

**~~FOR OFFICIAL USE ONLY~~**

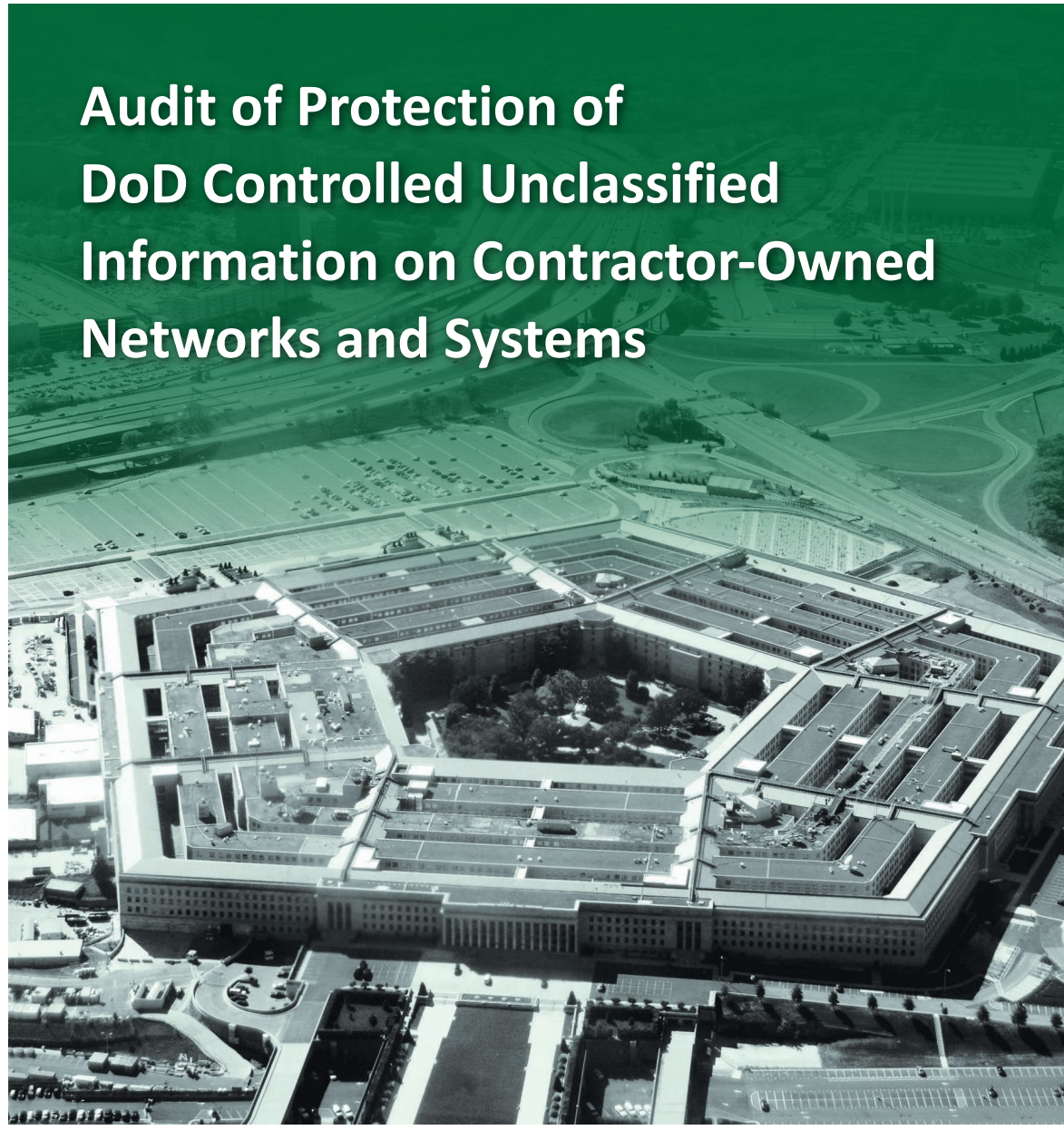
# INSPECTOR GENERAL

*U.S. Department of Defense*

JULY 23, 2019



## Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems



INTEGRITY ★ INDEPENDENCE ★ EXCELLENCE

The document contains information that may be exempt from  
mandatory disclosure under the Freedom of Information Act.

**~~FOR OFFICIAL USE ONLY~~**







# Results in Brief

## *Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems*

July 23, 2019

### Objective

We determined whether DoD contractors implemented adequate security controls to protect DoD-controlled unclassified information (CUI) maintained on their networks and systems from internal and external cyber threats. CUI is a designation for identifying unclassified information that requires proper safeguarding in accordance with Federal and DoD guidance.

We conducted this audit in response to a request from the Secretary of Defense that the DoD Office of Inspector General conduct a DoD-wide audit to determine whether contractors were protecting CUI on their networks and systems.

We selected a nonstatistical sample of 26 of 12,075 contractors with DoD contracts worth \$1 million or more. Of the 26 contractors selected, we assessed 9 contractors to evaluate the security controls that were implemented to protect DoD CUI. We did not assess 17 of the 26 contractors because either the contract had expired, the contractors did not have contracts containing CUI, or the contractors maintained CUI on government-furnished networks and systems and not on their own. We also assessed one contractor, not included in the nonstatistical sample, that we assessed in DODIG-2018-094, "Logical and Physical Access Controls at Missile Defense Agency Contractor Locations," March 29, 2018, to follow up on actions taken to address weaknesses we identified in that report.<sup>1</sup>

<sup>1</sup> We identify the 10 contractors we assessed as Contractors A through J to ensure that the contractors and their proprietary information are not identified.

### Background

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

From March 2015 through June 2018, 126 contractors reported 248 security incidents to the DoD Cyber Crime Center, which is the executive agency of the Secretary of the Air Force that is responsible for, among other responsibilities, tracking security incidents reported by DoD contractors. Security incidents reported to the DoD Cyber Crime Center between 2015 and 2018 included unauthorized access to contractors' networks by malicious actors; stolen equipment, such as laptops and cellular phones; inadvertent disclosure of information; data exfiltration; and the exploitation of network and system vulnerabilities by malicious actors.

### Findings

DoD contractors did not consistently implement DoD-mandated system security controls for safeguarding Defense information. We identified deficiencies at the nine contractors we assessed related to:

- using multifactor authentication;
- enforcing the use of strong passwords;
- identifying network and system vulnerabilities;
- mitigating network and system vulnerabilities;
- protecting CUI stored on removable media;
- overseeing network and boundary protection services provided by a third-party company;



# Results in Brief

## *Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems*

### *Findings (cont'd)*

- documenting and tracking cybersecurity incidents;
- configuring user accounts to lock automatically after extended periods and unsuccessful login attempts;
- implementing physical security controls;
- creating and reviewing system activity reports; and
- granting system access based on the user's assigned duties.

The DoD requires contractors to protect CUI by complying with National Institute of Standards and Technology requirements. However, we determined that DoD Component contracting offices and requiring activities did not establish processes to:

- verify that contractors' networks and systems met National Institute of Standards and Technology security requirements before contract award;
- notify contractors of the specific CUI category related to the contract requirements;
- determine whether contractors access, maintain, or develop CUI to meet contractual requirements;
- mark documents that contained CUI and notify contractors when CUI was exchanged between DoD agencies and the contractor; and
- verify that contractors implemented minimum security controls for protecting CUI.

Furthermore, DoD Component contracting offices and requiring activities did not always know which contracts required contractors to maintain CUI because the DoD did not implement processes and procedures to track which contractors maintain CUI. In addition, the contracting offices inconsistently tracked which contractors maintain CUI on their networks and systems.

As a result, the DoD does not know the amount of DoD information managed by contractors and cannot determine whether contractors are protecting unclassified DoD information from unauthorized disclosure. Without knowing which contractors maintain CUI on their networks and systems and taking actions to validate that contractors protect and secure DoD information, the DoD is at greater risk of its CUI being compromised by cyberattacks from malicious actors who will target DoD contractors. Malicious actors can exploit vulnerabilities on the networks and systems of DoD contractors and steal information related to some of the Nation's most valuable advanced defense technologies. Cyberattacks against DoD contractors' networks and systems require implementation of system security controls that reduce the vulnerabilities that malicious actors use to compromise DoD critical national security information.

In addition, a DoD Component contracting office and the contractor did not take appropriate action to address a spillage of classified information to unclassified cloud, internal contractor network, and webmail environments. Although the DoD requires contractors to protect classified information, neither the Defense Threat Reduction Agency nor the contractor took prompt action to report and address the spillage of classified DoD information to unclassified environments. As a result, classified information remained unprotected on the commercial cloud and the webmail server for almost 2 years. A compromise of classified information presents a threat to national security and may damage intelligence or operational capabilities; lessen the DoD ability to protect critical information, technologies, and programs; or reduce the effectiveness of DoD management.





# Results in Brief

## *Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems*

### Recommendations

(FOUO) We recommend that the Director for Contract Policy and Oversight for the Defense Threat Reduction Agency revise the agency's process for monitoring security incidents, [REDACTED], to verify that contractors took appropriate steps to identify, respond to, and report security incidents that involve DoD data. We also recommend that the Director review the performance of the contracting officer responsible for monitoring the security incident identified in this report and consider administrative action, as appropriate, for not ensuring that a contractor took actions to remove the classified information from its corporate network and the contractor's commercial cloud environment. Furthermore, we recommend that the Director for the Defense Counterintelligence and Security Agency (formerly known as the Defense Security Service) assess and document the risk of leaving classified information unprotected in unclassified environments and, based on the assessment, develop and implement controls to protect the information.

We recommend that the DoD Chief Information Officer direct DoD Component contracting offices and requiring activities to require contractors to use strong passwords that are, at a minimum, 15 characters, and configure their networks and systems to align with DoD requirements for locking accounts after 15 minutes of inactivity and three unsuccessful logon attempts.

In addition, we recommend that the Principal Director for Defense Pricing and Contracting:

- Revise its current policy related to assessing a contractor's ability to protect DoD information to require DoD Component contracting offices, as part of the Request for Proposal and source selection processes, and requiring activities,

during the contract performance, to validate, at least annually, that contractors comply with security requirements for protecting CUI before contract award and throughout the contract's period of performance.

- Develop and implement policy requiring DoD Component contracting offices and requiring activities to maintain an accurate accounting of contractors that access, maintain, or develop controlled unclassified information as part of their contractual obligations.
- Revise its current policy to include language that would require DoD Component contracting offices to validate contractor compliance with minimum security requirements.

We also recommend that the DoD Component contracting offices, in coordination with requiring activities, implement a plan to verify that the internal control weaknesses for the contractors discussed in this report are addressed.

### Management Comments and Our Response

The Principal Deputy Chief Information Officer, responding for the DoD Chief Information Officer, disagreed with the recommendations to require stronger passwords and lock accounts after 15 minutes of inactivity stating that those requirements were prohibited by 32 Code of Federal Regulation section 2002, "Controlled Unclassified Information" and contrary to Executive Order 13556, "Controlled Unclassified Information."<sup>2</sup> However, we do not consider the 32 CFR section 2002 and

<sup>2</sup> 32 Code of Federal Regulation 2002, "Controlled Unclassified Information," September 14, 2016. Executive Order 13556, "Controlled Unclassified Information," November 4, 2010.



# Results in Brief

## *Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems*

### **Management Comments (cont'd)**

Executive Order 13556 prohibitive in allowing the DoD to require contractors to implement more stringent requirements, when warranted. Therefore, the DoD Chief Information Officer should provide additional comments to clarify how the recommendations conflict with or are contrary to 32 Code of Federal Regulation section 2002 and the Executive Order 13556, or how the DoD Chief Information Officer will implement the recommendations as stated.

The U.S. Transportation Command Chief of Staff; U.S. Cyber Command Chief of Staff; Missile Defense Agency Director; and Defense Pricing and Contracting Acting Principal Director agreed to implement a plan to verify that the internal control weaknesses for the contractors discussed in this report are corrected. In addition, the Defense Threat Reduction Agency Director agreed to revise its process for monitoring security incidents. The Director also stated that he reviewed the performance of the contracting officer responsible for monitoring a 2016 security incident and found no reason to take administrative action.

The Operational Test and Evaluation Principal Deputy Director agreed to use multifactor authentication, mitigate vulnerabilities, implement physical security controls, generate system activity reports, and require written justification for obtaining system access. In addition, Contractor G took action to reduce the lockout period from 60 minutes to 30 minutes. However, planned actions by the contractor related to removable media will not ensure that all CUI stored on removable media is encrypted. Therefore, the Principal Deputy Director should provide additional comments describing how the Director of Operational Test and Evaluation plans to verify that the contractor's actions are sufficient to ensure that staff encrypts CUI stored on removable media.

(FOUO) Although the Defense Counterintelligence and Security Agency Executive Director agreed to include aspects of the recommendation in future incident responses and decisions, he did not state how the agency planned to [REDACTED].

Therefore, the Executive Director should provide additional comments describing how the Defense Counterintelligence and Security Agency plans to assess that risk.

Although the Defense Contract Management Agency Director stated that the agency would verify contractor compliance with DFARS clause 252.204-7012, he did not state how the agency would verify that the contractor corrected the weaknesses identified in this report. Therefore, the Director should provide additional comments describing how the Defense Contract Management Agency will verify that the contractor corrected weaknesses related to using multifactor authentication; mitigating vulnerabilities in a timely manner; and protecting and monitoring data on removable media.

The Deputy Assistant Secretary of the Army (Procurement) stated she would implement a plan to verify that the internal control weaknesses for the contractors discussed in this report are addressed. However, she did not state how the U.S. Army Corps of Engineers would verify that the contractor corrected identified weaknesses. Therefore, the Deputy Assistant Secretary should provide additional comments describing how the Corps of Engineers will verify that the contractor corrected the weaknesses.

The Deputy Assistant Secretary for the Navy (Research, Development, Test, and Evaluation), responding for the U.S. Navy Contracting Officer, acknowledged that the Navy was working with the Office of the Secretary of Defense to develop policy for ensuring contractor





# Results in Brief

## *Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems*

### **Management Comments (cont'd)**

compliance with DFARS clause 252.204-7012. However, he did not address actions that the Naval Information Warfare Systems Command (formerly known as the Space and Naval Warfare Center) will take to ensure the contractor corrected identified weaknesses. Therefore, the Deputy Assistant Secretary should provide additional comments describing how the Naval Information Warfare Systems Command will verify that the contractor corrected those weaknesses.

The Principal Deputy Assistant Secretary of the Air Force (Acquisition, Technology, and Logistics), responding for the U.S. Air Force Contracting Officer, neither agreed nor disagreed with the recommendations

and did not address actions that the Air Force will take to ensure the contractor corrected identified weaknesses. Therefore, the Principal Deputy Assistant Secretary should provide additional comments describing how the Air Force will verify that the contractor corrected those weaknesses.

The Contracting Officer, Defense Microelectronics Activity, did not respond to the recommendations in the report and therefore, we request that the Contracting Officer provide comments on the final report.

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

## Recommendations Table

Management	Recommendations Unresolved	Recommendations Resolved	Recommendations Closed
Deputy Assistant Secretary of the Army (Procurement)	A.3.a, A.3.b, A.3.c, A.3.e, A.3.f, A.3.g, A.3.h		
The Deputy Assistant Secretary for the Navy (Research, Development, Test, and Evaluation)	A.3.a, A.3.b, A.3.f, A.3.g, A.3.h		
Principal Deputy Assistant Secretary of the Air Force (Acquisition, Technology, and Logistics)	A.3.a, A.3.b, A.3.c		
Chief of Staff, U.S. Transportation Command		A.3.a, A.3.b, A.3.c	
Contracting Officer, U.S. Cyber Command			A.3.b, A.3.e
Department of Defense, Chief Information Officer	A.1.a, A.1.b		
Principal Deputy Director, Office of the Director of Operational Test and Evaluation	A.3.c	A.3.b, A.3.d, A.3.e	
Director, Contract Policy and Oversight, Defense Threat Reduction Agency		B.1.a	B.1.b
Director, Defense Counterintelligence and Security Agency	B.2		
Director, Missile Defense Agency		A.3.a, A.3.b, A.3.c, A.3.e, A.3.g, A.3.h A.4.b, A.4.c	A.4.a
Director, Defense Contract Management Agency	A.3.a, A.3.b, A.3.c		
Principal Director, Defense Pricing and Contracting		A.2.a, A.2.b, A.2.c, A.2.d, A.2.e	
Contracting Officer, Defense Microelectronics Activity	A.3.a, A.3.b, A.3.c		

Please provide Management Comments by August 23, 2019.

**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 23, 2019

**MEMORANDUM FOR DISTRIBUTION**

**SUBJECT: Audit of Protection of DoD Controlled Unclassified Information on  
Contractor-Owned Networks and Systems (Report No. DODIG-2019-105)**

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 when preparing the final report. Those comments are included in the report.

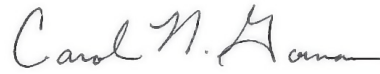
This report contains 25 recommendations that are considered unresolved because management officials did not provide written comments to the draft report or did not fully address the recommendations. Therefore, as discussed in the Recommendations, Management Comments, and Our Response sections of this report, the recommendations will remain unresolved until an agreement is reached on the actions to be taken to address the recommendations. Once an agreement is reached, the recommendations will be considered resolved but will remain open until adequate documentation has been submitted showing that the agreed-upon action has been completed. Once we verify that the action is complete, the recommendations will be closed.

This report contains 20 recommendations that are considered resolved. Therefore, as discussed in the Recommendations, Management Comments, and Our Response sections of this report, the recommendations will remain open until adequate documentation has been submitted showing that the agreed-upon action has been completed. Once we verify that the action is complete, the recommendations will be closed.

This report contains four recommendations that are considered closed as discussed in the Recommendations, Management Comments, and Our Response sections of this report. Those recommendations do not require further comments.

DoD Instruction 7650.03 requires that recommendations be resolved promptly. For the unresolved recommendations, please provide us within 30 days your response concerning specific actions in process or alternative corrective actions proposed on the recommendations. For the resolved recommendations, please provide us within 90 days documentation showing that the agreed-upon action has been completed. Your response should be sent as a PDF file to either [audcso@dodig.mil](mailto:audcso@dodig.mil) if unclassified or [anissa.nash@dodig.smil.mil](mailto:anissa.nash@dodig.smil.mil) 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. Please direct questions to me at (703) 699-7331 (DSN 499-7331).

A handwritten signature in black ink, appearing to read "Carol N. Gorman". The signature is fluid and cursive, with the first name "Carol" being the most prominent.

Carol N. Gorman  
Assistant Inspector General for Audit  
Cyberspace Operations



***Distribution:***

DEPARTMENT OF DEFENSE, CHIEF INFORMATION OFFICER  
PRINCIPAL DIRECTOR, DEFENSE PRICING AND CONTRACTING  
COMMANDER, U.S. CYBER COMMAND  
COMMANDER, U.S. TRANSPORTATION COMMAND  
DIRECTOR, OPERATIONAL TEST AND EVALUATION  
DIRECTOR, DEFENSE THREAT REDUCTION AGENCY  
DIRECTOR, MISSILE DEFENSE AGENCY  
DIRECTOR, DEFENSE CONTRACT MANAGEMENT AGENCY  
DIRECTOR, DEFENSE MICROELECTRONICS ACTIVITY  
NAVAL INSPECTOR GENERAL  
AUDITOR GENERAL, DEPARTMENT OF THE ARMY  
AUDITOR GENERAL, DEPARTMENT OF THE AIR FORCE

## Contents

---

### Introduction

Objective .....	1
Background .....	2
Review of Internal Controls .....	4

### Finding A. Contractor Security Controls for Networks and Systems Containing CUI Were Not Consistently Implemented .....

