60th Maintenance Group (60 MXG) Commander, in coordination with designated Additive Manufacturing Leads: [redacted]

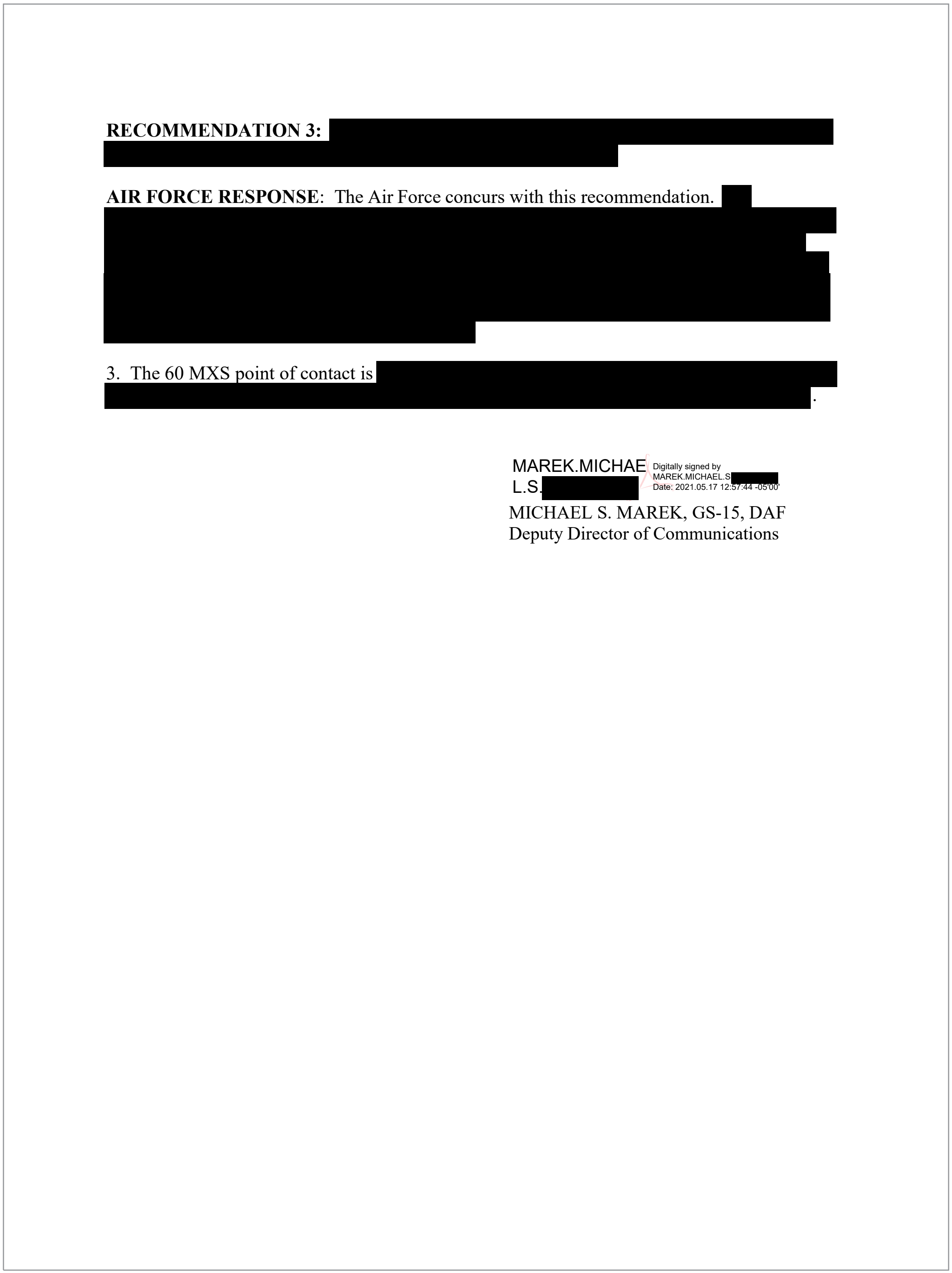
AIR FORCE RESPONSE: The Air Force concurs with this recommendation. [redacted]

RECOMMENDATION 2: [redacted]

AIR FORCE RESPONSE: The Air Force concurs with this recommendation. [redacted]

AIR MOBILITY WARRIORS
PROJECTING DECISIVE STRENGTH AND DELIVERING HOPE...ALWAYS!

Air Force 60th Maintenance Group (cont'd)



RECOMMENDATION 3: [redacted]