5

Contractors Did Not Implement Security Controls to Protect CUI .....	6
Neither DoD Component Contracting Offices Nor DoD Requiring Activities Assessed Contractors' Actions for Protecting Information .....	27
Unauthorized Access to or Disclosure of CUI Weakens National Security .....	33
Comments on the Finding and Our Response .....	33
Recommendations, Management Comments, and Our Response .....	36
Management Comments Required .....	50

### (FOUO) Finding B. Contractor C [REDACTED] .....

51

Exposing Classified DoD Information Threatens National Security .....	54
Recommendations, Management Comments, and Our Response .....	54

### Appendixes

Appendix A. Scope and Methodology .....	57
Use of Computer-Processed Data .....	58
Use of Technical Assistance .....	59
Prior Coverage .....	59
Appendix B. Sampling Approach .....	61

Management Comments .....	63
Deputy Assistant Secretary of the Army (Procurement) .....	63
Deputy Assistant Secretary of the Navy (Research, Development, Test, and Evaluation) .....	66



## Contents (cont'd)

---

Assistant Secretary of the Air Force (Acquisition, Technology & Logistics) .....	75
U.S. Transportation Command Chief of Staff .....	78
U.S. Cyber Command Chief of Staff .....	82
Principal Deputy Chief Information Officer .....	83
Office of the Director of Operational Test and Evaluation, Principal Deputy Director .....	85
Defense Threat Reduction Agency Chief Information Officer .....	89
Defense Counterintelligence and Security Agency Executive Director .....	91
Missile Defense Agency Director .....	92
Defense Contract Management Agency Director .....	97
Defense Pricing and Contracts Acting Principal Director .....	100
<b>Acronyms and Abbreviations</b> .....	103
<b>Glossary</b> .....	104

# Introduction

---

## Objective

The objective of this audit was to determine whether DoD contractors implemented adequate security controls to protect DoD controlled unclassified information (CUI) maintained on their networks and systems from internal and external cyber threats. CUI is a designation for identifying unclassified information that requires proper safeguarding in accordance with Federal and DoD guidance. We initiated the audit in response to a June 8, 2018, request from the Secretary of Defense to conduct an audit of the controls in place to protect CUI managed by DoD contractors.

We selected a nonstatistical sample of 26 of 12,075 contractors with DoD contracts worth \$1 million or more. Of the 26 contractors selected, we assessed 9 contractors to evaluate the security controls that were implemented to protect DoD CUI. We did not assess 17 of the 26 contractors because either the contract had expired, the contractors did not have contracts containing CUI, or the contractors maintained CUI on government-furnished networks and systems and not on their own. We also assessed one contractor, not included in the nonstatistical sample, which we assessed in DODIG-2018-094 to follow up on actions taken to address identified weaknesses.<sup>3</sup> We assessed a total of 10 contractors in this audit.<sup>4</sup> The 9 contractors from the nonstatistical sample have 3,374 contracts across 18 of the 24 DoD contracting agencies in our sample (or across 75 percent of DoD Component contracting offices). Although 1 of the 10 contractors used government-furnished equipment, we identified a security incident that the Government agency did not fully resolve. We will only discuss the security incident for that contractor.

This report contains information that may be considered contractor proprietary data, such as information related to contractor internal operating processes. Public release of contractor proprietary data violates criminal provisions in title 18, section 1905, United States Code.<sup>5</sup> Therefore, we identify the 10 contractors we assessed as Contractors A through J to ensure that the contractors and their associated proprietary information are not identified. See Table 4 in Appendix A for a list of the associated contracting agencies for the 10 contractors. Also see Appendix A for a discussion on the scope and methodology and Appendix B for our detailed sampling approach for selecting and assessing the contractors. See the Glossary for the technical term definitions.

---

<sup>3</sup> DODIG-2018-094, "Logical and Physical Access Controls at Missile Defense Agency Contractor Locations," March 29, 2018.

<sup>4</sup> We identify the 10 contractors we assessed as Contractors A through J to ensure that the contractors and their proprietary information are not identified.

<sup>5</sup> 18 U.S.C § 1905, "Disclosure of Confidential Information Generally," January 7, 2011.

## Background

In November 2010, the President issued Executive Order 13556, “Controlled Unclassified Information,” to address agencies’ inconsistent methods for marking, controlling, and safeguarding privacy, security, proprietary business interest, and law enforcement investigations information.<sup>6</sup> The Executive Order also designated the National Archives and Records Administration as the Executive Agent responsible for overseeing agency compliance with the Order’s requirements. The National Archives and Records Administration developed a public CUI registry that lists CUI categories that require marking and safeguarding. The National Archives and Records Administration lists four CUI categories for Defense-related information: controlled technical information, DoD critical infrastructure security information, Naval nuclear propulsion information, and unclassified controlled nuclear information. The registry also includes guidance for applying appropriate markings on CUI documents. According to DoD Manual 5200.01, Volume 4, “DoD Information Security Program: Controlled Unclassified Information (CUI),” Incorporating Change 1, Effective May 9, 2018, the DoD plans to implement Executive Order 13556 when it updates the manual. Table 1 lists the organizational index grouping for the CUI categories maintained in the registry.

*Table 1. CUI Categories*

CUI Categories		
Critical Infrastructure	Defense	Export Control
Financial	Immigration	Intelligence
International Agreements	Law Enforcement	Legal
Natural and Cultural Resources	North Atlantic Treaty Organization	Nuclear
Patent	Privacy	Procurement and Acquisition
Proprietary Business Information	Provisional	Statistical
Tax	Transportation	

Source: The DoD OIG.

<sup>6</sup> Executive Order 13556, “Controlled Unclassified Information,” November 4, 2010.



## ***Requirements for Protecting CUI Managed By Contractors***

The Defense Pricing and Contracting (DPC) Office, a component within the Office of the Under Secretary of Defense for Acquisition and Sustainment, establishes DoD contracting and procurement policy, including safeguarding DoD information in accordance with Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012.<sup>7</sup> DFARS clause 252.204-7012 requires contractors that maintain CUI to implement security controls specified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, which lists security requirements for safeguarding sensitive information on non-Federal information systems.<sup>8</sup> The requirements include controls related to user authentication, user access, media protection, incident response, vulnerability management, and confidentiality of information.

On May 17, 2018, the Office of the Under Secretary of Defense for Intelligence designated the Defense Counterintelligence and Security Agency (formerly known as the Defense Security Service)(DCSA) as the lead agency for providing oversight of CUI maintained by DoD contractors. The DCSA is responsible for identifying CUI that has the potential to affect national security and overseeing its protection across the DoD's contractors. The DCSA is also responsible for communicating CUI requirements for contractors to all DoD components. The Under Secretary of Defense for Intelligence tasked the DCSA with implementing a plan to oversee CUI protection and requested an initial report on resource restraints, policy required to support CUI oversight authority, and program improvement recommendations by November 2018. On February 7, 2019, a DCSA official stated that the DCSA finalized the report and planned to brief the Under Secretary of Defense for Intelligence but did not indicate when the briefing would occur. As of February 2019, DCSA had not begun conducting oversight activities of DoD contractors that maintain CUI on contractor networks and systems.

In the October 24, 2018, memorandum establishing the Protecting Critical Technology Task Force (Task Force), the Secretary of Defense stated he recognized that American industry loses more than \$600 billion to theft and that the loss of CUI puts the DoD's investments at risk. The Task Force was tasked to address basic problems and broader systemic issues with protecting the DoD's intellectual property and data. According to Task Force officials, as of February 2019,

<sup>7</sup> The Defense Pricing and Contracting Office was formally known as the Defense Pricing/Defense Procurement and Acquisition Policy Office. DFARS Part 252, "Solicitation Provisions and Contract Clauses," Subpart 252.2, "Text of Provisions and Clauses," Clause 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting," October 2016.

<sup>8</sup> NIST SP 800-171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations," Revision 1, December 2016 (updated June 7, 2018).

the Task Force was evaluating how to address Secretary of Defense priorities, which include working with DoD industry partners (commonly known as DoD contractors) to ensure the integrity and security of DoD information.

### ***Security Incidents Reported by DoD Contractors***

Security incidents are acts of violating an explicit or implied security policy, which includes, but is not limited to, attempts to gain unauthorized access to systems; disruption or denial of service; and unauthorized changes to system configurations. Contractors are required to report security incidents for contracts that contain CUI to the DoD Cyber Crime Center, which is the executive agency of the Secretary of the Air Force that is responsible for, among other responsibilities, tracking security incidents reported by DoD contractors. From March 2015 through June 2018, 126 contractors reported 248 security incidents to the DoD Cyber Crime Center. The reported security incidents included unauthorized access to contractors' networks by malicious actors; stolen equipment, such as laptops and cellular phones; inadvertent disclosure of information; data exfiltration; and the exploitation of vulnerabilities. Of the 48 security incidents reported, 12 involved the disclosure of personally identifiable information, which the National Archives and Records Administration includes in the Privacy CUI category (see the next section for details on CUI categories). In addition, contractors reported that 24 security incidents potentially involved the disclosure of privacy information, but they could not determine whether privacy information was involved for 84 other security incidents.

### **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.<sup>9</sup> We identified internal control weaknesses related to contractors implementing physical and cybersecurity controls to protect networks and systems that contain DoD CUI. Specifically, DoD Component contracting offices and requiring activities did not implement processes to verify that contractors complied with Federal and DoD requirements for protecting CUI maintained in non-Federal systems and organizations. We will provide a copy of the report to the senior officials responsible for internal controls in the Army, Air Force, U.S. Transportation Command (USTRANSCOM), U.S. Cyber Command, Department of the Navy, Director of Operational Test and Evaluation (DOT&E), Defense Contract Management Agency, Defense Microelectronics Activity, Defense Threat Reduction Agency (DTRA), and the Missile Defense Agency (MDA).

---

<sup>9</sup> DoD Instruction 5010.40, "Managers' Internal Control Program Procedures," May 30, 2013.

## Finding A

### Contractor Security Controls for Networks and Systems Containing CUI Were Not Consistently Implemented

DoD contractors did not consistently implement security controls in accordance with Federal and DoD requirements for safeguarding Defense CUI. Specifically, of the 10 contractors that we assessed:

- seven contractors did not enforce the use of multifactor authentication to access their networks and systems;
- seven contractors did not configure their systems to enforce the use of strong passwords;
- two contractors did not identify network and system vulnerabilities;
- six contractors did not mitigate network and system vulnerabilities in a timely manner;
- six contractors did not protect CUI stored on removable media by using technical and nontechnical safeguards to restrict the use of removable media;
- one contractor did not oversee network and boundary protection services provided by a third-party company;
- one contractor did not document and track cybersecurity incidents;
- eight contractors configured user sessions to lock after extended periods and did not limit unsuccessful logon attempts to reduce the risk of malicious activities;
- two contractors did not implement physical security controls, such as installing internal surveillance cameras, maintaining visitor logs, and securing servers, at their facilities that maintain CUI;
- three contractors did not configure their networks and systems to generate system activity reports nor did they review the networks and systems for malicious or unusual activity; and
- three contractors did not grant system access based on the user's assigned duties and apply the principle of least privilege when granting access.

Although the DoD requires contractors to protect CUI by complying with NIST SP 800-171 requirements, DoD Component contracting offices and requiring activities did not establish processes to:

- verify that contract offerors' networks and systems that process, store, and transmit CUI met the NIST security requirements before contract award;

- notify contractors of the specific CUI category related to the contract requirements;
- determine whether contractors accessed, maintained, or developed CUI to meet contractual requirements;
- properly mark documents that contained CUI; and
- verify that contractors implemented minimum security controls required by NIST SP 800-171.<sup>10</sup>

Furthermore, DoD Component contracting offices and requiring activities did not always know which contracts required contractors to maintain CUI because the DoD did not have controls in place to track which contractors maintain CUI, and the contracting offices inconsistently tracked which contracts include DFARS clause 252.204-7012. As a result, the DoD does not know the amount of DoD CUI managed by contractors and does not have accurate information to determine whether contractors are protecting CUI from unauthorized access and disclosure. Without knowing which contractors maintain CUI on their networks and systems and taking actions to validate that contractors protect and secure DoD information, the DoD is at greater risk of its CUI being compromised by cyberattacks from malicious actors who will target DoD contractors. Malicious actors can exploit vulnerabilities on the networks and systems of DoD contractors and steal information related to some of the Nation's most valuable advanced defense technologies. Cyberattacks against DoD contractors' networks and systems require implementation of system security controls that reduce the vulnerabilities that malicious actors use to compromise DoD critical national security information.

## **Contractors Did Not Implement Security Controls to Protect CUI**

DoD contractor controls and processes for networks and systems that process, store, and transmit CUI were insufficient to protect against potential unauthorized access to, or disclosure of, CUI. To determine whether contractors protected CUI, we assessed cybersecurity controls, processes, and technology used for managing network and system authentication; vulnerabilities; and stored and transmitted data. In addition, we assessed physical security controls, such as facility access. Based on our analyses and testing, we identified security weaknesses at 10 contractors. Table 2 identifies the security weaknesses identified, by contractor.

<sup>10</sup> Requiring activities are DoD Components that identify required contracted services to accomplish their mission. For this audit, "effectively" means the implemented security controls operated as intended by the Federal and DoD policies cited in this report. In addition, "verify" means to determine whether the NIST SP 800-171 security requirements implemented by contractors are appropriate and operate as intended.

Table 2. Security Weaknesses Identified at Contractors Visited

Control Deficiencies	Contractor									
	A	B	C	D	E	F	G	H	I	J
Multifactor authentication was not consistently used		X		X	X	X		X	X	X
Password lengths were susceptible to password attacks		X		X	X	X		X	X	X
Contractors did not always mitigate the vulnerabilities on their networks and systems	X	X		X	X	X	X	X		X
CUI on removable media was not protected				X	X	X	X	X		X
Oversight of third-party service provider's network protection activities was not provided								X		
Cybersecurity incidents were not documented and tracked							X			
Systems lockouts after inactivity or unsuccessful logon attempts were insufficient to prevent unauthorized access	X			X			X	X		
Physical security controls were not used to detect unauthorized access		X		X						
System activity reports were not properly generated and reviewed		X		X				X		
Administrators did not consistently assign user access and privileges that aligned with user responsibilities		X		X				X		

Note: Grayed boxes indicate areas that were not assessed. Contractor C self-identified a security incident and we discuss only that incident in Finding B of this report.

Source: The DoD OIG.



## **Multifactor Authentication Was Not Used**

*Contractors B, E, F, G, H, I, and J did not implement multifactor authentication on all workstations.*

Contractors A and D did not use multifactor authentication to access their networks that contained CUI. In addition, Contractors B, E, F, G, H, I, and J did not implement multifactor

authentication on all workstations. Authentication is a process that verifies the identity of a user and is a prerequisite to allowing access to an information system. Multifactor authentication requires using something in a user's possession, such as a token, in combination with something known only to the user, such as a personal identification number.<sup>11</sup> DFARS clause 252.204-7012 was included in the contracts for Contractors A, B, D, E, F, G, H, I, and J. The clause requires the implementation of NIST SP 800-171, which requires contractors to use multifactor authentication to access unclassified networks that maintain CUI.

Initially, Contractor A did not configure its network to support multifactor authentication. However, during the audit, Contractor A configured its network to support multifactor authentication and required its employees to use a token and personal identification number to access the network. Contractor A provided a screenshot of configuration settings that shows that the contractor locked user accounts if users did not activate multifactor authentication on workstations.

Contractor D required personnel to use only single-factor authentication, such as a username and password, to access its network. Single-factor authentication is less stringent and presents a greater risk of malicious actors compromising networks and systems. Contractor D's system administrator stated that, although the contract contained DFARS clause 252.204-7012 requiring the implementation of NIST SP 800-171, implementing multifactor authentication resulted in financial hardship for small businesses. The system administrator believed that using multifactor authentication was not standard for small businesses. However, the system administrator stated that Contractor D would implement multifactor authentication by June 2019.

(FOUO) Contractors B, F, and J [REDACTED]  
[REDACTED]  
[REDACTED]. Users who connected to Contractor B's and F's networks [REDACTED]  
[REDACTED]. A Contractor B official stated that, [REDACTED]

<sup>11</sup> Multifactor authentication uses two or more factors to achieve authentication by using something you know (password or personal identification number), something you have (cryptographic identification device), or something you are (biometric). A token authenticates a user's identity.

(FOUO) [REDACTED]. The official stated that Contractor B needed to [REDACTED]. Users at Contractor F accessed its network [REDACTED] because Contractor F configured its workstations to automatically authenticate users when they [REDACTED]. The official at Contractor F stated that his company implemented strong physical security controls to gain access to its facility; therefore, Contractor F did not consider multifactor authentication necessary for accessing its network. However, in January 2019, Contractor F officials stated that they were conducting a study with a small group of employees to determine the impact of deploying multifactor authentication across the company. Contractor J required [REDACTED] to use multifactor authentication; users who connected to Contractor J's network [REDACTED]. According to the Chief Information Security Officer, Contractor J planned to enforce the use of multifactor authentication for all users [REDACTED].

(FOUO) Contractors E and G did not [REDACTED]. According to the principal information security analyst at Contractor E, [REDACTED]. The Contractor E official stated that Contractor E planned to [REDACTED]. However, [REDACTED]. During the audit, Contractor G was modifying its network to support multifactor authentication. On November 8, 2018, we verified that Contractor G had fully enforced the use of multifactor authentication to access its network.

Additionally, we followed up on two contractors, Contractors H and I, for which we had previously reported weaknesses related to using multifactor authentication in report DODIG-2018-094.<sup>12</sup> In May 2017, we reported that Contractor H used only single-factor authentication to access its network that contained CUI. In November 2018, we determined that Contractor H still had not fully implemented multifactor authentication. A Contractor H official stated that

<sup>12</sup> Contractor H was identified in report DODIG-2018-094 as Contractor D while Contractor I was identified in that report as Contractor E. In addition, our sample listed Defense Microelectronics Activity as the contracting agency for Contractor I for this audit. However, since we identified issues with Contractor I in DODIG 2018-094, we followed up on the status of identified issues.

Contractor H had not fully implemented multifactor authentication across its entire network because network administrators needed to manually configure each of the company's 200 workstations to use multifactor authentication instead of remotely configuring all workstations at one time. However, the official stated that he expected all configuration changes to require the use of multifactor authentication on all workstations to be completed by mid-year 2019. In report DODIG-2018-094, Contractor I acknowledged that it was not compliant with the NIST requirement to implement multifactor authentication and included the weakness in a plan of action and milestones (POA&M). According to the contract manager, Contractor I planned to configure multifactor authentication software by December 2018 and enforce the use of multifactor authentication by April 2019. However, the contract manager stated that Contractor I expected problems in meeting the NIST requirement for multifactor authentication as Contractor I introduced new devices to its network. As of February 2019, Contractor I reported that it had configured 95 percent of its workstations with multifactor authentication software.

Allowing users to access networks that maintain CUI without using multifactor authentication makes it easier for an unauthorized user or malicious actor to assume the identity of an authorized user and to compromise the security of networks and systems that maintain CUI. The Director of Acquisition for the Missile Defense Agency should ensure that Contractor H configured all devices on its network to use multifactor authentication.

### ***Password Lengths Were Susceptible to Password Attacks***

(FOUO) Of the seven contractors that did not implement multifactor authentication as required by the NIST SP 800-171, system administrators at Contractors D, E, F, and J configured systems that maintained CUI to require [REDACTED]; Contractor I required 12-character passwords; and Contractors B and H required a [REDACTED].<sup>13</sup> Although NIST SP 800-171 does not specify a minimum number of characters when using passwords, contractors should configure their passwords based on an assessment of the ease of which a malicious actor could exploit [REDACTED] passwords and configure their networks and systems to accept a minimum password length with the lowest probability of exploitation. According to a white paper from the SysAdmin, Audit, Network and Security Institute (known as the SANS Institute), an information security research and education organization, there are more than 6 quadrillion

<sup>13</sup> (FOUO) Contractors D, E, F, and H required users to create passwords that included [REDACTED]. Although Contractor A initially required only single-factor authentication using a 9-character password, the contractor configured its network to use multifactor authentication during the audit. In addition, Contractor G initially required only single-factor authentication using a 14-character password, but the contractor configured its network to use multifactor authentication during the audit. Therefore, Contractors A and G now comply with NIST requirements for using multifactor authentication.

~~(FOUO)~~ combinations for 8-character passwords that include uppercase and lowercase characters, numbers, and special characters.<sup>14</sup> The SANS Institute calculated that password-cracking tools would take less than a day to crack an 8-character password. The DoD requires DoD system passwords to be at least 15 characters in length; however, this requirement does not apply to DoD contractors.<sup>15</sup>

While industry best practices vary on password length, shorter passwords reduce the number of possible combinations that attackers need to test before compromising the password. According to the DoD Chief Information Officer, the DoD should not allow contractors to use less stringent password length and complexity requirements when protecting DoD data than what is required of DoD users. The DoD's Procurement Toolbox website states that DoD Components can request that contractors implement more stringent security requirements if the Component identifies a specific need to increase security above the "Moderate" impact level.<sup>16</sup> Therefore, DoD Component contracting offices and requiring activities are not precluded from requiring contractors to configure their passwords to align with DoD password length and complexity requirements. Some contractors maintain information on some of the DoD's most secret and valuable defense technologies and, if that information is disclosed to malicious actors, the loss could have a serious adverse effect on DoD assets or individuals. DoD Component should assess the impact if DoD information maintained by contractor is disclosed and, when necessary, request that contractors implement more stringent security requirements.

Cyber attackers continuously attempt to gain unauthorized access to networks, systems, and DoD data and use several methods to exploit weak passwords, such as dictionary attacks, phishing, and brute force attacks.<sup>17</sup> For example, a dictionary attack uses a simple file that contains words found in a dictionary. A cyber attacker randomly groups potential words based on the words in the dictionary file in an effort to guess user passwords. Some programs try to gain access to information systems by guessing common words and phrases, using personal information associated with specific users, or using a combination of various methods and programs to repeatedly attempt to access sensitive information

<sup>14</sup> SANS Institute, "Combating the Lazy User: An Examination of Various Password Policies and Guidelines," 2019.

<sup>15</sup> Defense Information Systems Agency, "Application Security and Development Security Technical Implementation Guide," release 8, October 26, 2018.

<sup>16</sup> According to the Federal Information Processing Standards Publication 199, "Standards for Security Categorization of Federal Information and Information Systems," February 2004, a potential impact is "moderate" if the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational assets or individuals.

<sup>17</sup> Phishing is a method malicious actors use to pose as a reputable entity or person to obtain sensitive information, such as passwords and financial information. Brute force attacks are a trial and error method used to guess passwords.

protected by passwords. The use of longer, more complex passwords increases the time and resources required to compromise passwords and decreases the ability of hackers and others performing cyberattacks to compromise passwords to networks and systems that process, store, and transmit CUI. Therefore, contractors using passwords shorter than 15 characters makes contractors more vulnerable to malicious actors attempting to gain unauthorized access to contractor networks and systems that maintain DoD information. The DoD Chief Information Officer, in coordination with Defense Pricing and Contracting, should implement or revise policy to require all systems and networks that maintain DoD information, including those owned by contractors, to meet the minimum DoD password length and complexity requirements that are consistent with password requirements for DoD information systems.

### ***Contractors Did Not Always Mitigate the Vulnerabilities on Their Networks and Systems***

Contractors A and D did not scan their networks for vulnerabilities, and Contractors B, E, F, G, H, and J did not mitigate vulnerabilities as defined by their vulnerability management programs.<sup>18</sup> For example, Contractors B, E, and J had

*Contractors A and D did not scan their networks for vulnerabilities, and Contractors B, E, F, G, H, and J did not mitigate vulnerabilities as defined by their vulnerability management programs.*

vulnerability management programs that required them to mitigate high vulnerabilities within 2 to 14 days. Contractors F and G stated that they worked to mitigate vulnerabilities through monthly security updates and based on a three-week patching process respectively. Although Contractor H

did not have a written vulnerability management program, a Contractor H official stated that they worked to mitigate high vulnerabilities weekly. However, the contractors did not always mitigate identified vulnerability within these timeframes.

In addition, contractors did not always develop POA&Ms for vulnerabilities that they were unable to mitigate. NIST SP 800-171 requires contractors to periodically scan systems and applications to identify vulnerabilities, mitigate the vulnerabilities, and develop POA&Ms if they are unable to mitigate the vulnerabilities in a timely manner. However, Contractors A and D did not scan their networks to identify vulnerabilities and take actions to mitigate vulnerabilities affecting their networks. According to a Contractor A official, its parent company

<sup>18</sup> We did not assess the vulnerability management program for Contractor C because the contractor used government-furnished equipment.



performed nightly vulnerability scans and only provided Contractor A with a list of patches for it to install to mitigate vulnerabilities. However, the parent company did not provide Contractor A with a list of the specific vulnerabilities that impacted its network. Without knowing specific vulnerabilities affecting the contractor's network, Contractor A could miss opportunities to address emerging threats and vulnerabilities, which increases the risk of the exposure or loss of CUI. Contractor D also did not scan its network for vulnerabilities and only implemented automatic security updates.<sup>19</sup> According to the system administrator for Contractor D, the company plans to implement a new cybersecurity tool that will allow the contractor to scan its network to identify and mitigate network vulnerabilities by March 2019. Failure to patch systems will result in vulnerabilities persisting that can be used to gain unauthorized access to a network and system, introduce malware, and exfiltrate CUI.

We compared unclassified network scan results from July 2018 through January 2019 for Contractors B, E, F, G, H, I, and J. Contractor I managed risks and mitigated vulnerabilities as defined in its vulnerability management program. However, network vulnerabilities were not mitigated for Contractors B, E, F, G, H, and J in a timely manner according to the contractor's individual policies and processes for remediating vulnerabilities. Table 3 lists the number of unmitigated vulnerabilities at the seven contractor locations.

---

<sup>19</sup> A security update is a widely released fix for a product-specific, security-related vulnerability.

~~(FOUO)~~ Table 3. Unmitigated Network Vulnerabilities at Contractors B, E, F, G, H, I, and J

<del>(FOUO)</del> Contractor	Vulnerability Scan Dates	Number of Vulnerabilities Identified	Number of Unmitigated Vulnerabilities	Number, by Category, of Vulnerabilities That Were Not Mitigated			
				Critical	High	Medium	Low
Contractor A*	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Contractor B	September 2018 and January 2019	■	■	■	■	■	■
Contractor C**	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Contractor D*	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Contractor E	October 2018 and December 2018	■	■	■	■	■	■
Contractor F	August 2018 and October 2018	■	■	■	■	■	■
Contractor G	July 2018 and September 2018	638	432	37	333	62	0
Contractor H***	September 2018 and November 2018	■	■	■	■	■	■
Contractor I	August 2018 and November 2018	■	■	■	■	■	■
Contractor J	August 2018 and December 2018	■	■	■	■	■	■

~~(FOUO)~~

\* Contractors A and D did not scan their networks for vulnerabilities.

\*\* Contractor C used government-furnished equipment. Therefore, we did not assess network and system vulnerabilities.

\*\*\* The September 2018 and November 2018 scans included vulnerabilities with an “informational” severity code. Symantec describes informational vulnerabilities as events that result from scans for malicious services and intrusion detection activities that do not have a significant impact on the network. Therefore, the number of vulnerabilities identified does not include informational vulnerabilities.

Source: The DoD OIG.

(FOUO) At Contractor B, a January 2019 scan revealed that [REDACTED] of the [REDACTED] vulnerabilities identified on a September 2018 scan remained unmitigated. The September 2018 scan included [REDACTED] vulnerabilities and the January 2019 scan included [REDACTED] vulnerabilities. [REDACTED]  
[REDACTED]. For example, a [REDACTED] vulnerability from September 2018 could allow cyber attackers to execute malicious software code on networks and systems that maintain CUI. The NIST assessment of this vulnerability states that a remote attacker could exploit the vulnerability to gain unauthorized access to systems that contain CUI. Although [REDACTED] released a solution to fix this vulnerability in 2011, Contractor B still had not mitigated the vulnerability by September 2018. Although Contractor B's vulnerability management program included a process for developing POA&Ms for vulnerabilities that cannot be mitigated in a timely manner, Contractor B did not have a POA&M for the vulnerabilities we identified.

(FOUO) At Contractor E, a December 2018 scan revealed that [REDACTED] of the [REDACTED] vulnerabilities identified on an October 2018 network scan remained unmitigated. The [REDACTED] vulnerabilities included [REDACTED] and [REDACTED] vulnerabilities. [REDACTED]  
[REDACTED]<sup>20</sup> For example, an unmitigated [REDACTED] vulnerability from October 2018 identified on Contractor E's network could allow an unauthenticated, remote attacker to exploit code in the server. The NIST assessment of this vulnerability states that it could allow remote attackers to execute unauthorized commands to obtain and modify information on the systems that maintain CUI. Although the vulnerability was first identified in 2015, Contractor E still had not mitigated the vulnerability by December 2018. According to a Contractor E official, Contractor E did not create POA&Ms for unmitigated vulnerabilities because the scan results show unmitigated vulnerabilities until they are mitigated. However, without a POA&M, Contractor E could not correct network weaknesses, establish risk mitigation activities, or determine how long a vulnerability remained unmitigated.

(FOUO) At Contractor F, an October 2018 scan revealed that [REDACTED] of the [REDACTED] vulnerabilities identified on an August 2018 network scan remained unmitigated. The [REDACTED] vulnerabilities included [REDACTED] and [REDACTED] vulnerabilities. For example, an unmitigated [REDACTED] vulnerability from August 2018 could allow an attacker to remotely execute commands to weaken programs designed to prevent, detect, and remove malicious software.

<sup>20</sup> (FOUO) Privileged access allows users to set access rights for other users.

~~(FOUO)~~ The NIST assessment of this vulnerability states that the vulnerability allows unauthorized access and modification to systems that maintain CUI. Although the [REDACTED] vulnerability was initially identified in December 2017, Contractor F still had not mitigated the vulnerability by October 2018. According to a Contractor F official, Contractor F did not create POA&Ms for unmitigated vulnerabilities because there were too many unmitigated vulnerabilities to track. Contractor F did not take any actions, such as developing and implementing a POA&M, to determine a timeline to correct network weaknesses. Contractor F's lack of actions prevented it from tracking risk mitigation activities and how long a vulnerability remained unmitigated.

At Contractor G, a September 2018 scan revealed that 432 of the 638 vulnerabilities identified on a July 2018 network scan remained unmitigated. The 432 vulnerabilities included 37 critical and 333 high vulnerabilities. For example, an unmitigated high Microsoft vulnerability from July 2018 could allow remote attackers to obtain and modify information from systems that contain CUI. Although this vulnerability was initially identified in December 2015, Contractor G still had not mitigated the vulnerability by September 2018. A Contractor G official stated that the contractor did not create POA&Ms to document and track vulnerabilities because it would take too much effort to maintain a comprehensive list of unmitigated vulnerabilities. The official also stated that he prioritized vulnerabilities based on a 3-week pattern of applying fixes throughout the company. However, the high Microsoft vulnerability originally identified in December 2015 was still unmitigated as of September 2018.

~~(FOUO)~~ At Contractor H, a November 2018 scan revealed that [REDACTED] of the [REDACTED] vulnerabilities identified on a September 2018 network scan remained unmitigated. The [REDACTED] vulnerabilities included [REDACTED] and [REDACTED] vulnerabilities.<sup>21</sup> For example, an unmitigated [REDACTED] vulnerability from September 2018 identified in Contractor H's network could allow an attacker to gain elevated privileges and obtain information that is stored on a workstation. The NIST assessment of this vulnerability concluded that the vulnerability impacts [REDACTED] and [REDACTED], which allows an attacker to exploit a security feature bypass vulnerability and modify information on systems that contain CUI. This vulnerability was initially identified in June 2017 and Contractor H still had not mitigated the vulnerability by our review in November 2018. Although Contractor H significantly

<sup>21</sup> ~~(FOUO)~~ The September 2018 scans showed [REDACTED] vulnerabilities that included [REDACTED] vulnerabilities that had an "informational" severity code. The November 2018 scan revealed [REDACTED] unmitigated vulnerabilities that included [REDACTED] unmitigated vulnerabilities that had an "informational" severity code. Symantec describes informational vulnerabilities as events that result from scans for malicious services and intrusion detection activities that do not have a significant impact on the network. Therefore, the vulnerabilities included in the table represent non-informational vulnerabilities.

(FOUO) reduced the number of network vulnerabilities between September and November 2018, there were still [REDACTED] and [REDACTED] vulnerabilities that remained unmitigated. According to a Contractor H official, Contractor H did not develop POA&Ms and could not provide an explanation for not developing them.

(FOUO) At Contractor I, a November 2018 scan revealed that [REDACTED] of the [REDACTED] vulnerabilities identified on an August 2018 network scan remained unmitigated. The [REDACTED] unmitigated vulnerabilities identified in the November 2018 scan included [REDACTED] and [REDACTED] vulnerabilities. According to Symantec, [REDACTED]  
[REDACTED]  
[REDACTED]. Symantec also describes vulnerabilities with a low severity level as minor threats where successful exploitation of the vulnerabilities would not result in a complete compromise of information stored on and transmitted to the system. Although Contractor I did not provide a POA&M for the [REDACTED] unmitigated vulnerabilities, the contractor managed risk by mitigating all [REDACTED] and [REDACTED] vulnerabilities, and reducing the number of [REDACTED] and [REDACTED] vulnerabilities by more than [REDACTED] percent.

(FOUO) At Contractor J, a December 2018 scan revealed that [REDACTED] of the [REDACTED] vulnerabilities identified on an August 2018 network scan remained unmitigated. The [REDACTED] vulnerabilities included [REDACTED] vulnerabilities. If exploited, [REDACTED] of the [REDACTED] vulnerabilities could allow an attacker to gain control of the system. The remaining [REDACTED]  
[REDACTED].

In January 2019, Contractor J stated that [REDACTED] of the [REDACTED] [REDACTED] vulnerabilities were already mitigated and that [REDACTED] [REDACTED] vulnerability was included in a POA&M. However, Contractor J did not provide the subsequent network scan results to show that the [REDACTED] [REDACTED] vulnerabilities were mitigated or the POA&M that included the [REDACTED] vulnerability. Although Contractor J reduced the total number of vulnerabilities by more than [REDACTED] percent between August and December 2018, it did not comply with its own vulnerability management program by mitigating [REDACTED] vulnerabilities within 48 hours of identifying the vulnerability.

Although seven of the contractors that we assessed had vulnerability management programs that identified and mitigated some vulnerabilities, only Contractor I managed risk in a timely manner by mitigating known vulnerabilities. Contractors B, E, F, G, H, and J identified and mitigated some vulnerabilities, but they did not comply with the requirements of

Although seven of the contractors that we assessed had vulnerability management programs that identified and mitigated some vulnerabilities, only Contractor I managed risk in a timely manner by mitigating known vulnerabilities.



their own vulnerability management programs or internal processes to manage risk when they allowed critical and high vulnerabilities to remain unmitigated on their networks. For example, Contractor J's vulnerability management plan required high vulnerabilities to be mitigated within 48 hours of identifying the vulnerability. However, the network scan results showed that five vulnerabilities remained unmitigated between August and December 2018. The DoD Chief Information Officer stated in July 2018, during a speech at a Defense Systems Summit, that countless cyber incident reports show that the overwhelming majority of incidents are preventable by implementing basic cyber hygiene and data safeguards. Implementing basic cyber hygiene includes regularly patching known vulnerabilities. Without a thorough and systematic process to mitigate vulnerabilities in a timely manner, the contractors increased the risk that cyberattacks or other malicious actions could exploit the vulnerabilities. As a result, CUI that supports critical DoD programs could be compromised through cyberattacks that are designed to exploit those weaknesses. The DoD Component contracting offices, in coordination with DoD requiring activities, should develop and implement a plan to verify that contractors correct the weaknesses related to mitigating vulnerabilities in a timely manner.

### ***CUI Was Not Protected on Removable Media***

Contractors D, E, F, G, H, and J did not comply with NIST requirements, whereas Contractors A, B, and I complied with the requirements to control the use of removable media on systems that process, store, and transmit CUI. NIST SP 800-53 states that organizations can use technical and nontechnical safeguards to restrict the use of removable media.<sup>22</sup> An example of a technical safeguard that restricts the use of removable media is disabling ports that allow the connection of removable media. Other safeguards include, but are not limited to, restricting or limiting the use of removable media by:

- allowing only organization-approved and -issued devices, and
- denying "write" access to the devices.

~~(FOUO)~~ Contractor A stored removable media received from the requiring activity in locked safes. A Contractor A official stated that information was only stored on removable media when Contractor A needed to hand-deliver removable media to the requiring activity. The official also stated that Contractor A monitored the amount of information stored on removable media using anomaly detection. An anomaly detection control alerts Contractor A to unusual patterns in data exfiltration activities. In addition, Contractor B had [REDACTED]

<sup>22</sup> NIST SP 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," Revision 4, April 2013 (includes updates as of January 22, 2015).

(FOUO) [REDACTED]  
[REDACTED]  
[REDACTED].

Furthermore, Contractor I issued removable media devices to specific personnel and only those individuals were authorized to store information on removable media devices. Contractor I's control of the users who were issued removable media devices allowed it to identify the individuals responsible for protecting the removable media if a security incident occurred and begin a process to track incident activities.