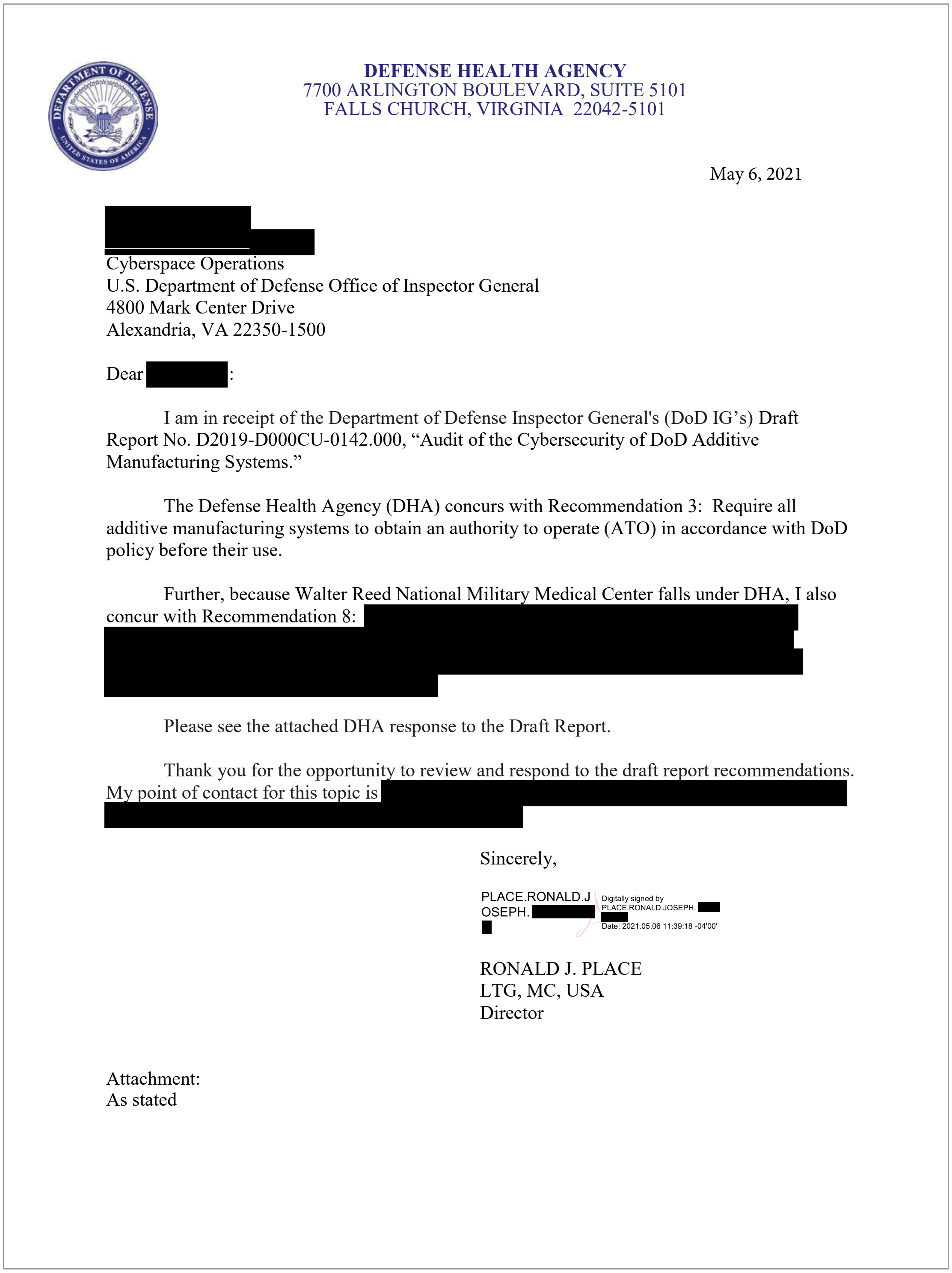
AIR FORCE RESPONSE: The Air Force concurs with this recommendation. [redacted]

3. The 60 MXS point of contact is [redacted].

MAREK.MICHAEL.S.[redacted] Digitally signed by MAREK.MICHAEL.S[redacted] Date: 2021.05.17 12:57:44 -05'00'

MICHAEL S. MAREK, GS-15, DAF
Deputy Director of Communications

Defense Health Agency



DEFENSE HEALTH AGENCY
7700 ARLINGTON BOULEVARD, SUITE 5101
FALLS CHURCH, VIRGINIA 22042-5101

May 6, 2021

[redacted]
Cyberspace Operations
U.S. Department of Defense Office of Inspector General
4800 Mark Center Drive
Alexandria, VA 22350-1500

Dear [redacted]:

I am in receipt of the Department of Defense Inspector General's (DoD IG's) Draft Report No. D2019-D000CU-0142.000, "Audit of the Cybersecurity of DoD Additive Manufacturing Systems."

The Defense Health Agency (DHA) concurs with Recommendation 3: Require all additive manufacturing systems to obtain an authority to operate (ATO) in accordance with DoD policy before their use.

Further, because Walter Reed National Military Medical Center falls under DHA, I also concur with Recommendation 8: [redacted]

Please see the attached DHA response to the Draft Report.

Thank you for the opportunity to review and respond to the draft report recommendations. My point of contact for this topic is [redacted]