*Officials at Contractors D, E, F, G, H, and J allowed users to store CUI on removable media devices without ensuring that security controls met NIST requirements.*

Officials at Contractors D, E, F, G, H, and J allowed users to store CUI on removable media devices without ensuring that security controls met NIST requirements. Contractors D, F, and G allowed users to export CUI

from their respective networks to any type of removable media device without implementing safeguards to protect the data stored on the devices. Contractors D and G relied on users to encrypt removable media devices. According to the systems administrator for Contractor D, the information stored on removable media devices was not "sensitive enough" to implement a requirement to encrypt the devices. A Contractor F official stated that it could not encrypt removable media devices because the equipment used with the devices did not support encryption. A Contractor G official stated that implementing a control to limit the use of removable media devices would be costly because the contractor would have to purchase new removable media devices to replace the devices already deployed throughout the company. The official also stated that Contractor G made a risk-based decision to allow employees to use any removable media device but did not have a formal risk assessment of that decision.

Although Contractor E limited the use of universal serial bus (commonly known as USB or thumb drives) and external hard drives to company-issued devices, it did not implement security controls to protect CUI stored on compact discs and digital versatile discs (commonly known as CDs and DVDs). A Contractor E official stated that the contractor relied on its acceptable use policy to limit the use of non-company-issued devices, which places the responsibility on the user to protect CUI. Contractor E also considered the risk of data disclosure as low because compact discs and digital versatile discs have limited storage capacity compared to thumb drives and external hard drives. Nevertheless, compact discs and digital versatile discs can be used to steal or compromise CUI; therefore, restricting their use is also necessary.

In report DODIG-2018-094, we identified that Contractor H did not implement security controls to prevent users from storing CUI on unapproved devices. As of November 2018, Contractor H continued to allow users to store CUI on any removable media device without technical safeguards, such as encryption, to protect the information on the devices. Contractor H officials stated that it reduced the amount of CUI on its network; therefore, users had less access to CUI. However, reducing user access to CUI does not prevent users from storing CUI on removable media devices. In addition, a Contractor H official stated that, although the company identified a tool to limit and encrypt removable media devices and it expected to deploy the tool by the first quarter of 2019, the company could not deploy the tool until it first upgraded its server software. The Contractor H official stated that the contractor could not provide a more accurate estimated date for deploying the tool until the server software upgrade is completed.

(FOUO) Although Contractor J had policies that required users to [REDACTED], Contractor J did not implement tools that [REDACTED]. According to a Contractor J official, Contractor J deployed a tool that [REDACTED] when personnel [REDACTED]. However, the tool [REDACTED]. A Contractor J official stated that the contractor identified a tool that would [REDACTED] and that Contractor J plans to fully deploy the tool by the third quarter of 2019.

Although encryption does not prevent users from transferring CUI onto removable media, it is effective at preventing unauthorized individuals from accessing information stored on removable media. Unless contractors encrypt removable media, malicious actors and unauthorized users could easily access critical data that supports DoD programs. The DoD Component contracting offices, in coordination with DoD requiring activities, should develop and implement a plan to verify that contractors correct the weaknesses related to protecting and monitoring data on removable media.

### ***No Oversight of Third-Party Service Provider's Network Protection Activities***

In report DODIG-2018-094, we identified that Contractor H did not have oversight of its network perimeter protection activities. Network perimeter protection includes, among other activities, blocking unwanted traffic, allowing remote access, filtering dangerous content, and detecting potential network attacks. Service-level agreements provide details on the type and level of service that customers receive. NIST SP 800-171 requires contractors to monitor, control, and

protect communications at the external boundaries and key internal boundaries of organizational systems. However, when Contractor H hired the third-party service provider, it did not establish a service-level agreement with the provider and subsequently did not have oversight of the provider's activities.

As of November 2018, Contractor H continued to have no oversight over the third-party service provider activities for protecting Contractor H's network. However, according to an official for Contractor H, the contract with the current third-party service provider expires in April 2019. The official stated that Contractor H identified a different contractor that would allow it to monitor network boundary security and implement its own firewalls and intrusion detection system. Additionally, he stated that Contractor H would begin testing the new contractor's capabilities in March 2019 and fully transition to the new contractor by April 2019. The Director of Acquisition for the Missile Defense Agency should ensure that Contractor H transitioned to a third-party service provider that allows oversight activities of the provider.

### ***Cybersecurity Incidents Were Not Documented and Tracked***

*Although Contractor G reported cybersecurity incidents to the Defense Cyber Crime Center as required by DFARS clause 252.204-7012, it did not implement a formal process for documenting and tracking cybersecurity incidents that affected its network.*

Contractor G did not document and track all cybersecurity incidents affecting its network. NIST SP 800-171 requires non-Federal organizations to document, track, and report incidents to appropriate officials both internal and external to the organization such as the contractor's security personnel (internal), and the DoD Component contracting agency, requiring activity, and Defense Cyber Crime Center (external). Although

Contractor G reported cybersecurity incidents to the Defense Cyber Crime Center as required by DFARS clause 252.204-7012, it did not implement a formal process for documenting and tracking cybersecurity incidents that affected its network.

A formal process includes recording the facts related to the incident in an issue tracking system used to monitor the status of the incident through its resolution. The issue tracking system should include information such as actions taken to resolve the incident, impact assessments, and the next steps after incident resolution. Instead, Contractor G notified users involved in a cybersecurity incident by e-mail and did not track actions taken to resolve the incident. According to a Contractor G official, the contractor only tracked the removal of

workstation hard drives and unapproved programs. The official stated that limited resources prevented Contractor G from implementing a tool to document and track security incidents. However, the official stated that Contractor G initially deployed a tool for documenting security incidents in August 2018 and fully implemented the tool in February 2019. The Contractor G official indicated that it could take up to 3 years for Contractor G to fully meet NIST SP 800-171 requirements because of budget constraints and challenges with integrating the tool within its network. Failure to document and track cybersecurity incidents could impact the timeliness and completeness of Contractor G's incident response activities by limiting the organization's ability to determine whether a specific incident is part of a larger, more nefarious threat against the organization. The DoD Component contracting offices, in coordination with DoD requiring activities, should develop and implement a plan to verify that contractors correct the weaknesses related to documenting and tracking cybersecurity incidents.

### ***System Lockouts After Inactivity or Unsuccessful Logon Attempts Were Insufficient to Prevent Unauthorized Access***

The system administrator for Contractor D configured user sessions to lock after extended periods of inactivity because employees complained that they had to enter their password too many times. In addition, Contractor D stated that it did not receive many visitors and determined that there was a low risk of unauthorized individuals accessing contractor computers. NIST SP 800-171 requires user sessions to lock after a period of inactivity but does not specify the period.<sup>23</sup> Although NIST SP 800-171 does not specify a time period for automatically locking user sessions, Contractor D configured sessions to automatically lock after 60 minutes of inactivity without assessing the risks associated with that decision. The Defense Information Systems Agency Security Technical Implementation Guide for Application Security limits inactivity to 15 minutes before systems and networks automatically lock. However, contractors were not required to comply with Security Technical Implementation Guide requirements. Employee complaints are not a sufficient rationale for allowing inactive user sessions to extend to 60 minutes before locking the session. Additionally, Contractor D did not consider insider threat possibilities when determining that there was a low risk of unauthorized access to its computers.

~~(FOUO)~~ Contractors E, F, and G conducted risk-based assessments for locking user sessions after specific periods of inactivity. For example, Contractor E made a risk-based decision to [REDACTED]

<sup>23</sup> DoD Components are required to limit inactivity to 15 minutes in accordance with the Defense Information Systems Agency Application Security and Development Security Technical Implementation Guide, release 8, October 26, 2018; however, contractors are not required to comply with Security Technical Implementation Guide requirements.



(FOUO) [REDACTED]. In addition, the system administrator for Contractor G stated that locking workstations after [REDACTED] of inactivity was necessary because workstations needed to remain operational while the contractor executed programs and tests. The system administrator also stated that the security measures in place at Contractor G were sufficient to allow workstations to lock after 60 minutes of inactivity. Contractor F also made a risk-based decision, based on business needs, to configure systems to lock [REDACTED] of inactivity because [REDACTED] did not allow personnel adequate time to complete their job tasks. While Contractors E, F, and G decided to lock workstations after [REDACTED] minutes of inactivity based on business needs, risk assessments, and physical security controls, insider threat activities could make unlocked workstations easy targets for stealing DoD information. During the audit, Contractor E reassessed risk and changed its workstation configuration settings to lock automatically for inactivity from [REDACTED], which aligns with DoD standards. Industry best practices vary for locking networks and system automatically for periods of inactivity, but shorter lock out times limits the potential for unauthorized access to CUI and prevents malicious actions, such as data manipulation or theft, from occurring.

NIST SP 800-171 also requires contractors that maintain CUI to limit unsuccessful logon attempts but does not specify the maximum number of logon attempts. System administrators for Contractor A configured user accounts to not automatically lock after any number of failed logon attempts. According to a Contractor A official, users received messages through e-mail or mobile devices of unsuccessful logon attempts that required them to answer challenge questions to confirm their identity. However, the user accounts remained unlocked during this process. Although the Defense Information Systems Agency Security Technical Implementation Guide for Application Security limits the number of unsuccessful logon attempts to three before systems and networks automatically lock, contractors are not required to comply with the Security Technical Implementation Guide requirements.

(FOUO) Contractors B, D, E, F, and J officials stated that the contractors made risk-based decisions to lock user accounts after [REDACTED] unsuccessful logon attempts. For example, Contractors B and F stated that they conducted a study on the business impact for unlocking user accounts and made a risk-based decision to configure their network to lock user accounts after [REDACTED] unsuccessful logon attempts. The system administrator for Contractor D stated that the contractor configured its network to lock user accounts after [REDACTED] unsuccessful logon attempts because the company believed that [REDACTED] attempts was sufficient to protect against brute force attempts and still allow users a sufficient number of attempts to correctly enter their password without being locked out of their account.

(FOUO) Contractor E and J officials stated that their management made a risk-based decision to allow users [REDACTED] unsuccessful logon attempts before locking user accounts. Because Contractors B, D, E, F, and J assessed the risks and associated impacts of unsuccessful logon attempts, we concluded that the contractors complied with the intent of NIST SP 800-171 related to limiting unsuccessful logon attempts.

Contractor H officials explained that they configured accounts to lock after three unsuccessful log on attempts but users were allowed three additional attempts after every 25 minutes to log on to the network. Ultimately, Contractor H allows unlimited attempts to log into its network, which would allow a malicious actor unlimited attempts to execute a brute force attack. According to the Contractor H officials, the contractor allowed the unlimited attempts to prevent an increase in the number of help desk requests for assistance for unlocking user accounts.

Without a network configuration that locks user sessions, malicious cyber intruders would have unlimited attempts to access contractor systems. Additionally, failure to limit unsuccessful logon attempts makes the system susceptible to brute force attacks. Automatically locking systems and user accounts limits the potential for unauthorized access and prevents malicious actions that could jeopardize the confidentiality and integrity of CUI. The DoD Chief Information Officer, in coordination with Defense Pricing and Contracting, should implement or revise policy to require all systems and networks that maintain DoD information, including those owned by contractors, to configure systems and networks to align with DoD requirements to lock automatically after defined periods of inactivity and unsuccessful logon attempts. In addition, the DoD Component contracting offices, in coordination with DoD requiring activities, should develop and implement a plan to verify that contractors correct the weaknesses related to utilizing automatic lock after inactivity or unsuccessful logon attempts.

### ***Physical Security Controls Were Not Implemented to Detect Unauthorized Access***

(FOUO) A security official at Contractor B did not implement physical security measures to allow security personnel to [REDACTED] [REDACTED] that maintained CUI. NIST SP 800-171 requires organizations to protect and monitor the physical facility and support infrastructure for organizational systems. To meet the NIST requirement, NIST SP 800-53 suggests active and timely surveillance with equipment such as cameras, as well as archived security footage, is necessary to respond to suspicious activities and physical security incidents.<sup>24</sup>

<sup>24</sup> NIST SP 800-171 security controls are derived from the moderate security control baseline in NIST SP 800-53.

(FOUO) However, Contractor B did not [REDACTED] [REDACTED] that maintain CUI. In addition, [REDACTED] [REDACTED]. Furthermore, [REDACTED]. According to the security official, the camera system at one facility was old and Contractor B did not allocate resources to [REDACTED]. Using surveillance equipment allows security officials to continuously monitor personnel activity, external facility entry and exit points, and publically accessible areas for signs of unusual or prohibited behaviors. By not installing surveillance cameras to [REDACTED], Contractor B reduced its ability to promptly identify and respond to security incidents and suspicious activities in and around the facilities that maintain CUI.

*Contractor D did not implement physical security measures such as maintaining visitor logs, monitoring the interior and exterior of the facility, or installing security mechanisms to protect servers from unauthorized access.*

In addition, Contractor D did not implement physical security measures such as maintaining visitor logs, monitoring the interior and exterior of the facility, or installing security mechanisms to protect servers from unauthorized access. NIST SP 800-171 requires organizations to limit physical access to systems, equipment, and facilities.

Contractor D's office manager stated that the contractor did not have many visitors and did not believe stricter security was needed. Maintaining visitor logs, monitoring the facility, and ensuring that servers are secure reduces the risk of unauthorized individuals from gaining access to DoD information maintained on Contractor D's network. The DoD Component contracting offices, in coordination with DoD requiring activities, should develop and implement a plan to verify that contractors correct the weaknesses related to implementing physical security controls.

### **System Activity Reports Were Not Generated and Reviewed**

(FOUO) System administrators for Contractors B, D, and H did not [REDACTED] [REDACTED]. NIST SP 800-171 requires contractors to generate audit records that allow the contractors to monitor, analyze, investigate, and report unauthorized system activity. Audit logs are a type of activity report that provide automated and chronological records of users' activity.

(FOUO) Although Contractor B had the ability to generate and retain user activity reports, officials did not [REDACTED]. An official at Contractor B stated that it did not develop and implement a policy requiring [REDACTED] and [REDACTED]. In addition, Contractor D installed a tool that, among other capabilities, can generate system activity reports that would aid contractor officials in reviewing system activity; however, [REDACTED]. The system administrator for Contractor D did not provide a reason for not using the tool it had. The DoD Component contracting offices, in coordination with DoD requiring activities, should develop and implement a plan to verify that contractors correct the weaknesses related to generating system activity reports.

In report DODIG-2018-094, we identified that Contractor H did not have a process for generating and reviewing system activity reports. By November 2018, Contractor H had installed a tool that allows it to generate and review system activity reports. However, Contractor H configured only 18 of the more than 200 assets on its network to generate system activity reports. According to the cybersecurity engineer, limited storage capacity prevented Contractor H from configuring the tool to generate system activity reports for all its assets. A Contractor H official stated that the contractor planned to implement the tool on all its assets by the second quarter of calendar year 2019.

When system activity reports are regularly reviewed, they could identify unauthorized access attempts and activity, help prevent breaches, and provide forensic evidence when investigating malicious behavior. If the system is incapable of tracing actions to individuals, it cannot identify and correct improper or illegal activity on the network. The Director of Acquisition, Missile Defense Agency, should ensure that Contractor H configured all assets on its network to create system activity reports.

### ***Administrators Did Not Consistently Assign User Access and Privileges That Aligned With User Responsibilities***

(FOUO) System administrators for Contractors B, D, and H did not [REDACTED]. NIST SP 800-171 requires contractors to limit system access to authorized users. However, the process implemented by Contractor B and H may not ensure that only authorized personnel gain access to CUI. For example, both Contractors B and H [REDACTED]. Specifically, system administrators at Contractors B and H relied on [REDACTED].

(FOUO) [REDACTED]. The SharePoint engineer at Contractor B stated that the [REDACTED]

[REDACTED]. An official at Contractor H stated that the contractor identified a tool to purchase that would document and grant access to users, which they plan to deploy by the summer of 2019. Contractor D granted access to a system that contained CUI through an informal e-mail process that included notifying the system administrator of the need for access. However, the system administrator did not require users to justify the need for access. The system administrator at Contractor D stated that all users had the same level of access to the information maintained on the system because some employees perform multiple job functions, which dictated the need for granting the same level of access to all users.

A formal request process includes completing a standard form that requires user roles, justification for access, and supervisory approval. Informally granting access could potentially result in individuals maintaining access to CUI despite no longer having a need for access to it. Failure to apply the principle of least privilege, which is a security objective requiring users to have only the access needed to perform their official duties, may result in a single individual being able to conduct unauthorized or inappropriate activities, increasing the security risk to the system and the likelihood of unauthorized access to CUI. The DoD Component contracting offices, in coordination with DoD requiring activities, should develop and implement a plan to verify that contractors correct the weaknesses related to requiring and maintaining justification for accessing systems that contain controlled unclassified information.

## **Neither DoD Component Contracting Offices Nor DoD Requiring Activities Assessed Contractors' Actions for Protecting Information**

Although DoD Component contracting offices took steps to require contractors to protect CUI by including DFARS clause 252.204-7012 in contracts, the contracting offices were not always aware of which contract required contractors to manage CUI, and they did not develop and implement processes to verify that potential contractors' networks and systems complied with NIST-directed security controls for protecting CUI.

The reasons the contracting offices did not ensure that contractors were protecting DoD information varied. For example, the Contracting Officer Representative for the U.S. Army Corps of Engineers (Contractor D) stated that he did not believe it was necessary to request information, such as a system security plan, that

would provide details on how DoD information would be protected. In addition, the Contracting Officer Representative for Contractor D stated that he was unaware of plans for Contractor D to implement the controls as outlined in the NIST SP 800-171 and that he was not knowledgeable of DFARS clause 252.204-7012. An Air Force official (Contractor E) stated that the Air Force was waiting for direction from the Protecting Critical Technology Task Force on ensuring contractor compliance with DFARS clause 252.204-7012. A Defense Contract Management Agency official (Contractor J) stated that the agency was waiting for DoD guidance to establish an assessment process to verify contractor compliance with DFARS clause 252.204-7012. However, the Undersecretary of Defense for Acquisition and Sustainment already issued a memorandum in November 2018 providing guidelines to acquisition personnel for assesses contractor compliance with cybersecurity requirements.<sup>25</sup> Furthermore, the Director of Software stated that the Defense Contract Management Agency would take a risk-based approach when selecting which contractors to assess because the agency did not have the resources to review compliance with the DFARS clause for all contractors they oversee.

DoD Component contracting offices such as the MDA (Contractors H and I) and the Naval Information Warfare Systems Command (Contractor B) expressed concern over the Department's ability to assess non-Federal networks and systems.<sup>26</sup> Specifically, a Missile Defense Agency official stated that the agency did not have the contractual authority to oversee compliance on contractor networks. In addition, the MDA official stated that a clear delineation of the legal jurisdiction, authority, and boundaries of the Government needed to be established before it could implement oversight of contractor compliance with DFARS clause 252.204-7012. A Naval Information Warfare Systems Command (Contractor B) official expressed concerns that existing contract language did not allow the command to oversee contractor systems for compliance with NIST SP 800-171 requirements. While DoD Component contracting offices oversee contractor performance, they expressed confusion on whether they could conduct oversight activities of contractor networks and systems specific to cybersecurity protections. To alleviate confusion, the DPC should revise current policy to include a requirement that would allow DoD Component contracting offices and requiring activities to assess contractor networks and systems for compliance with NIST SP 800-171 requirements. For example, DoD Component contracting offices could include a right-to-audit statement in contracts that would

<sup>25</sup> Undersecretary of Defense for Acquisition and Sustainment Memorandum, "Guidance for Assessing Compliance and Enhancing Protections Required by DFARS Clause 252.204.7012, Safeguarding Covered Defense Information and Cyber Incident Reporting," November 2018.