Sincerely,

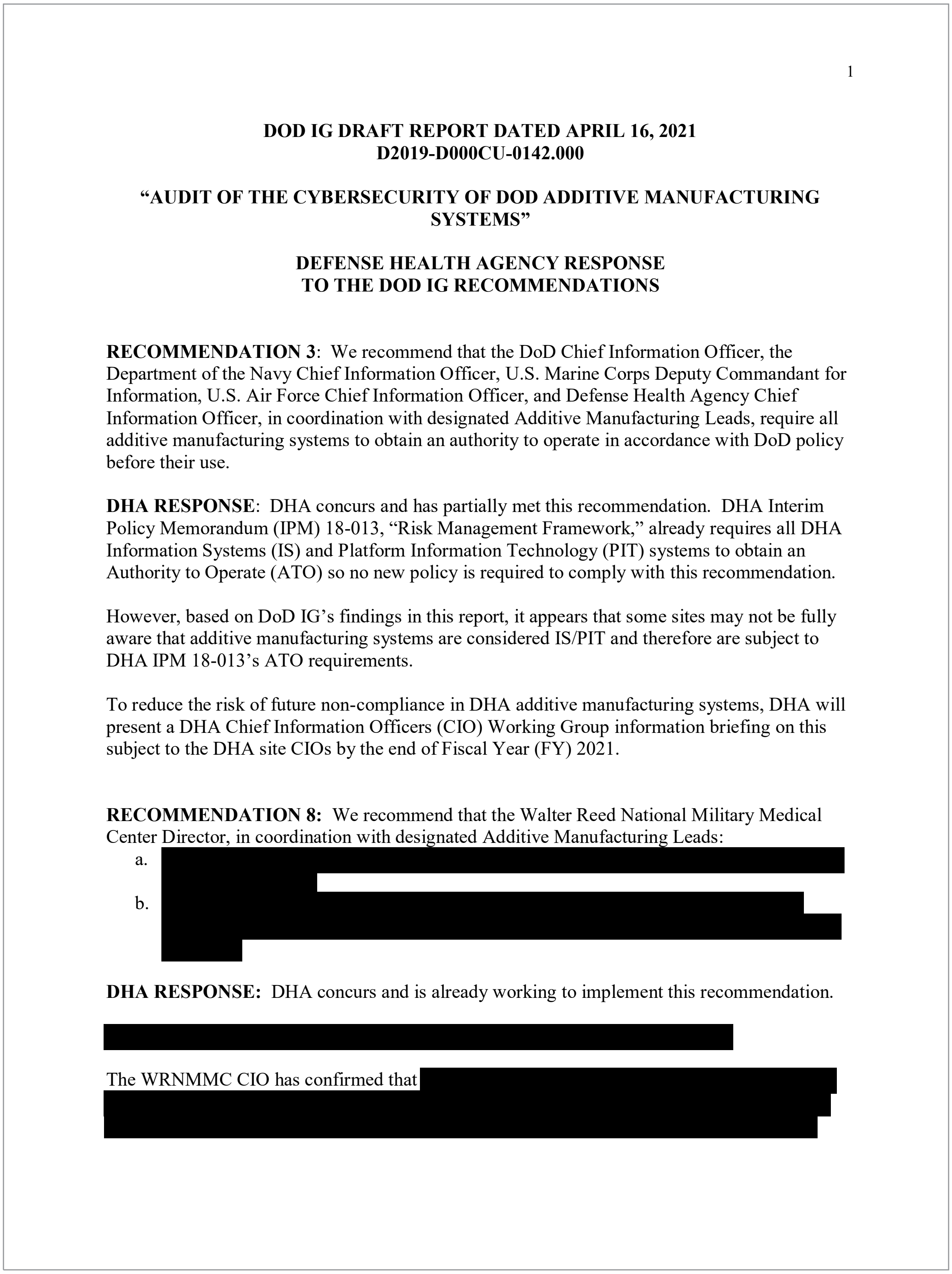
PLACE.RONALD.J
OSEPH.[redacted]
[redacted]

Digitally signed by
PLACE.RONALD.JOSEPH.[redacted]
[redacted]
Date: 2021.05.06 11:39:18 -04'00'

RONALD J. PLACE
LTG, MC, USA
Director

Attachment:
As stated

Defense Health Agency (cont'd)



1

DOD IG DRAFT REPORT DATED APRIL 16, 2021
D2019-D000CU-0142.000

"AUDIT OF THE CYBERSECURITY OF DOD ADDITIVE MANUFACTURING SYSTEMS"

DEFENSE HEALTH AGENCY RESPONSE
TO THE DOD IG RECOMMENDATIONS

RECOMMENDATION 3: We recommend that the DoD Chief Information Officer, the Department of the Navy Chief Information Officer, U.S. Marine Corps Deputy Commandant for Information, U.S. Air Force Chief Information Officer, and Defense Health Agency Chief Information Officer, in coordination with designated Additive Manufacturing Leads, require all additive manufacturing systems to obtain an authority to operate in accordance with DoD policy before their use.

DHA RESPONSE: DHA concurs and has partially met this recommendation. DHA Interim Policy Memorandum (IPM) 18-013, "Risk Management Framework," already requires all DHA Information Systems (IS) and Platform Information Technology (PIT) systems to obtain an Authority to Operate (ATO) so no new policy is required to comply with this recommendation.

However, based on DoD IG's findings in this report, it appears that some sites may not be fully aware that additive manufacturing systems are considered IS/PIT and therefore are subject to DHA IPM 18-013's ATO requirements.

To reduce the risk of future non-compliance in DHA additive manufacturing systems, DHA will present a DHA Chief Information Officers (CIO) Working Group information briefing on this subject to the DHA site CIOs by the end of Fiscal Year (FY) 2021.

RECOMMENDATION 8: We recommend that the Walter Reed National Military Medical Center Director, in coordination with designated Additive Manufacturing Leads:

a. [redacted]

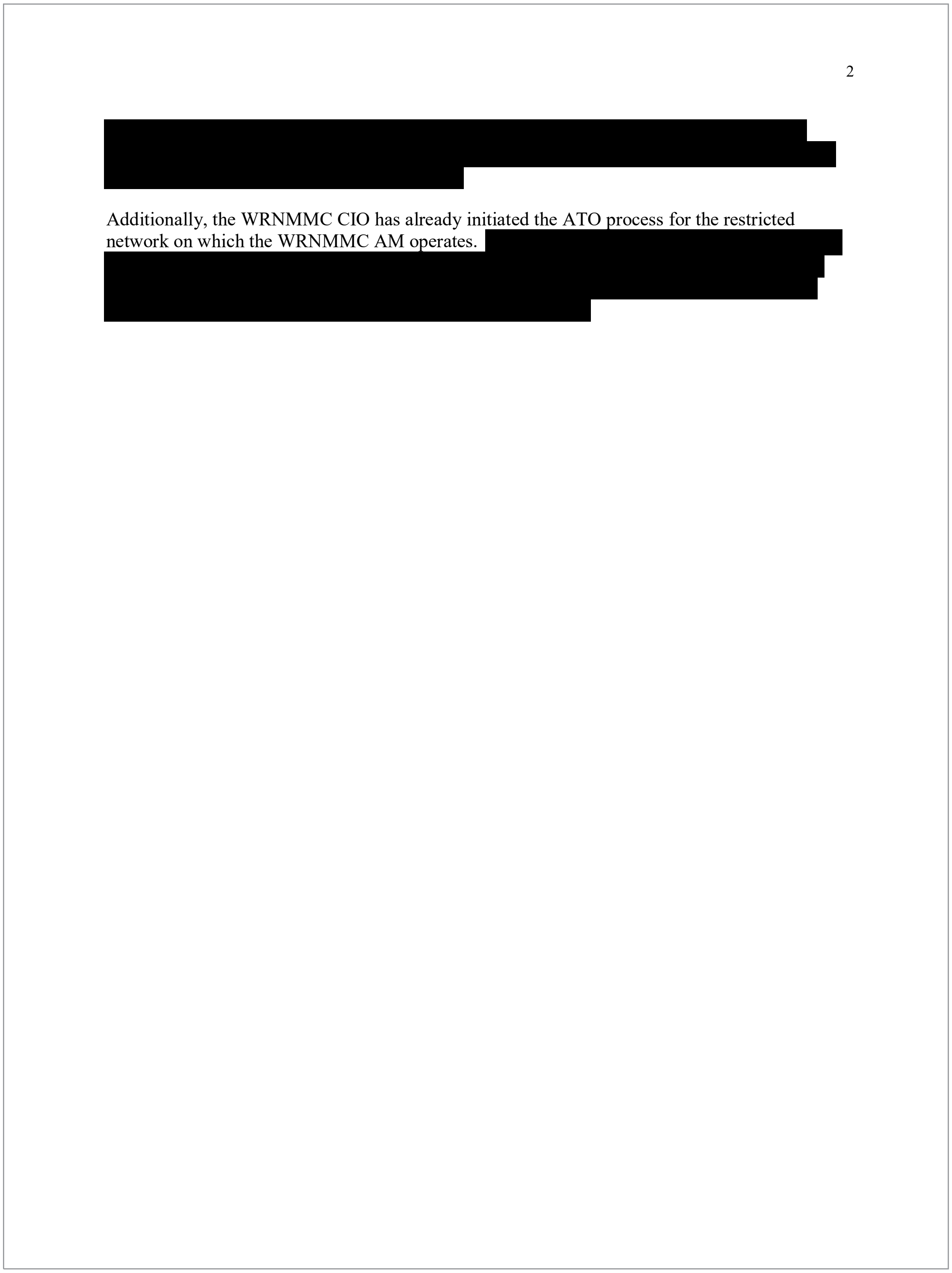
b. [redacted]

DHA RESPONSE: DHA concurs and is already working to implement this recommendation.

[redacted]

The WRNMMC CIO has confirmed that [redacted]

Defense Health Agency (cont'd)