<sup>26</sup> In February 2019, the Space and Naval Warfare Center was renamed the Naval Information Warfare Systems Command.



allow representatives of the agencies to assess the cybersecurity protections implemented on contractor networks and systems that maintain DoD CUI. The Principal Director for Defense Pricing and Contracting, in coordination with the appropriate DoD Component responsible for developing policy, should revise its current policy to include language that would require DoD Component contracting offices and requiring activities to validate contractor compliance with NIST SP 800-171.

Officials for U.S. Cyber Command (Contractor A), USTRANSCOM (Contractor F), and Office of the Director, Operational Test and Evaluation (Contractor G), all acknowledged that their contracting offices did not conduct oversight activities related to ensuring compliance with cybersecurity controls. The contracting offices planned to meet with the contractors mentioned in this report to determine how the contractors are addressing the weaknesses identified during the audit. However, just meeting with the contractors mentioned in this report will not be sufficient for enforcing NIST SP 800-171 requirements at all DoD contractors that have access to CUI. Although not currently required to verify that contractors comply with DFARS clause 252.204-7012, contracting offices should ensure that all of their contractors are sufficiently enforcing NIST SP 800-171 requirements. The Program Counsel for the Naval Information Warfare Systems Command believed that Contractor B's self-certification of compliance with NIST SP 800-171 controls was sufficient oversight and did not believe the Naval Information Warfare Systems Command had contractual rights to verify compliance with NIST requirements. However, the Program Counsel stated they would coordinate with Contractor B to address the weaknesses identified.

An official from the MDA (Contractors H and I) stated that it was the contractor's responsibility to implement NIST SP 800-171 security requirements and believed that Contractors H and I were fully compliant with the requirements because the contractors developed a system security plan documenting how they would address the control weaknesses. System security plans, which provide an overview of an organization's plans to implement security controls, do not provide a basis for determining whether the controls are actually implemented and operating as intended.<sup>27</sup> Although DoD Component contracting offices may use the system security plans to obtain an understanding of a contractor's security posture, verification is still necessary to confirm that the contractors implemented the security controls outlined in the system security plan. The Undersecretary of Defense for Acquisition and Sustainment memorandum issued in November 2018 gives DoD component contracting offices the authority to oversee contractor

<sup>27</sup> NIST SP 800-18, "Guide for Developing Security Plans for Federal Information Systems," Revision 1, February 2006.

compliance with NIST SP 800-171. The DoD and the Defense contractors share the responsibility for ensuring that security controls are implemented to protect critical DoD data. Increasing threats of cyberattacks against DoD contractors' networks and systems require the effective implementation of system security controls to reduce the number of vulnerabilities that malicious actors can and have used to compromise information critical to national security.

Recognizing that oversight of contractor security was needed to protect CUI, the DoD issued a series of policy memorandums related to verifying compliance with NIST SP 800-171 security requirements. The Director of the Defense Pricing/Defense Procurement and Acquisition Policy issued a memorandum in September 2017 to add oversight requirements to the terms of the contract if an agency determined that oversight of DFARS clause 252.204-7012 security requirements was necessary.<sup>28</sup> However, the September 2017 memorandum also states that DFARS clause 252.204-7012 does not add any requirement for the Government to monitor contractor implementation of NIST SP 800-171. This statement can result in contracting agencies assuming they do not have the authority to validate contractor compliance with NIST SP 800-171 security controls, similar to the views expressed by the MDA and the Naval Information Warfare Systems Command. In addition, contractors may conclude that the DoD will not assess contractor compliance with NIST SP 800-171 and can make it difficult for the DoD to conduct an assessment on the contractor systems and networks. For example, according to a Contractor E official, personnel from the DoD Office of the Chief Information Officer previously stated that the DoD would not verify contractor compliance and would continue to rely on the contractors' self-certification of compliance with the NIST SP 800-171 controls.

*The Undersecretary of Defense for Acquisition and Sustainment's November 2018 memorandum included guidance for requiring activities to review system security plans and plans of action and milestones for security requirements that contractors have not implemented.*

The Undersecretary of Defense for Acquisition and Sustainment's November 2018 memorandum included guidance for requiring activities to review system security plans and POA&M for security requirements that contractors have not implemented. According to the memorandum, requiring activities can tailor their assessments of contractor compliance based on program risks. For example, the guidance states that

<sup>28</sup> Defense Pricing/Defense Procurement and Acquisition Policy (currently known as Defense Pricing and Contracting), "Implementation of DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting," September 21, 2017.

requiring activities should require self-attestations about compliance with DFARS clause 252.204-7012 from contractors before contract award. The guidance also states that requiring activities should establish measures to assess contractor compliance with cybersecurity requirements. Furthermore, for contracts that include DFARS clause 252.204-7012, the guidance states that requiring activities should conduct on-site assessments of the contractors' information systems to assess and monitor compliance with

NIST SP 800-171 requirements. However, this memorandum only encourages and does not explicitly require DoD Components to implement the guidance included in the memorandum. A DPC official acknowledged that the memorandum is not DoD policy; therefore, DoD Component contracting

*However, this memorandum only encourages and does not explicitly require DoD Components to implement the guidance included in the memorandum.*

offices are not required to follow the guidance. Without adding contractual language that provides the authority for DoD Component contracting offices and requiring activities to conduct on-site assessments of compliance with NIST SP 800-171 requirements, the DoD is unable to verify the implementation of security controls outlined in contractors' system security plan or assess their progress in addressing weaknesses included in their POA&Ms.

In addition, the memorandum does not sufficiently address the responsibility of the Government to properly mark CUI and communicate it to the contractor. A DPC official stated that not all contracts involved CUI. The official also stated that the November 2018 memorandum allows DoD Components to implement procedures for verifying contractor compliance with NIST SP 800-171 controls for the contracts with CUI. However, to implement these procedures, each contracting office and requiring activity should know which contractors maintain CUI on contractor-owned networks and systems.

The Undersecretary of Defense for Acquisition and Sustainment stated in a memorandum issued in February 2019 that an individual contract approach to assess compliance with DFARS clause 252.204-7012 was inefficient for the Government. As a result, she directed the Director of the Defense Contract Management Agency to propose a strategy to obtain and assess contractor system security plans and associated POA&Ms and determine industry cybersecurity readiness for the contracts they administer. The Undersecretary of Defense for Acquisition and Sustainment stated that other contracting offices could implement a solution similar to the Defense Contract Management Agency's proposed methodology for assessing compliance with the DFARS clause. However, according to a DPC official, as of

March 2019, the proposed strategy was not complete. Until a strategy is developed and implemented, the DoD remains challenged in verifying whether its contractors appropriately protect DoD information.

Oversight activities could include coordinating with DoD Component officials with cybersecurity responsibilities to assess whether contractors implemented NIST SP 800-171 security controls on their networks and systems. Understanding that many DoD Component contracting offices manage hundreds of contracts, the contracting offices could develop and implement a risk-based plan for overseeing their contractors. The Principal Director for Defense Pricing and Contracting, in coordination with the appropriate DoD Component responsible for developing policy, should revise its current policy to require DoD Component contracting offices, as part of the Request for Proposal and source selection processes, and requiring activities, during the contract performance, to provide oversight to ensure that contractors comply with the NIST requirements for protecting CUI throughout the contract's period of performance. In addition, the Principal Director should require DoD Component contracting offices, in coordination with requiring activities, to:

- develop and implement a risk-based process for verifying that contractors comply with DFARS clause 252.204-7012 for protecting CUI, and
- take corrective actions against contractors that fail to meet the NIST requirements for protecting CUI.

In addition, DoD Component contracting offices, in coordination with DoD requiring activities, should develop and implement a plan to verify that contractors correct the weaknesses identified in this report related to multifactor authentication, mitigating vulnerabilities, removable media, cybersecurity incidents, automatically locking systems, physical security controls, system activity reports, and user access justification.

As of June 2018, the Federal Procurement Data System (FPDS) showed that the DoD awarded 48,663 contracts to 12,075 contractors. However, DoD Component contracting offices did not always know which contracts required contractors to maintain CUI. According to the contracting offices, the DoD does not have a process in place to track which contractors maintain CUI and only tracks which contracts include DFARS clause 252.204-7012. Without knowing whether current and potential contracts include CUI, and without providing oversight of the contractors' actions for protecting DoD CUI, the DoD increases its risk that contractors would maintain critical and sensitive DoD information on networks and systems that do not meet minimum requirements for protecting DoD information. When security requirements are not applied or are ineffective, networks and

systems that process, store, and transmit CUI are vulnerable to data breaches, data loss and manipulation, and unauthorized disclosure of critical information. This leaves DoD CUI vulnerable to cyberattacks by malicious actors who target DoD contractors. The Principal Director for Defense Pricing and Contracting, in coordination with the appropriate DoD Component responsible for developing policy, should develop and implement policy requiring DoD Component contracting offices and requiring activities to maintain an accurate accounting of contractors that access, maintain, or develop CUI as part of their contractual obligations.

## **Unauthorized Access to or Disclosure of CUI Weakens National Security**

Contractors use CUI to produce services or products for the DoD. DFARS clause 252.204-7012 requires Defense contractors to secure contractor information networks and systems using the applicable security requirements outlined in NIST SP 800-171. Security measures, such as multifactor authentication, vulnerability management, and data encryption, decrease the risk of unauthorized access to CUI. In addition, identifying and mitigating vulnerabilities in a timely manner decreases the risk that cyberattacks could exploit known system and network weaknesses. Furthermore, limiting access to CUI to users with a mission-related need to know reduces the risk of intentional or unintentional disclosures of data critical to national security. Active and passive security surveillance measures, such as installing and maintaining operating security cameras that provide the ability to monitor movement throughout a facility, reduce the capability of insiders to intentionally compromise networks and systems that contain CUI. Defense contractors that do not implement the proper security controls to protect DoD information risk disclosing critical technical details of DoD programs to U.S. adversaries.

As a result of DoD contractors not fully implementing the security controls outlined in NIST SP 800-171 and DoD requiring activities and Component contracting offices not monitoring contractor compliance with these controls, DoD contractors could become victims of cyber attacks. Malicious actors can exploit vulnerabilities on the networks and systems of DoD contractors and steal information related to some of the Nation's most valuable advanced defense technologies. If the DoD does not include security as a major factor in considering whether to do business with Defense contractors, there is an increased risk that DoD CUI related to national security could fall into the hands of our adversaries.

## Comments on the Finding and Our Response

### *Deputy Assistant Secretary of the Navy (Research, Development, Test, and Evaluation) Comments*

The Deputy Assistant Secretary of the Navy (Research, Development, Test, and Evaluation) (DASN), responding for the U.S. Navy Contracting Officer, stated that information included in the report about DoD Component contracting offices and the subsequent recommendations exceeded the stated audit objective. The DASN stated that the DoD and DoD Components, not contracting offices and requiring activities, were responsible for developing policy and processes for verifying contractor compliance with NIST. In addition, he stated that policy requiring the implementation of internal controls and processes to verify that contractors comply with Federal and DoD requirements for protecting CUI maintained on contractor systems did not exist. The DASN also stated that requiring activities, and not contracting offices, should determine which NIST requirements contractors must meet. The DASN further stated that tracking contracts including the DFARS clause would not help identify which contractors maintained CUI because the clause is required in all contracts. Lastly, he clarified that, when Naval Information Warfare Systems Command officials expressed concern over the DoD's ability to assess non-Federal networks and systems, they were referring only to Naval Information Warfare Systems Command concerns and not DoD or the Department of the Navy concerns.

### *Our Response*

We disagree that our findings and recommendations specific to DoD Component contracting offices were outside of the scope of the audit objective. According to NIST SP 800-171, the DoD and the Defense contractors share the responsibility for ensuring that security controls are implemented to protect critical DoD data. Therefore, DoD Component contracting offices and requiring activities share responsibility for ensuring that contractors comply with DFARS clause 252.204-7012 and NIST SP 800-171 requirements. The Undersecretary of Defense for Acquisition and Sustainment's November 2018, memorandum includes guidance for DoD acquisition personnel to establish measures to assess contractor compliance with cybersecurity requirements and states that requiring activities should conduct on-site assessments of the contractors' information systems to assess and monitor compliance with NIST SP 800-171 requirements. Although the DoD did not require Component contracting offices and requiring activities to verify compliance with the DFARS clause 252.204-7012 and NIST SP 800-171 requirements when the audit began, the November 2018 memorandum provides methods for assessing and verifying contractor compliance with those requirements.



We did not state that DoD Component contracting offices should only track contracts based on the DFARS clause to identify contractors that maintain CUI. We stated that DoD Component contracting offices and requiring activities should maintain an accurate accounting of the contractors that maintain CUI, which will enable DoD Component contracting offices and requiring activities, and the DoD, to know which contractors are responsible for implementing the NIST SP 800-171 security controls.

With respect to the DASN's clarification of the comments concerning the DoD's ability to assess non-Federal networks and systems, we correctly attributed the comment to the Naval Information Warfare Systems Command Program Counsel in this report.

### *USTRANSCOM Comments*

The USTRANSCOM Chief of Staff, responding for the USTRANSCOM Contracting Officer, disagreed that the use of the word "verify," as used in the report, could be accomplished through only on-site visits to contractor facilities. The Chief of Staff stated that, while DoD guidance allows on-site Government assessments of contractors' compliance with NIST SP 800-171, DFARS clause 252.204-7012 does not provide a contractual means to assess a contractor's system until a cyber incident occurs.<sup>29</sup> He also stated that the DoD previously decided to not require on-site compliance assessments during an industry information session on June 23, 2017, and; therefore, all USTRANSCOM contracts were written based on that decision. He stated that any contract modifications to verify compliance with NIST SP 800-171 requirements would require an agreement from all contractors involved. In addition, the Chief of Staff stated that USTRANSCOM was not resourced to conduct on-site visits to verify NIST SP 800-171 compliance.

### *Our Response*

We used the term "verify" in conjunction with performing on-site visits because the visits are the most effective way to observe the security controls implemented by contractors. In November 2018, the Undersecretary of Defense for Acquisition and Sustainment issued a memorandum that allows DoD Components and requiring activities to conduct on-site assessments of contractor information systems compliance with NIST SP 800-171 requirements for contracts that include DFARS clause 252.204-7012 at any time, not only after a cyber incident occurs. In addition, it was not our intent for USTRANSCOM to conduct on-site assessments

<sup>29</sup> The DoD guidance that the USTRANSCOM Chief of Staff referred to is the Undersecretary of Defense for Acquisition and Sustainment Memorandum, "Guidance for Assessing Compliance and Enhancing Protections Required by DFARS Clause 252.204.7012, Safeguarding Covered Defense Information and Cyber Incident Reporting," November 2018.

at every contractor facility, but rather conduct on-site assessments based on risk. We contacted Defense Pricing and Contracting Program officials concerning the decision not to require on-site compliance assessments. The officials stated that their consistent message is that if DoD Components want more stringent requirements than what the DFARS Clause 252.204-7012 includes (such as on-site compliance assessments), then those Components must add the more stringent requirements to the solicitation and contract.

## Recommendations, Management Comments, and Our Response

### ***Recommendation A.1***

**We recommend that the DoD Chief Information Officer, in coordination with Defense Pricing and Contracting, implement or revise policy to require all systems and networks that maintain DoD information, including those owned by contractors that maintain DoD information to:**

- a. Use strong passwords that, at a minimum, meet DoD password length and complexity requirements.**
- b. Configure their systems and networks to align with DoD requirements for locking after 15 minutes of inactivity and 3 unsuccessful logon attempts.**

### ***DoD Principal Deputy Chief Information Officer Comments***

The Principal Deputy Chief Information Officer, responding for the DoD Chief Information Officer, disagreed, stating that requiring stronger passwords and configuring systems to lock automatically after 15 minutes of inactivity and three unsuccessful logon attempts was not appropriate because these requirements were applicable to national security systems and not contractor-owned systems and networks.<sup>30</sup> The Principal Deputy stated that the stronger requirements that the DoD OIG requested were defined in the Committee on National Security System Instruction 1253, "Security Categorization and Control Selection for National Security Systems."<sup>31</sup> In addition, the Principal Deputy stated that title 32 Code of Federal Regulation (CFR) section 2002 (2016), "Controlled Unclassified Information," prohibits agencies from adding specific requirements to ensure a

<sup>30</sup> A national security system is an information system used or operated by the U.S. Government, its contractors, or its agents that contains classified information or involves intelligence and cryptologic activities related to national security, command and control of military forces, equipment that is an integral part of a weapon or weapons system, or is critical to meeting military or intelligence missions.

<sup>31</sup> Committee on National Security System Instruction No. 1253, "Security Categorization and Control Selection for National Security Systems," March 27, 2014.

single standard was used in safeguarding CUI.<sup>32</sup> Furthermore, the Principal Deputy stated that implementing the recommendations was contrary to the purpose of Executive Order 13556 to establish an open and uniform program managing information that requires safeguarding and dissemination controls and eliminate agency-specific policies, procedures, and marking requirements.<sup>33</sup>

### *Our Response*

Comments from the Principal Deputy did not address the specifics of the recommendations; therefore, the recommendations are unresolved. Although we agree that stronger requirements are defined in the Committee on National Security System Instruction 1253, the 32 CFR does not prohibit agencies from requiring more stringent requirements to protect CUI. Specifically, 32 CFR sec. 2002.14 (2016) requires agencies to implement NIST SP 800-171 to establish security requirements to protect CUI. The CFR also states that agencies MAY NOT **[emphasis added]** implement safeguarding or dissemination controls for CUI OTHER THAN THOSE CONTROLS CONSISTENT **[emphasis added]** with the CUI Program, as defined by Executive Order 13556. However, 32 CFR sec. 2002.14 (2016) allows agencies to specify data that requires more stringent security controls.<sup>34</sup> Specifically, agencies can designate data as basic, specified, or a hybrid of basic and specified controls.<sup>35</sup> According to the CUI Registry, for contracts that include DFARS clause 252.204-7012 and involves the contractor handling CUI, agencies can add specific requirements for safeguarding CUI.<sup>36</sup> Therefore, the DoD Chief Information Officer can require contractors that maintain CUI on their systems and networks to implement more stringent password and lockout controls if the DoD or a DoD Component determines that the loss of confidentiality, integrity, or availability of DoD information could be expected to have a serious adverse effect on organizational assets or individuals.

Therefore, the Principal Deputy should provide additional comments on the final report to clarify how the recommendations conflict with or are contrary to 32 CFR and Executive Order 13556, or how the DoD Chief Information Officer will implement the recommendations as stated.

<sup>32</sup> Title 32 Code of Federal Regulation section 2002, "Controlled Unclassified Information," 2016. The CUI Program established policy for designating, handling, and decontrolling information that qualifies as CUI. The program is designed to standardize the way the executive branch handles information that requires protection under laws, regulations, or Government-wide policies.

<sup>33</sup> Executive Order 13556, "Controlled Unclassified Information," November 4, 2010.

<sup>34</sup> 32 CFR sec. 2002.4(r) (2016), "Controlled Unclassified Information Specified."

<sup>35</sup> CUI Basic is information that requiring or permitting agencies control or protect but does not provide specific controls. CUI Specific is information that requiring or permitting agencies control or protect, and provide specific controls for doing so.

<sup>36</sup> DFARS clause 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting."

*DOT&E Principal Deputy Director Comments*

Although not required to comment, the DOT&E Principal Deputy Director agreed with the recommendations.

*Defense Contract Management Agency Director Comments*

Although not required to comment, the Defense Contract Management Agency Director disagreed with the recommendation, stating that the recommendation for password length and complexity exceeded the required security controls outlined in NIST SP 800-171. He stated that the recommendation may be sound, but that the DoD OIG should provide the recommendations to the NIST for possible inclusion in future revisions of the standards.

*Our Response*

As previously stated, 32 CFR sec. 2002.14 (2016) allows agencies to specify data that requires more stringent security controls. For contracts that include DFARS clause 252.204-7012 and involve CUI, the DoD Chief Information Officer can require contractors to implement more stringent password and lockout controls if the DoD or a DoD Component determines that the loss of confidentiality, integrity, or availability of DoD information could be expected to have a serious adverse effect on organizational assets or individuals. Therefore, DoD Component contracting offices and requiring activities are not precluded from requiring contractors to configure their passwords to align with DoD password length and complexity requirements. If DoD Components determine that the disclosure of the information maintained by contractors would not have an adverse effect, then DoD Components should not include the DFARS clause in the contracts and contractors should not mark the information as CUI. Contracting offices and requiring activities should be using all available measures to protect the DoD's information and technologies in the hands of DoD contractors. We typically do not make recommendations to Federal government agencies outside of the DoD, such as the NIST. However, we encourage the DoD Chief Information Officer and the Defense Contract Management Agency Director to work with the NIST to revise policy related to strong passwords and minimum system locks for system inactivity and failed logon attempts. We will also work with the DoD Chief Information Officer to clarify the expectations of 32 CFR and Executive Order 13556 so that the DoD Chief Information Officer can implement the recommendations as stated.

## **Recommendation A.2**

**We recommend that the Principal Director for Defense Pricing and Contracting, in coordination with the appropriate DoD Component responsible for developing policy:**

- a. Revise its current policy to require DoD Component contracting offices, as part of the Request for Proposal and source selection processes, and requiring activities, during the performance of the contract, to assess whether contractors comply with the National Institute of Standards and Technology requirements for protecting controlled unclassified information before contract award and throughout the contracts' period of performance.**
- b. Develop and implement policy requiring DoD Component contracting offices and requiring activities to maintain an accurate accounting of contractors that access, maintain, or develop controlled unclassified information as part of their contractual obligations.**
- c. Revise its current policy to include language that will require DoD Component contracting offices and requiring activities to validate contractor compliance with National Institute of Standards and Technology Special Publication 800-171 requirements.**
- d. Require DoD Component contracting offices, in coordination with DoD requiring activities, to develop and implement a risk-based process to verify that contractors comply with the Defense Federal Acquisition Regulation Supplement clause 252.204-7012 for protecting controlled unclassified information.**
- e. Require DoD Component contracting offices, in coordination with DoD requiring activities, to take corrective actions against contractors that fail to meet the National Institute of Standards and Technology and contract requirements for protecting controlled unclassified information.**

### ***DCP Acting Principal Director Comments***

The DPC Acting Principal Director agreed, stating that the DPC requires offerors to represent that they will implement NIST SP 800-171 security requirements as part of the Request for Proposal and source selection processes. The Acting Principal Director also stated that the February 5, 2019, memorandum from the Under Secretary of Defense for Acquisition and Sustainment directed the Defense Contract Management Agency, for contracts it administers, to assess contractor compliance with NIST SP 800 171 requirements. The Acting Principal Director stated that, from June through September 2019, the Defense Contract Management Agency would lead a pilot program to provide a strategic, DoD-wide approach for assessing

contractor compliance with NIST SP 800-171 requirements. After completing the pilot program, the Acting Principal Director stated that DPC would work with, among others, the Defense Contract Management Agency, DoD Components, and the DoD Chief Information Officer to:

- determine how to use the results before contract award,
- revise DoD policy accordingly,
- develop a risk-based process that uses a common methodology to assess contractor compliance with NIST 800-171 requirements, and
- update DFARS clause 252.204-7008, "Compliance with Safeguarding Covered Defense Information Controls," October 2016.

The Acting Principal Director also stated that the DPC used enterprise contract data to track contracts that included DFARS clause 252.204-7012 and provide DoD Components with a quarterly update of contractors subject to DFARS clause 252.254-7012 requirements. Furthermore, the Acting Principal Director agreed with the need for DoD Components to take corrective action against contractors that fail to meet NIST SP 800-171 and contract requirements for protecting CUI. The Acting Principal Director stated that DoD Components are authorized to implement any or all of the penalties and remedies for noncompliance with the DFARS clause and NIST requirements. The Acting Principal Director further stated that the implementation of DoD-wide approach for assessing contractor compliance with the DFARS clause and NIST requirements would enable the Defense Contract Management Agency and any contract administering organization to apply penalties and remedies when warranted.

### *Our Response*

Comments from the Acting Principal Director addressed all specifics of the recommendations; therefore, the recommendations are resolved but remain open. We will close the recommendations once the Acting Principal Director provides the revised or new policies and procedures that establishes a risk-based process for assessing contractor compliance with NIST SP 800-171 requirements before contract award and throughout the contract's period of performance. In addition, the Acting Principal Director should provide the quarterly lists of contractors subject to DFARS clause 252.201-7012, the revised contractual language included in DFARS clause 252.204-7008, and the list of penalties and remedies that DoD Components could apply to contractors that fail to meet NIST and contract requirements.



### *DOT&E Principal Deputy Director Comments*

Although not required to comment, the DOT&E Principal Deputy Director stated that assessing contractor compliance with NIST requirements before contract award and throughout the contract's period of performance was a reasonable action for protecting CUI. The Principal Deputy Director acknowledged; however, that DOT&E and other smaller DoD Components were not staffed to conduct on-site assessments and, therefore, suggested using independent organizations, such as DCSA, to verify compliance. He stated that DOT&E would use the independent assessment results to develop and implement corrective action plans when required.

### *Our Response*

We acknowledge that smaller DoD agencies such as DOT&E may not have the resources to conduct on-site assessments of all contractors' compliance with NIST. The intent of the recommendations are for DoD Components to develop and implement a risk-based plan for overseeing and conducting on-site assessments of their contractors' compliance with the NIST requirements.

### **Recommendation A.3**

**We recommend that the Assistant Secretary of the Air Force (Acquisition, Technology & Logistics); Director of Acquisitions for the Missile Defense Agency; and Contracting Officers for the U.S. Army, U.S. Navy, U.S. Cyber Command, U.S. Transportation Command, Defense Contract Management Agency, Office of the Director of Operational Test and Evaluation, and Defense Microelectronics Activity, in coordination with DoD requiring activities, develop and implement a plan to verify that contractors correct the weaknesses identified in this report related to:**

- a. using multifactor authentication;**
- b. mitigating vulnerabilities in a timely manner;**
- c. protecting and monitoring data on removable media;**
- d. documenting and tracking cybersecurity incidents;**
- e. using an automatic system lock after inactivity or unsuccessful logon attempts;**
- f. implementing physical security controls;**
- g. generating system activity reports; and**
- h. requiring and maintaining justification for accessing systems that contain controlled unclassified information.**

*Deputy Assistant Secretary of the Army (Procurement), Office of the Assistant Secretary of the Army (Acquisition, Logistics, and Technology) Comments*

The Deputy Assistant Secretary of the Army (Procurement), Office of the Assistant Secretary of the Army (Acquisition, Logistics, and Technology), responding for the U.S. Army Corps of Engineers Contracting Officer, agreed, stating that the Corps of Engineers was developing a plan to ensure contractors that maintain CUI implemented NIST SP 800-171 security controls. However, the Deputy Assistant Secretary stated that overseeing and monitoring the contractor's network and systems could be costly.

*Our Response*

Comments from the Deputy Assistant Secretary of the Army (Procurement) partially addressed the specifics of the recommendations; therefore, the recommendations are unresolved. Although the Deputy Assistant Secretary stated that the Corps of Engineers was developing a plan to ensure contractors that maintain CUI implemented NIST SP 800-171 security controls, she did not state how the Corps of Engineers would verify that Contractor D corrected identified weaknesses. Therefore, the Deputy Assistant Secretary should provide additional comments describing how the Corps of Engineers will verify that Contractor D corrected those weaknesses.

*DASN (Research, Development, Test, and Evaluation) Comments*

The DASN (Research, Development, Test, and Evaluation), responding for the U.S. Navy Contracting Officer, neither agreed nor disagreed, stating that the Navy was working with the Office of the Secretary of Defense to develop DoD-wide policy for implementing DFARS clause 252.204-7012 requirements, including NIST SP 800-171 standards. He stated that the implementation of policy would meet the intent of the recommendations.

*Our Response*

Comments from the DASN (Research, Development, Test, and Evaluation) did not address the specifics of the recommendation; therefore, the recommendations are unresolved. Although the DASN acknowledged that the Navy was working with the Office of the Secretary of Defense to develop policy for ensuring contractor compliance with DFARS clause 252.204-7012 requirements, he did not address actions the Naval Information Warfare Systems Command will take to ensure Contractor B corrected identified weaknesses. The DASN should provide additional comments describing how the Naval Information Warfare Systems Command will verify that Contractor B corrected those weaknesses.

### *Principal Deputy Assistant Secretary of the Air Force (Acquisition, Technology, and Logistics) Comments*

The Principal Deputy Assistant Secretary of the Air Force (Acquisition, Technology, and Logistics), responding for the U.S. Air Force Contracting Officer, neither agreed nor disagreed with the recommendations, stating that the recommendation should be redirected to the DoD Chief Information Officer, in coordination with the Military Services, DoD agencies, and requiring activities because Contracting Officers were not cybersecurity experts. However, she stated that, once a plan or policy is developed, contracting officers will be able to hold contractors accountable.

### *Our Response*

Comments from the Principal Deputy Assistant Secretary of the Air Force (Acquisition, Technology, and Logistics) did not address the specifics of the recommendations; therefore, the recommendations are unresolved. Specifically, she did not address actions that the Air Force will take to ensure Contractor E corrected identified weaknesses. We disagree that contracting officers cannot assess whether contractors comply with NIST SP 800-171 requirements. The Undersecretary of Defense for Acquisition and Sustainment issued a memorandum in November 2018 that provides guidance for assessing contractors' compliance with cybersecurity protections required by DFARS clause 252.204.7012. Contracting officers and requiring activities should use the November 2018 guidance to hold contractors accountable for not complying with DFARS and NIST requirements. Therefore, the Principal Deputy Assistant Secretary of the Air Force should provide additional comments describing how the Air Force will verify that Contractor E corrected identified weaknesses.

### *USTRANSCOM Chief of Staff Comments*

The USTRANSCOM Chief of Staff, responding for the USTRANSCOM Contracting Officer, agreed, stating that USTRANSCOM would verify that Contractor F implemented multifactor authentication for internal and external users, mitigated vulnerabilities in a timely manner, and configured systems to lock automatically after a defined period of inactivity and unsuccessful login attempts. The Chief of Staff acknowledged that Contractor F did not use multifactor authentication for users within its facilities, but was implementing a pilot program on the practicality and impact of implementing multifactor authentication enterprise-wide, including internal and external users connecting to its network. The Chief of Staff stated that the contracting officer would further coordinate NIST SP 800-171 compliance

*The Chief of Staff stated that the contracting officer would further coordinate NIST SP 800-171 compliance with Contractor F by July 1, 2019.*

with Contractor F by July 1, 2019.<sup>37</sup> In addition, the Chief of Staff agreed that USTRANSCOM would verify that Contractor F mitigated vulnerabilities in a timely manner. However, he stated that USTRANSCOM needed until

July 1, 2019, to further coordinate corrective actions with Contractor F because a previous memorandum from the DoD OIG did not identify the issue as a weakness. Furthermore, the Chief of Staff stated that Contractor F locked user accounts automatically after 20 minutes of inactivity and after 5 unsuccessful login attempts based on the contractor's assessment of risk. As such, he stated that Contractor F's actions complied with NIST SP 800-171 requirements and, therefore, Contractor F was not required to implement more stringent standards until contractual requirements changed.

The Chief of Staff disagreed that Contractor F did not encrypt information on removable media, stating that, on March 4, 2019, Contractor F clarified that it scanned USB devices connected to the network to ensure the network was protected from malware. The Chief of Staff also stated that Contractor F's POA&M identified that it had a media protection policy and implemented media protection standards. Furthermore, he stated that DoD guidance, issued on November 6, 2018, states that implementing a policy and process on using removable media and monitoring compliance addresses the intent of NIST SP 800-171 requirements on controlling the use of removable media on system components.<sup>38</sup> The Chief of Staff stated that, until the DoD Chief Information Officer and Director for Defense Pricing and Contracting require additional controls through an updated contractual clause, Contractor F's mitigation approach meets the intent of the control for protecting removable media.

### *Our Response*

Comments from the Chief of Staff addressed all specifics of Recommendations A.3.a and A.3.b; therefore, those recommendations are resolved but remain open. We will close Recommendations A.3.a and A.3.b once the Chief of Staff provides the results of Contractor F's pilot program for implementing multifactor authentication internally at all contractor facilities and documentation showing that USTRANSCOM verified that Contractor F took action, based on the results of the pilot, to implement a solution company-wide. We also require documentation showing that Contractor F

<sup>37</sup> The USTRANSCOM followed up with Contractor F on June 17, 2019, and determined that Contractor F did not take further action to correct weaknesses related to multifactor authentication and mitigating vulnerabilities.

<sup>38</sup> The guidance the USTRANSCOM Chief of Staff cited is the "Guidance for Assessing Compliance of and Enhancing Protections for a Contractor's Internal Unclassified Information System," November 8, 2018.

mitigated its outstanding vulnerabilities. We acknowledge in this report that Contractor F complied with lock out requirements outlined in NIST SP 800-171. Although the Chief of Staff stated that the USTRANSCOM was not aware of issues with Contractor F's vulnerability management program, the DoD OIG provided USTRANSCOM with a discussion draft on March 21, 2019, that included vulnerability management weaknesses applicable to Contractor F.

Although the Chief of Staff disagreed with Recommendation A.3.c, actions taken by Contractor F met the intent of the recommendation; therefore, the recommendation is resolved but remains open. We will close the recommendation once the Chief of Staff provides documentation, such as a screenshot of the configuration settings, showing that USB devices are scanned when connected to Contractor F's network.

### *U.S. Cyber Command Chief of Staff Comments*

The U.S. Cyber Command Chief of Staff, responding for the U.S. Cyber Command Contracting Officer, agreed, stating that the Acquisition and Program Management Divisions verified that Contractor A corrected the weaknesses identified in the report on March 22, 2019.

### *Our Response*

Comments from the Chief of Staff addressed all specifics of the recommendations. Furthermore, the Chief of Staff provided documentation confirming that U.S. Cyber Command verified that Contractor A corrected identified weaknesses. Therefore, Recommendations A.3.b and A.3.e are closed and no further comments are required.

### *DOT&E Principal Deputy Director Comments*

The DOT&E Principal Deputy Director, responding for the DOT&E Director, agreed to verify that Contractor G used multifactor authentication; mitigated vulnerabilities in a timely manner; implemented physical security controls; generated system activity reports; and required and maintained written justification to support the need for system access. The Principal Deputy Director stated that Contractor G was developing a process to document and track outstanding vulnerabilities and remediation plans, and it would reduce or eliminate existing vulnerabilities by August 15, 2019. The Principal Deputy Director also stated that Contractor G would provide regular updates on its progress to correct deficiencies to the DOT&E throughout the process.

However, the Principal Deputy Director disagreed that Contractor G needed to protect and monitor data on removable media; document and track cybersecurity incidents; and automatically lock systems after periods of inactivity or unsuccessful logon attempts. Specifically, the Principal Deputy Director stated that Contractor G

was compliant with protecting data stored on removable media because it used encryption tools and implemented procedures to protect data when using removable media. However, the Principal Deputy Director stated that Contractor G acknowledged that it relied on staff adhering to its policies and, therefore, would strengthen staff training and recommunicate the contractor's policies to all staff by September 1, 2019.

In addition, the Principal Deputy Director stated that Contractor G reported all cyber incidents to the Defense Cyber Crime Center and tracked the incidents using a local Service Management System. The Principal Deputy Director stated that Contractor G agreed to implement a formal reporting program and use a consolidated, single repository that included comprehensive documentation about security incidents by September 1, 2019. Furthermore, the Principal Deputy Director stated that Contractor G's 30-minute period for locking user accounts automatically balanced the risk of compromise, based on the contractor's physical and operational controls, with business requirements and staff productivity.

### *Our Response*

Comments from the Principal Deputy Director addressed all specifics of Recommendation A.3.b; therefore, the recommendation is resolved but remains open. We will close the recommendation once the Principal Deputy Director provides the approved, updated processes and procedures for addressing vulnerabilities and documentation showing that outstanding vulnerabilities were mitigated by the date agreed to by Contractor G and DOT&E.

Although the Principal Deputy Director disagreed with Recommendations A.3.d and A.3.e, the contractor's planned actions meet the intent of the recommendations; therefore, the recommendations are resolved but remain open. We will close Recommendation A.3.d once the Principal Deputy Director provides the approved processes and procedures for tracking and reporting cyber incidents and documentation from DOT&E showing it verified that Contractor G implemented a consolidated system to record, track, and maintain documentation related to all incidents. We will close Recommendation A.3.e once the Principal Deputy Director provides documentation, such as the risk assessment results, showing that Contractor G assessed and accepted the risks associated with insider threat activities using a period of 30 minutes before its systems and network locked automatically for inactivity.

Comments from the Principal Deputy Director partially addressed the specifics of Recommendation A.3.c; therefore, the recommendation is unresolved. Although the Principal Deputy Director stated that Contractor G would strengthen staff training and reinforce the contractor's policies on encrypting data stored on removable



media, those actions alone will not ensure that all CUI stored on removable media is encrypted. Unless Contractor G implements additional processes to ensure its staff encrypt the information stored on removable media, there is a risk that staff will intentionally or unintentionally fail to encrypt data stored on removable media and, therefore, expose DoD information to malicious actors and unauthorized users if the removable media is compromised. The Principal Deputy Director should provide additional comments on the final report describing how DOT&E plans to verify that Contractor G's actions are sufficient to ensure that staff encrypts CUI stored on removable media.