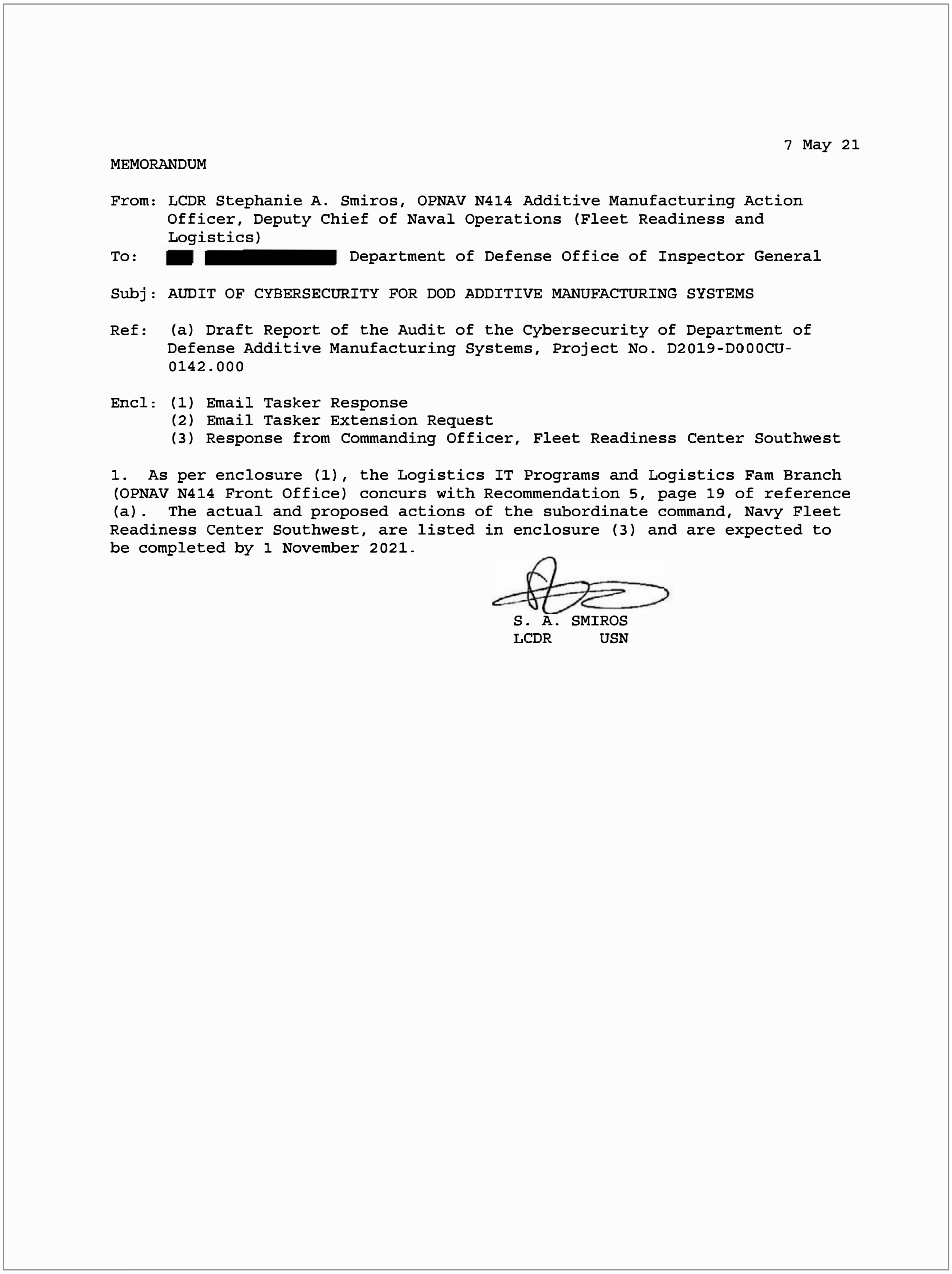


2

[redacted]

Additionally, the WRNMMC CIO has already initiated the ATO process for the restricted network on which the WRNMMC AM operates. [redacted]

Naval Operations for Fleet Readiness and Logistics



7 May 21

MEMORANDUM

From: LCDR Stephanie A. Smiros, OPNAV N414 Additive Manufacturing Action Officer, Deputy Chief of Naval Operations (Fleet Readiness and Logistics)
To: [redacted] [redacted] Department of Defense Office of Inspector General

Subj: AUDIT OF CYBERSECURITY FOR DOD ADDITIVE MANUFACTURING SYSTEMS

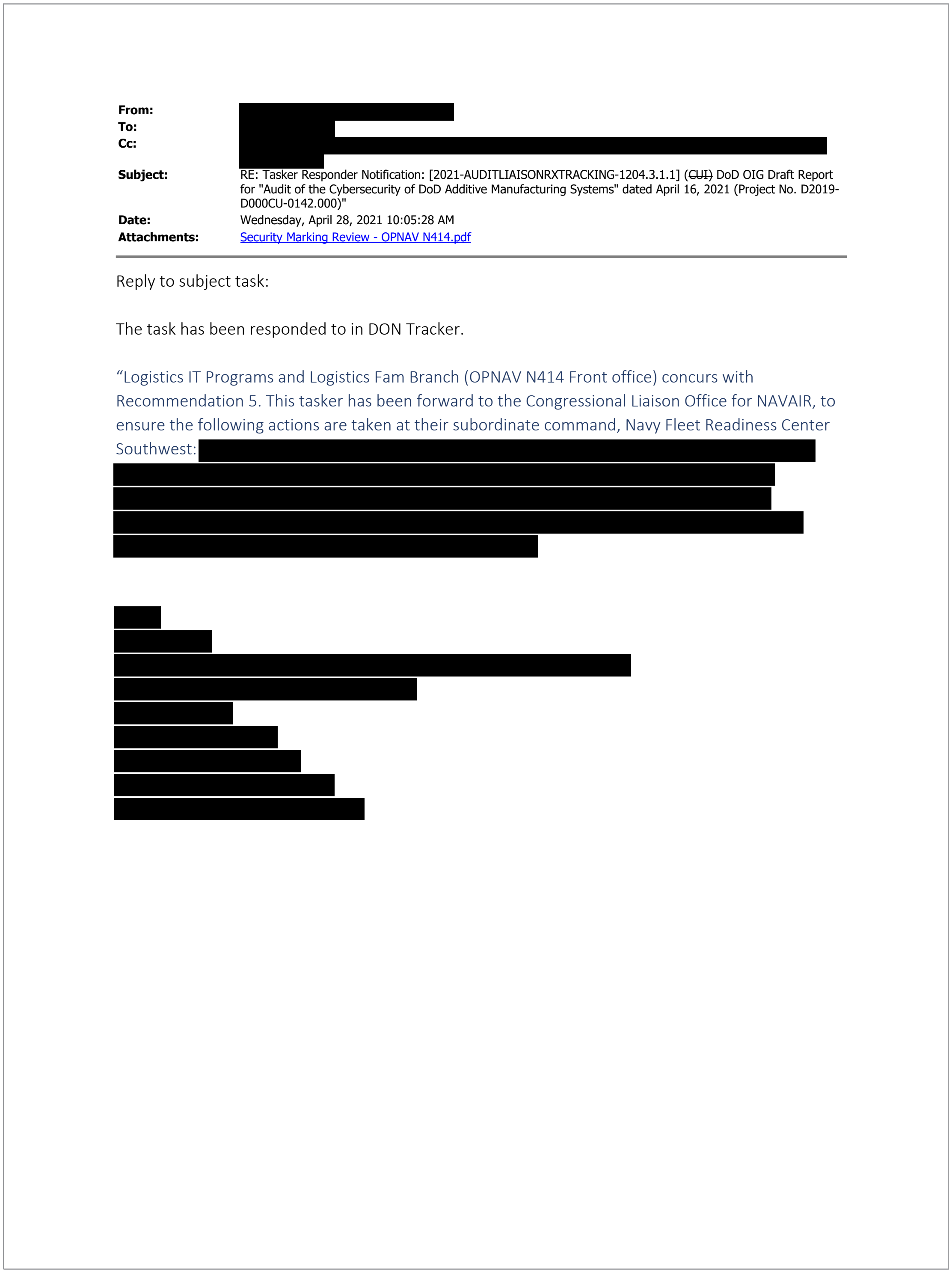
Ref: (a) Draft Report of the Audit of the Cybersecurity of Department of Defense Additive Manufacturing Systems, Project No. D2019-D000CU-0142.000

Encl: (1) Email Tasker Response
(2) Email Tasker Extension Request
(3) Response from Commanding Officer, Fleet Readiness Center Southwest

1. As per enclosure (1), the Logistics IT Programs and Logistics Fam Branch (OPNAV N414 Front Office) concurs with Recommendation 5, page 19 of reference (a). The actual and proposed actions of the subordinate command, Navy Fleet Readiness Center Southwest, are listed in enclosure (3) and are expected to be completed by 1 November 2021.

S. A. SMIROS
LCDR USN

Naval Operations for Fleet Readiness and Logistics (cont'd)



From: [redacted]
To:
Cc:

Subject: RE: Tasker Responder Notification: [2021-AUDITLIAISONRXTRACKING-1204.3.1.1] (~~CUI~~) DoD OIG Draft Report for "Audit of the Cybersecurity of DoD Additive Manufacturing Systems" dated April 16, 2021 (Project No. D2019-D000CU-0142.000)"
Date: Wednesday, April 28, 2021 10:05:28 AM
Attachments: Security Marking Review - OPNAV N414.pdf

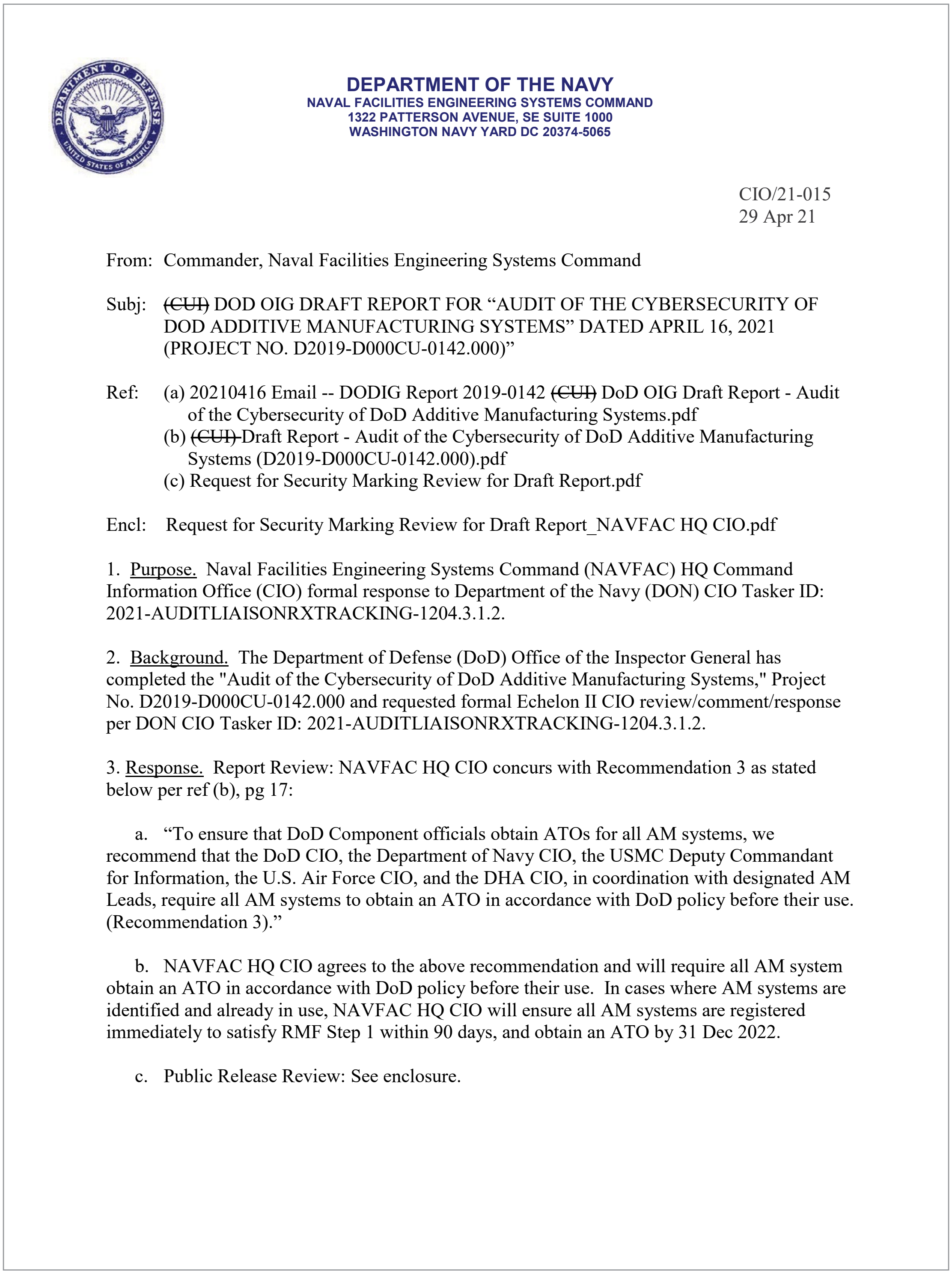
Reply to subject task:

The task has been responded to in DON Tracker.