### *MDA Director Comments*

The MDA Director, responding for the MDA Director of Acquisitions, agreed, stating that DoD policy requires contractors to self-assess compliance with NIST SP 800-171 requirements, develop a system security plan, and develop a POA&M for implementing noncompliant security controls. The Director also stated that neither DFARS clause 252.204-7012 nor DoD policy required Government personnel to conduct on-site reviews of contractor compliance with the NIST security controls, but acknowledged that the Under Secretary of Defense for Acquisition and Sustainment issued guidance in November 2018 that addressed conducting on-site reviews of non-Federal systems. The Director stated that the MDA and Contractor H were working together to improve Contractor's H compliance with DFARS clause 252.204-7012 requirements, noting that Contractor H agreed to an on-site assessment by the MDA Cyber Assistance Team as Contractor H completed corrective actions.

The Director further stated that, after the DoD OIG completed its assessment of Contractor H, the contractor developed a comprehensive corrective action plan in March 2019 to address the DoD OIG's findings. The Director stated that the MDA Procuring Contracting Officer confirmed that Contractor H was on schedule to implement all corrective actions by June 2019. Specifically, the Director stated that Contractor H:

- implemented multifactor authentication for all users at its Huntsville facility and is in the process of implementing multifactor authentication company-wide as well as Public Key Infrastructure for key personnel;
- increased storage capacity and added end-point scanning to its infrastructure to generate system activity reports that enable Contractor H to monitor and report unauthorized system activity and identify and correct vulnerabilities; and
- changed Active Directory group policies to disable the use of USB ports for unapproved devices.

In addition, the Director stated that Contractor H planned to:

- change Active Directory group policies to lock user accounts after three unsuccessful logon attempts and configure accounts to require a 15-character password; and
- implement formal procedures that used standard forms and an automated workflow, which would be documented in its System Security Plan, to ensure users received Data Content Owner's approval before obtaining access.

Furthermore, the Director stated that the MDA actively participated in DoD working groups to develop DoD-wide procedures for conducting on-site assessments of contractor compliance with DFARS clause 252.204-7012 requirements.

### *Our Response*

Comments from the MDA Director addressed all specifics of the recommendations; therefore, the recommendations are resolved but remain open. The Director provided documentation from Contractor H that described the contractor's plans for correcting the weaknesses identified in this report. In addition, MDA's Cyber Assistance Team review will provide MDA assurance that Contractor H's actions address the specific weaknesses identified in this report. We will close the recommendations once the MDA Director provides documentation, such as the results of the MDA Cyber Assistance Team review, showing that the MDA confirmed that Contractor H corrected identified weaknesses.

### *Defense Contract Management Agency Director Comments*

The Defense Contract Management Agency Director partially agreed, stating that the Defense Contract Management Agency would verify contractor compliance with DFARS clause 252.204-7012 requirements. The Director also stated that the Defense Contract Management Agency and other DoD Components would begin implementing a pilot program from June through September 2019 to develop a standard capability assessment process for verifying contractor compliance with applicable requirements.

### *Our Response*

Comments from the Director did not address the specifics of the recommendations; therefore, the recommendations are unresolved. Although the Defense Contract Management Agency is participating in a pilot program to determine an approach for assessing contractor compliance with NIST requirements, the pilot will not specifically address weaknesses identified at Contractor J. The Director should provide additional comments on the final report describing how the

Defense Contract Management Agency will verify that Contractor J corrected the weaknesses related to using multifactor authentication; mitigating vulnerabilities in a timely manner; and protecting and monitoring data on removable media.

### ***Recommendation A.4***

**We recommend that the Director of Acquisition, Missile Defense Agency, verify that Contractor H:**

- a. Transitioned to a third-party service provider where the oversight activities of the provider are feasible.**
- b. Configured all assets on its network to create system activity reports.**
- c. Configured all devices on its network to use multifactor authentication.**

### ***MDA Director Comments***

The MDA Director, responding for the Director of Acquisitions, agreed, stating that DoD policy requires contractors to self-assess compliance with NIST SP 800-171 requirements, develop a system security plan, and develop a POA&M for implementing noncompliant security controls. However, the Director stated that the MDA directly engaged Contractor H to support improved compliance, noting that Contractor H agreed to an on-site assessment by the MDA Cyber Assistance Team. The Director stated that the MDA Procuring Contracting Officer monitored Contractor H's compliance with DFARS clause 252.204-7012 requirements and confirmed that Contractor H completed its self-assessment and developed a system security plan and POA&M that supports a corrective action plan to comply with DFARS clause requirements by June 2019. The Director stated that Contractor H could not terminate the contract with its third-party provider without severe penalties; however, Contractor H:

- installed network equipment and software and transitioned to Voice-Over-Internet Protocol phones in May 2019 to enable Contractor H to monitor and log activity on its network instead of relying on a third-party service provider for network perimeter defenses;
- implemented multifactor authentication for all users at its Huntsville facility and is in the process of implementing multifactor authentication company-wide as well as Public Key Infrastructure for key personnel; and
- was in the process of increasing storage capacity and adding end-point scanning to its infrastructure to generate system activity reports that enable Contractor H to analyze, monitor, and report unauthorized system activity on all devices.

In addition, the Director stated that the MDA actively participated in DoD working groups to develop DoD-wide procedures for conducting on-site assessments of contractor compliance with DFARS clause 252.204-7012 requirements.

### *Our Response*

Comments from the MDA Director addressed all specifics of the recommendations. Recommendations A.4.b and A.4.c are resolved but remain open. We will close Recommendations 4.b and 4.c once the MDA Director provides documentation, such as the results of the MDA Cyber Assistance Team review, showing that the MDA confirmed that Contractor H corrected identified weaknesses. The Director provided documentation from Contractor H that describes the contractor's plans for configuring its network to create system activity reports and implementing multifactor authentication company-wide by June 2019. In addition, the MDA's recommendation, and Contractor H's acceptance, of an MDA Cyber Assistance Team review describes the MDA's plans to verify that Contractor H took corrective actions for identified weaknesses. Furthermore, the Director provided documentation from the MDA Procuring Contracting Officer confirming that Contractor H implemented technical solutions to monitor its network perimeter instead of relying on another network service provider for these services. Therefore, Recommendation A.4.a is closed and no further comments are required.

### **Management Comments Required**

The Contracting Officer, Defense Microelectronics Activity, did not respond to the recommendations in the report. Therefore, the recommendations are unresolved. We request that the Contracting Officer provide comments on the final report.

## Finding B

### ~~(FOUO)~~ Contractor C [REDACTED]

~~(FOUO)~~ A DoD Component contracting office and Contractor C did not take appropriate action to [REDACTED]. Specifically, Contractor C did not properly store and transmit [REDACTED]. Contractor C sent a contract deliverable that [REDACTED] to a contracting officer's representative on the DTRA [REDACTED]. Contractor C also sent the [REDACTED] [REDACTED]. Although the DoD requires contractors to protect classified information, neither DTRA nor Contractor C took prompt action to report and address the spillage of classified DoD information to unclassified environments.

~~(FOUO)~~ As a result, [REDACTED] [REDACTED]. The DoD has an obligation to verify that unauthorized access to [REDACTED] information is effectively prevented. This obligation includes immediately communicating any reports of [REDACTED] [REDACTED]. A compromise of [REDACTED] presents a threat to national security and may damage intelligence or operational capabilities; lessen the DoD ability to protect critical information, technologies, and programs; or reduce the effectiveness of DoD management.

### ~~(FOUO)~~ Events Leading to the [REDACTED]

~~(FOUO)~~ According to a DTRA investigation report issued in December 2016, a Contractor C employee developed a monthly status report (the report) in November 2016 which [REDACTED] [REDACTED]. The investigation report also stated that, although the employees had concerns that the [REDACTED], the employee still transmitted the information to at least two other Contractor C employees through the DTRA [REDACTED]. One of the two employees forwarded the information to another Contractor C employee's [REDACTED] [REDACTED]; that employee then forwarded the report [REDACTED] [REDACTED]. When Contractor C finally forwarded the report [REDACTED] to the DTRA contracting officer representative, DTRA determined that the report included [REDACTED].

(FOUO) The actions by Contractor C's employees resulted in a [REDACTED]

[REDACTED]  
[REDACTED].<sup>39</sup>

**(FOUO) DTRA's Investigation of the [REDACTED]**

(FOUO) DTRA's investigation of the [REDACTED], which began on November 28, 2016, included interviewing Contractor C employees involved in the incident. The investigation report concluded that the [REDACTED] was contained and remediated; therefore, the risk of [REDACTED]. However, the investigation did not include an assessment of the risk of [REDACTED]. The investigation report recommended additional actions to sanitize Contractor C's [REDACTED] involved in the security incident but not the [REDACTED]. In fact, DTRA's investigation officer recommended that DTRA not engage the [REDACTED]. However, DTRA did not verify that Contractor C [REDACTED] and, as of September 2018, [REDACTED].

**(FOUO) [REDACTED]**

(FOUO) As a result of our follow up activities and this audit, in September 2018, Contractor C identified [REDACTED]. In October 2018, we verified that Contractor C successfully [REDACTED]. DCSA guidance states that a cleared Defense contractor's field security officer is required to notify the appropriate security officials where [REDACTED]. However, for uncleared companies, [REDACTED], the DCSA guidance states that contractors should not notify the company [REDACTED].<sup>40</sup> As of February 2019, Contractor C has yet to take action to [REDACTED]. The investigation concluded that Contractor C employees were negligent because the sender of the

<sup>39</sup> (FOUO) [REDACTED]

<sup>40</sup> DSS Office of the Designated Approving Authority, "Manual for the Certification and Accreditation of Classified Systems Under the National Industrial Security Program Operating Manual (NISPOM)," Version 3.2, November 15, 2013, prescribes requirements, restrictions, and other safeguards to prevent unauthorized disclosure of classified information.



(FOUO) [REDACTED]  
[REDACTED]  
[REDACTED].

(FOUO) Although DTRA personnel stated that they informed Contractor C that the information included in the report was [REDACTED], aside from directing Contractor C personnel to [REDACTED] [REDACTED], DTRA did not follow up with Contractor C to ensure actions were taken to [REDACTED]. Instead, DTRA officials stated that they relied on the contractor to contact DCSA [REDACTED].<sup>41</sup>

(FOUO) DCSA oversees the security of classified information managed by DoD contractors. DCSA requires contractors to execute a DCSA-approved classified spillage cleanup plan when a classified spillage occurs. The plan requires all contaminated computing environments to be included in the cleanup procedures. It also requires the contractor's field security officer—[REDACTED]  
[REDACTED]. Between November 2016 and September 2018, neither Contractor C nor DTRA notified DCSA of the [REDACTED]  
[REDACTED]. Contractor C officials stated that they did not [REDACTED]  
[REDACTED]. Although Contractor C stated that the information was [REDACTED], DTRA officials stated that the [REDACTED]. Contractor C officials also disagreed that DTRA provided them with the results of the [REDACTED]  
[REDACTED]. While DTRA did not provide the [REDACTED] to Contractor C, a DTRA contracting officer's representative did notify Contractor C on February 10, 2017, via e-mail, that the [REDACTED]  
[REDACTED].

(FOUO) The DTRA Security Division Chief acknowledged that DTRA's incident reporting and response procedures did not ensure that its contractors notified DCSA when a security incident on a contractor network occurred. As a result of the audit, the Security Division Chief stated that DTRA was reviewing its procedures to identify improvements to its processes to regularly coordinate with DCSA on security incidents involving its contractors. DTRA officials further noted that, after notifying DCSA in October 2018 about the 2016 security incident, DCSA [REDACTED].

<sup>41</sup> (FOUO) The DCSA provides guidance to contractors on how to mitigate classified information spillages.

## Exposing Classified DoD Information Threatens National Security

Contractors use classified information to produce services or products for the DoD. DCSA requires contractors to execute a DCSA-approved classified spillage cleanup plan when a classified spillage occurs on contaminated computing environments. DCSA also requires the contractors to notify appropriate security personnel to coordinate cleanup actions involving other sites or networks. Protecting classified information, whether in the hands of the DoD or contractors, is essential to maintaining security and achieving mission success in DoD operational and warfighting environments. Prompt reporting of security incidents ensures that such incidents are properly investigated and the necessary actions are taken to negate or minimize the adverse effects of an actual loss or unauthorized disclosure of classified information. The DoD must ensure that its contractors make the security of classified information a priority. The compromise of classified information presents a threat to National security, may damage intelligence or operational capabilities, and lessens the ability of the DoD and its contractors to protect critical information, technologies, and programs.

## Recommendations, Management Comments, and Our Response

### **Recommendation B.1**

**We recommend that the Director for Contract Policy and Oversight, Defense Threat Reduction Agency:**

- a. ~~(FOUO)~~ **Revise its process for monitoring security incidents, [REDACTED], to verify that contractors took the appropriate steps to identify, respond to, and report security incidents that involve DoD data.**

### *DTRA Information Integration and Technology Services Director and Chief Information Officer Comments*

~~(FOUO)~~ The DTRA Information Integration and Technology Services Director and Chief Information Officer, responding for the Contract Policy and Oversight Director, partially agreed, stating that DTRA's Chief of Security was responsible for monitoring security incidents, [REDACTED]. The Director stated that the Chief of Security was working with the DTRA Incident Response Team to revise its Negligent Disclosure of Classified Information instruction and form by June 30, 2019, to ensure that contractors notify appropriate contracting officers and the DCSA of a security incident.

### *Our Response*

Although the Director only partially agreed, her comments addressed all specifics of the recommendation; therefore, the recommendation is resolved but will remain open. We will close the recommendation once the Director provides the revised Negligent Disclosure of Classified Information Spillage security instruction and corresponding reporting form and we verify that the instruction addresses steps to ensure that contractors identify, respond to, and report security incidents that involve DoD data. The Director should also provide evidence that the instructions were disseminated to responsible parties.

- b. ~~(FOUO)~~ Review the performance of the contracting officer responsible for monitoring the 2016 security incident identified in this report and consider administrative action, as appropriate, for not ensuring that Contractor C took actions to [REDACTED].

### *DTRA Information Integration and Technology Services Director and Chief Information Officer Comments*

~~(FOUO)~~ The DTRA Information Integration and Technology Services Director and Chief Information Officer, responding for the Contract Policy and Oversight Director, partially agreed, stating that the Contract Policy and Oversight Director reviewed the contracting officer's performance and found no reason to take administrative action. The Director stated that contracting officers are not trained or required to validate contractor compliance with NIST SP 800-171 requirements. The Director also stated that DoD policy does not require contracting officers to ensure [REDACTED]. However, the Director reiterated that DTRA would update its Negligent Disclosure of Classified Information instruction and corresponding reporting form by June 30, 2019, to ensure that the appropriate DTRA offices received timely notification and contracting officers received relevant information about security incidents.

### *Our Response*

~~(FOUO)~~ We disagree that contracting officers are not required to [REDACTED]. DCSA requires the contractor's field security officer—in this case, Contractor C—to [REDACTED]. In addition, the Undersecretary of Defense for Acquisition and Sustainment's November 2018 memorandum includes guidance for DoD acquisition personnel to establish measures to assess contractor compliance with cybersecurity requirements and states that requiring activities should conduct on-site

(FOUO) assessments of the contractors' information systems to assess and monitor compliance with NIST SP 800-171 requirements. Although the DoD did not require Component contracting offices and requiring activities to verify compliance with the DFARS clause 252.204-7012 and NIST SP 800-171 requirements when the audit began, the November 2018 memorandum provides methods for assessing and verifying contractor compliance with those requirements.

Although the Director partially agreed, her comments addressed all specifics of the recommendation; therefore, the recommendation is closed and no further comments are required.

### ***Recommendation B.2***

(FOUO) We recommend that the Director for the Defense Counterintelligence and Security Agency assess and document the risk of [REDACTED] and, based on the assessment, develop and implement controls to protect the information.

#### ***DCSA Executive Director Comments***

The DCSA Executive Director, responding for the DCSA Director, agreed, stating that the DCSA would include aspects of the recommendation in future incident responses and decisions.

#### ***Our Response***

(FOUO) Comments from the Executive Director partially addressed the specifics of the recommendation; therefore, the recommendation is unresolved. Specifically, the Executive Director did not state how the DCSA planned to assess the risk of [REDACTED] or the controls required when those situations occur. The Executive Director also did not clarify which aspects of the recommendation he would include in future incident responses and decisions. The Executive Director should provide additional comments on the final report describing the actions the DCSA will take to [REDACTED]. In addition, the Executive Director should describe the security controls required to protect that information.

## Appendix A

### Scope and Methodology

We conducted this performance audit from June 2018 through May 2019 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

To understand the process used to protect CUI, we interviewed officials from the Office of the Under Secretary of Defense Intelligence and U.S. Cyber Command. We also interviewed chief executive officers, information technology directors, facility security officers, managers, and system engineers at select contractor locations to identify security protocols implemented to protect CUI. Additionally, we reviewed Federal laws and DoD policy concerning DFARS clause 252.204-7012 and requirements for security controls on unclassified networks and systems to protect CUI.

We selected a nonstatistical sample of 26 of 12,075 contractors with DoD contracts worth \$1 million or more. Of the 26 contractors selected, we assessed 9 contractors to evaluate the security controls that were implemented to protect DoD CUI. We did not assess 17 of the 26 contractors because either the contract had expired, the contractors did not have contracts containing CUI, or the contractors maintained CUI on government-furnished networks and systems and not on their own. We also assessed one contractor, not included in the nonstatistical sample, which we assessed in DODIG-2018-094, to follow up on actions taken to address identified weaknesses. Therefore, we assessed a total of 10 contractors, Contractors A through J, for this audit. The 9 contractors from the nonstatistical sample have 3,374 contracts across 18 of the 24 DoD contracting agencies in our sample. Although 1 of the 10 contractors used government-furnished equipment, we identified a security incident that the Government agency did not fully resolve. We discuss only the security incident for that contractor. Table 4 lists the 10 DoD contractors we visited and the associated contracting agencies.

*Table 4. DoD Component Contracting Offices and Contractors Visited*

DoD Component Contracting Offices	Contractor
U.S. Cyber Command	Contractor A
Naval Information Warfare Systems Command	Contractor B
Defense Threat Reduction Agency *	Contractor C
Department of the Army	Contractor D
Department of the Air Force	Contractor E
U.S. Transportation Command	Contractor F
Director of Operational Test and Evaluation (DOT&E)	Contractor G
Missile Defense Agency	Contractor H
Defense Microelectronics Activity	Contractor I
Defense Contract Management Agency	Contractor J

\*Although Contractor C used government-furnished equipment, we identified a security incident that the Defense Threat Reduction Agency did not fully resolve. We discuss only the security incident for Contractor C in this report.

Source: The DoD OIG.