"Logistics IT Programs and Logistics Fam Branch (OPNAV N414 Front office) concurs with Recommendation 5. This tasker has been forward to the Congressional Liaison Office for NAVAIR, to ensure the following actions are taken at their subordinate command, Navy Fleet Readiness Center Southwest: [redacted]

[redacted]

Naval Facilities Engineering Systems Command



DEPARTMENT OF THE NAVY
NAVAL FACILITIES ENGINEERING SYSTEMS COMMAND
1322 PATTERSON AVENUE, SE SUITE 1000
WASHINGTON NAVY YARD DC 20374-5065

CIO/21-015
29 Apr 21

From: Commander, Naval Facilities Engineering Systems Command

Subj: ~~(CUI)~~ DOD OIG DRAFT REPORT FOR "AUDIT OF THE CYBERSECURITY OF DOD ADDITIVE MANUFACTURING SYSTEMS" DATED APRIL 16, 2021 (PROJECT NO. D2019-D000CU-0142.000)"

Ref: (a) 20210416 Email -- DODIG Report 2019-0142 ~~(CUI)~~ DoD OIG Draft Report - Audit of the Cybersecurity of DoD Additive Manufacturing Systems.pdf
(b) ~~(CUI)~~ Draft Report - Audit of the Cybersecurity of DoD Additive Manufacturing Systems (D2019-D000CU-0142.000).pdf
(c) Request for Security Marking Review for Draft Report.pdf

Encl: Request for Security Marking Review for Draft Report_NAVFAC HQ CIO.pdf

1. Purpose. Naval Facilities Engineering Systems Command (NAVFAC) HQ Command Information Office (CIO) formal response to Department of the Navy (DON) CIO Tasker ID: 2021-AUDITLIAISONRXTRACKING-1204.3.1.2.

2. Background. The Department of Defense (DoD) Office of the Inspector General has completed the "Audit of the Cybersecurity of DoD Additive Manufacturing Systems," Project No. D2019-D000CU-0142.000 and requested formal Echelon II CIO review/comment/response per DON CIO Tasker ID: 2021-AUDITLIAISONRXTRACKING-1204.3.1.2.

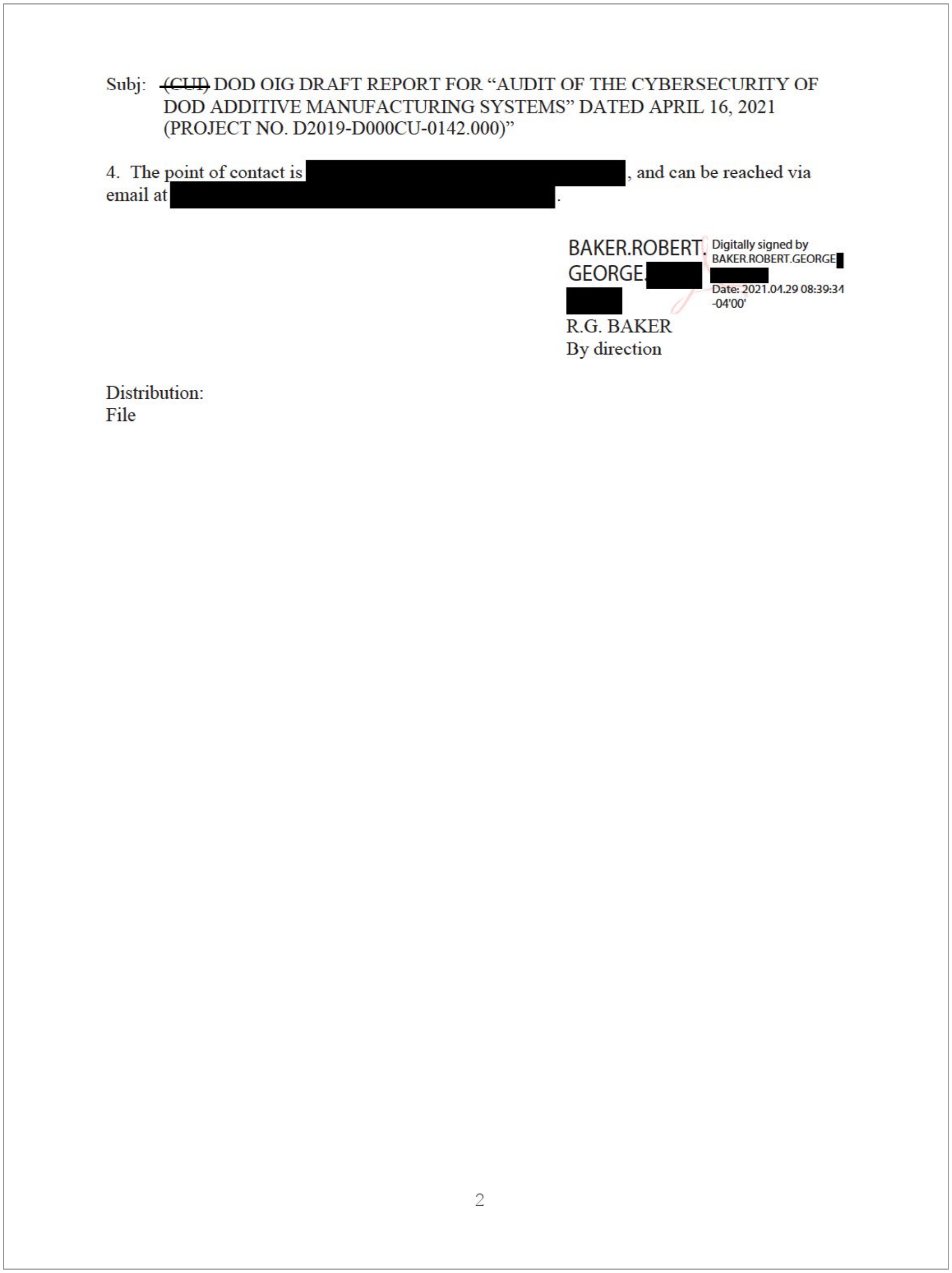
3. Response. Report Review: NAVFAC HQ CIO concurs with Recommendation 3 as stated below per ref (b), pg 17:

a. "To ensure that DoD Component officials obtain ATOs for all AM systems, we recommend that the DoD CIO, the Department of Navy CIO, the USMC Deputy Commandant for Information, the U.S. Air Force CIO, and the DHA CIO, in coordination with designated AM Leads, require all AM systems to obtain an ATO in accordance with DoD policy before their use. (Recommendation 3)."

b. NAVFAC HQ CIO agrees to the above recommendation and will require all AM system obtain an ATO in accordance with DoD policy before their use. In cases where AM systems are identified and already in use, NAVFAC HQ CIO will ensure all AM systems are registered immediately to satisfy RMF Step 1 within 90 days, and obtain an ATO by 31 Dec 2022.

c. Public Release Review: See enclosure.

Naval Facilities Engineering Systems Command (cont'd)



Subj: ~~(CUI)~~ DOD OIG DRAFT REPORT FOR "AUDIT OF THE CYBERSECURITY OF DOD ADDITIVE MANUFACTURING SYSTEMS" DATED APRIL 16, 2021 (PROJECT NO. D2019-D000CU-0142.000)"

4. The point of contact is [redacted], and can be reached via email at [redacted].

BAKER.ROBERT.
GEORGE.[redacted]
[redacted]

Digitally signed by
BAKER.ROBERT.GEORGE[redacted]
[redacted]
Date: 2021.04.29 08:39:34
-04'00'

R.G. BAKER
By direction

Distribution:
File

2

Acronyms and Abbreviations

3-D	Three-Dimensional
AM	Additive Manufacturing
ATO	Authority to Operate
CIO	Chief Information Officer
COVID-19	Coronavirus Disease–2019
DHA	Defense Health Agency
DODIN	DoD Information Network
GAO	Government Accountability Office
FRC-SW	Fleet Readiness Center Southwest
ISSM	Information System Security Manager
MEF	Marine Expeditionary Force
MXG	Maintenance Group
NAVFAC	Naval Facilities Engineering Systems Command
NIST	National Institute of Standards and Technology
NIWC-P	Naval Information Warfare Center Pacific
RMF	Risk Management Framework
SP	Special Publication
USD(A&S)	Undersecretary of Defense for Acquisition and Sustainment
USD(R&E)	Undersecretary of Defense for Research and Engineering
WRNMMC	Walter Reed National Military Medical Center

Glossary

Additive Manufacturing (AM). Process of creating an object by adding layers of material (plastics, metals, and ceramics) from 3-D data. AM is commonly known as 3-D printing and consists of the following seven processes: binder jetting, sheet lamination, powder bed infusion, material jetting, material extrusion, directed energy deposition, and vat photo polymerization.

AM Systems. For purposes of this report, AM systems refer to AM printers and computer workstations used to control the printers and to develop 3-D products.

Authentication. The process of verifying the identity of a user to a system by using authentication factors, such as a user name and password.

Computer Aided Design. A computer tool used for the development of design-drawings and documentation for manufacturing. Computer aided design software assists in developing parts through the 3-D printing process by eliminating hours of manual drawing.

Common Access Card. The standard identification/smart card issued by the DoD that has an embedded integrated chip storing public key infrastructure PKI certificates and, which serves as the Federal personal identity verification card for DoD implementation of Homeland Security Presidential Directive 12.

Department of Defense Information Network (DODIN). The globally interconnected, set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, including computing systems and services, software, data, security services, other associated services, and national security systems.

Logical Access Controls. The policies, procedures, organizational structure, and electronic access controls designed to restrict access to computer software and data files.

Operating System. An example of an all-inclusive configuration management solution through which service patches are often installed.

Public Key Infrastructure. A series of policies, processes, and technologies used to associate certificates and public key pairs with the entity to whom keys were issued.

Removable Media. Are portable devices such as compact discs or external hard drives that connect to information systems or networks to store and transfer data.

Risk Management Framework (RMF). A structured approach used to oversee and manage risk for an enterprise.

Slicing. With respect to AM, slicing is the process of converting a 3-D model into a series of instructions for the printer to carry out.

Stand-alone Computer. Computer that is not connected to any other network and does not transmit, receive, route, or exchange information outside of the system's authorization boundary.

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