We also tested security protocols for unclassified networks and systems related to:

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

## Use of Computer-Processed Data

We used computer-processed data that was extracted from FPDS to develop a universe of active contracts. Based on the information that was extracted from FPDS, the DoD Component contracting offices identified their contracts that required contractors to maintain CUI. We used the information from FPDS and identified by the DoD Component contracting offices to develop our universe of active contracts of contractors that maintained CUI. However, the list of contracts was not sufficiently reliable to determine whether contractors maintain CUI on contractor-owned networks and systems because there was no Federal, DoD,



or contractor system in place to track which contracts required contractors to maintain CUI. To assess the reliability of the data, we contacted the 26 contractors that were selected in our nonstatistical sample to verify that the contractor maintained CUI on its networks and systems as part of the identified contract. Of the 26 contractors we selected, 17 responded that they did not maintain CUI as part of their contract efforts because either the contract had expired, the contractors did not have contracts containing CUI, or the contractors maintained CUI on government-furnished networks and systems and not on their own.

## Use of Technical Assistance

The DoD Quantitative Methods Division provided assistance in developing the nonstatistical sampling methodology that we used to select the DoD contractors. (See Appendix B for more details on the sampling methodology).

## Prior Coverage

During the last 5 years, the Government Accountability Office (GAO) and the DoD OIG issued two reports discussing the protection of DoD information maintained on contractor networks and systems. Unrestricted DoD OIG reports can be accessed at <http://www.dodig.mil/reports.html/>.

## GAO

GAO-18-407, “Protecting Classified Information: Defense Security Service Should Address Challenges as New Approach is Piloted,” May 14, 2018

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

**DoD OIG**

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

MDA contractors did not consistently implement security controls and processes to protect classified and unclassified ballistic missile defense system technical information. Specifically, system and network administrators at three contractors that managed ballistic missile defense system technical information on classified networks did not identify and mitigate vulnerabilities on their networks and systems. In addition, two contractors did not conduct risk assessments associated with systems that contained classified ballistic missile defense system technical information. Furthermore, the system and network administrators of the seven contractors that managed ballistic missile defense system technical information on their unclassified networks did not consistently implement system security controls in accordance with DoD requirements for safeguarding Defense information.

## Appendix B

### Sampling Approach

The audit used two different sampling approaches—one approach to select a sample of contractors and DoD Component contracting offices to assess and another approach to select a sample of users at each contractor facility visited to test system access and privileges. The audit team used nonstatistical sampling to ensure representation of different contractors across the population of active DoD contracts.

The audit team obtained a list from the FPDS of 48,646 DoD contracts that were active between June 1, 2015, and June 22, 2018, that were awarded to 12,075 contractors. To obtain the universe of contracts, the audit team generated an FPDS report that included all open DoD contracts greater than \$1 million that were signed or modified no earlier than June 1, 2015, and for which the estimated completion date was after June 22, 2018. The following 24 DoD Components had contracts included in the report.

- Department of the Army
- U.S. Marine Corps
- Department of the Navy
- Department of the Air Force
- U.S. Cyber Command (USCYBERCOM)
- U.S. Special Operations Command (SOCOM)
- U.S. Transportation Command (USTRANSCOM)
- Defense Advanced Research Projects Agency (DARPA)
- Defense Information Systems Agency (DISA)
- Defense Logistics Agency (DLA)
- Defense Threat Reduction Agency (DTRA)
- Defense Security Cooperation Agency (DSCA)
- Missile Defense Agency (MDA)
- Defense Commissary Agency (DCA)
- Defense Finance and Accounting Services (DFAS)
- Defense Contract Management Agency (DCMA)
- Defense Health Agency (DHA)
- Department of Defense Education Activity (DoDEA)
- Defense Media Activity (DMA)

- Defense Microelectronics Activity (DMEA)
- Washington Headquarters Services (WHS)
- Defense Human Resources Activity (DHRA)
- Defense Microelectronics Activity (DMA)
- Defense Counterintelligence and Security Agency (formerly known as Defense Security Service)
- Joint Improvised Explosive Device Defeat Organization
- Uniform Services University of Health Sciences (USUHS)

The audit team conducted a separate data call for all open contracts for the following six DoD Components that did not maintain contract information in the FPDS.

- U.S. Southern Command (USSOUTHCOM)
- U.S. Strategic Command (USSTRATCOM)
- Office of the Director, Operational Test and Evaluation (DTO&E)
- Defense Intelligence Agency (DIA)
- Defense Contract Administration Agency (DCAA)
- North American Aerospace Defense Command

The Office of the Secretary of Defense, DOT&E, and the North American Aerospace Defense Command had a combined total of 17 open contracts, which increased our universe to 48,663 open DoD contracts. The audit team created individual lists of contracts awarded by DoD Component, provided the lists to the respective contracting offices, and requested that each office identify the contracts that require the contractors to process, store, and transmit CUI on their own networks and systems.

The audit team consolidated the responses from the contracting offices and selected a non-statistical sample from the universe of contracts using the “Random” function in Microsoft Excel. The audit team selected the first instance a contractor appeared under a DoD Component in the randomized list. The audit team repeated this methodology for each DoD Component in the list, resulting in a sample of 24 contractors.

## Management Comments

### Deputy Assistant Secretary of the Army (Procurement)



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

SAAL-ZP

MEMORANDUM FOR INSPECTOR GENERAL, DEPARTMENT OF DEFENSE,  
ATTN: [REDACTED], PROGRAM DIRECTOR, 4800 MARK CENTER DRIVE,  
ALEXANDRIA, VIRGINIA 22350-1500

SUBJECT: Audit of Protection of DoD Controlled Unclassified Information on  
Contractor-Owned Networks and Systems, Project No. D2018-D000CR-0171.000

1. On behalf of the Assistant Secretary of the Army (Acquisition, Logistics and Technology), the Office of the Deputy Assistant Secretary of the Army (Procurement) reviewed the subject report and I am providing the official Army position.
2. The Army concurs with the enclosed U.S. Corps of Engineers response to Recommendation A3. The estimated completion date is not later than the 30 June 2020.
3. The point of contact is [REDACTED], [REDACTED], or e-mail: [REDACTED].

Encl

THOMAS.KIM.ME Digitally signed by  
LISIA [REDACTED]  
Date: 2019.06.03 09:11:02 -04'00'

Rebecca Weirick  
Senior Services Manager  
Deputy Assistant Secretary  
of the Army (Procurement)

## Deputy Assistant Secretary of the Army (Procurement) (cont'd)



REPLY TO  
ATTENTION OF

DEPARTMENT OF THE ARMY  
U.S. ARMY CORPS OF ENGINEERS  
441 G STREET, NW  
WASHINGTON, DC 20314-1000

CECT

May 22, 2019

**Project:** D2018-DD2018-D000CR-0171.000

**Objective Title:** DoDIG Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems

**Objective:** To determine whether DoD contractors implemented adequate security controls to protect DoD-controlled unclassified information (CUI) maintained on their networks and systems from internal and external cyber threats. CUI is a designation for identifying unclassified information that requires proper safeguarding in accordance with Federal and DoD guidance.

**Recommendation A3.** Recommend that the Director of Acquisitions for the Missile Defense Agency; and Contracting Officers for the U.S. Army, U.S. Navy, U.S. Air Force, U.S. Cyber Command, U.S. Transportation Command, Defense Contract Management Agency, and Defense Microelectronics Activity, in coordination with DoD requiring activities, develop and implement a plan to verify that contractors correct the weaknesses identified in this report related to:

- a) using multifactor authentication
- b) mitigating vulnerabilities in a timely manner
- c) protecting and monitoring data on removable media
- d) documenting and tracking cybersecurity incidents
- e) utilizing an automatic system lock after inactivity or unsuccessful logon attempts
- f) implementing physical security controls
- g) generating system activity reports; and
- h) requiring and maintaining justification for accessing systems that contain controlled unclassified information.

**Action Taken or planned:** Concur with comment; The U.S. Army Corps of Engineers (USACE) concurs with recommendation A3 and is in the process of developing a plan for contractors to maintain CUI to implement security controls specified in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, to safeguard sensitive information on non-Federal information systems. However, the cost and labor involved in the oversight and monitoring the contractor's network and/or systems could be excessive.



## Deputy Assistant Secretary of the Army (Procurement) (cont'd)

-2-

If you have any questions or concerns, please contact me at  
[REDACTED] or at [REDACTED].

Respectively,

*Richard L. Jenkins*

Richard L. Jenkins  
Chief, Acquisition Support Division  
Directorate of Contracting



## Deputy Assistant Secretary of the Navy (Research, Development, Test, and Evaluation)

### SELECT A CLASSIFICATION

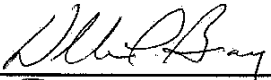
### COMPONENT COORDINATOR RESPONSE

June 7, 2019

**SUBJECT:** DOD OIG DRAFT REPORT, "AUDIT OF PROTECTION OF CONTROLLED UNCLASSIFIED INFORMATION ON CONTRACTOR-OWNED NETWORKS AND SYSTEMS" Choose an item.

On behalf of my Component, my formal response to this issuance is: Nonconcur.  
Consider our nonconcurrency withdrawn if you accept and incorporate comments .

My point of contact for this action is [REDACTED] at [REDACTED]

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

Coordinating Official's Name: William P. Bray  
Coordinating Official's Position Title: DASN(RDT&E)  
Coordinating Official's Component: ASN(RD&A)

DD FORM 818, AUG 2016

SELECT A CLASSIFICATION

## Deputy Assistant Secretary of the Navy (Research, Development, Test, and Evaluation) (cont'd)

**Final  
Report Reference**

UNCLASSIFIED// <del>FOUO</del>						
CONSOLIDATED DoD ISSUANCE COMMENT MATRIX						
DoDIG Draft Report D2018-D000CR-0171, Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems						
Space and Naval Warfare Systems Command (SPAWAR) Comments						
CLASS	#	PAGE	PARA	BASIS FOR NON- CONCUR?	COMMENTS, JUSTIFICATION, AND ORIGINATOR JUSTIFICATION FOR RESOLUTION	COMPONENT AND POC NAME, PHONE, AND E-MAIL
I					[REDACTED]	DASN RDTE STAFF [REDACTED]
I					[REDACTED]	DASN RDTE STAFF [REDACTED]
U					[REDACTED]	SPAWAR Audit Liaison POC: [REDACTED]

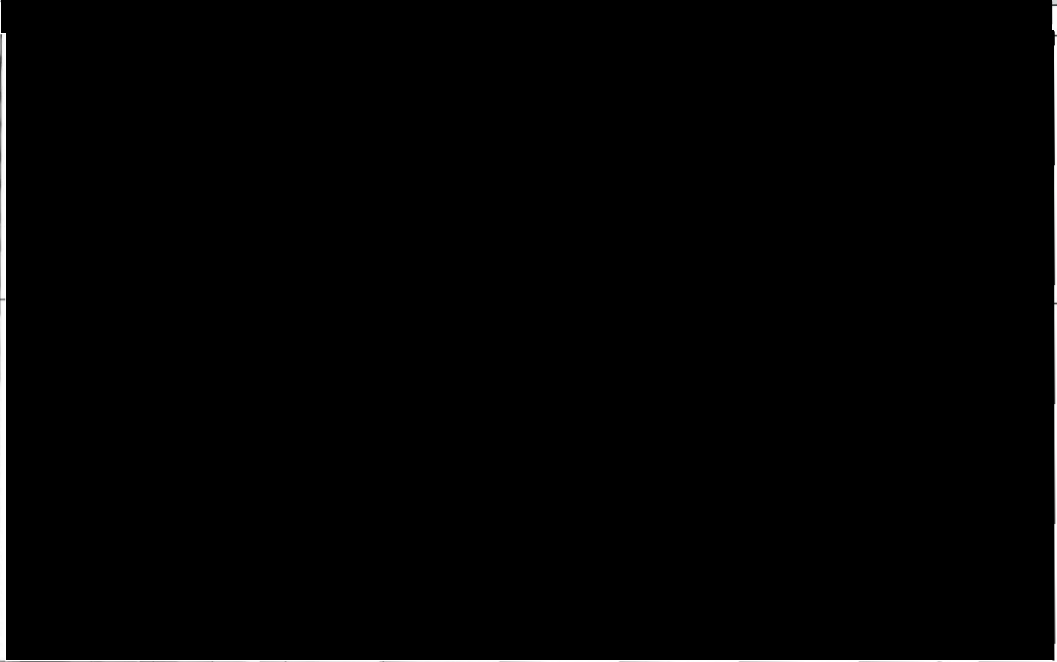


DD FORM 818-1, AUG 2016

SELECT A CLASSIFICATION

2

**Item 2  
on page 41**

## Deputy Assistant Secretary of the Navy (Research, Development, Test, and Evaluation) (cont'd)

<del>UNCLASSIFIED//FOUO</del>						
CONSOLIDATED DoD ISSUANCE COMMENT MATRIX						
DoDIG Draft Report D2018-D000CR-0171, Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems						
Space and Naval Warfare Systems Command (SPAWAR) Comments						
CLASS	#	PAGE	PARA	BASIS FOR NON- CONCUR?	COMMENTS, JUSTIFICATION, AND ORIGINATOR JUSTIFICATION FOR RESOLUTION	COMPONENT AND POC NAME, PHONE, AND E-MAIL
						SPAWAR Audit Liaison POC: 
						SPAWAR Audit Liaison POC: 

DD FORM 818-1, AUG 2016

SELECT A CLASSIFICATION

3

## Deputy Assistant Secretary of the Navy (Research, Development, Test, and Evaluation) (cont'd)

<del>UNCLASSIFIED//FOUO</del> <b>CONSOLIDATED DoD ISSUANCE COMMENT MATRIX</b> DoDIG Draft Report D2018-D000CR-0171, Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems Space and Naval Warfare Systems Command (SPAWAR) Comments						
CLASS	#	PAGE	PARA	BASIS FOR NON- CONCUR?	COMMENTS, JUSTIFICATION, AND ORIGINATOR JUSTIFICATION FOR RESOLUTION	COMPONENT AND POC NAME, PHONE, AND E-MAIL
						SPAWAR Audit Liaison POC: [REDACTED]
						SPAWAR Audit Liaison POC: [REDACTED]

DD FORM 818-1, AUG 2016

SELECT A CLASSIFICATION

4

## Deputy Assistant Secretary of the Navy (Research, Development, Test, and Evaluation) (cont'd)


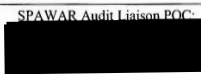
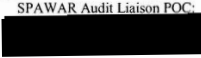
**Final  
Report Reference**

~~UNCLASSIFIED//FOUO~~

**CONSOLIDATED DoD ISSUANCE COMMENT MATRIX**

DoDIG Draft Report D2018-D000CR-0171, Audit of Protection of DoD Controlled  
Unclassified Information on Contractor-Owned Networks and Systems

Space and Naval Warfare Systems Command (SPAWAR) Comments

CLASS	#	PAGE	PARA	BASIS FOR NON- CONCUR?	COMMENTS, JUSTIFICATION, AND ORIGINATOR JUSTIFICATION FOR RESOLUTION	COMPONENT AND POC NAME, PHONE, AND E-MAIL
						SPAWAR Audit Liaison POC: 
						SPAWAR Audit Liaison POC: 

DD FORM 818-1, AUG 2016

SELECT A CLASSIFICATION

5

**Item 9  
on page 27**

**Item 10  
on page 27**

## Deputy Assistant Secretary of the Navy (Research, Development, Test, and Evaluation) (cont'd)

Final  
Report Reference

~~UNCLASSIFIED//FOUO~~

**CONSOLIDATED DoD ISSUANCE COMMENT MATRIX**

DoDIG Draft Report D2018-D000CR-0171, Audit of Protection of DoD Controlled  
Unclassified Information on Contractor-Owned Networks and Systems

Space and Naval Warfare Systems Command (SPAWAR) Comments

CLASS	#	PAGE	PARA	BASIS FOR NON- CONCUR?	COMMENTS, JUSTIFICATION, AND ORIGINATOR JUSTIFICATION FOR RESOLUTION	COMPONENT AND POC NAME, PHONE, AND E-MAIL
						SPAWAR Audit Liaison POC: [REDACTED]
						SPAWAR Audit Liaison POC: [REDACTED]
						SPAWAR Audit Liaison POC: [REDACTED]

DD FORM 818-1, AUG 2016

SELECT A CLASSIFICATION

6

Item 11  
on page 28

Item 12  
on page 28

## Deputy Assistant Secretary of the Navy (Research, Development, Test, and Evaluation) (cont'd)

Final  
Report Reference

Item 13  
on page 30

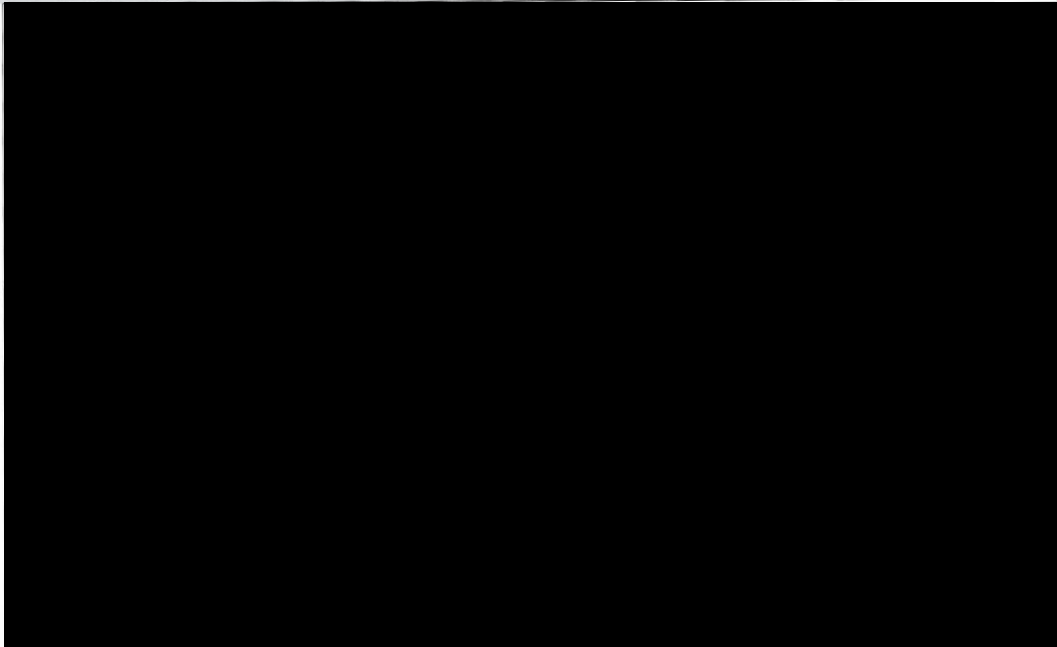
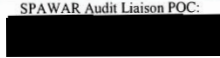
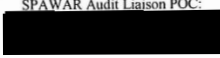
Item 14  
on page 30

~~UNCLASSIFIED//FOUO~~

**CONSOLIDATED DoD ISSUANCE COMMENT MATRIX**

DoDIG Draft Report D2018-D000CR-0171, Audit of Protection of DoD Controlled  
Unclassified Information on Contractor-Owned Networks and Systems

Space and Naval Warfare Systems Command (SPAWAR) Comments

CLASS	#	PAGE	PARA	BASIS FOR NON- CONCUR?	COMMENTS, JUSTIFICATION, AND ORIGINATOR JUSTIFICATION FOR RESOLUTION	COMPONENT AND POC NAME, PHONE, AND E-MAIL
						SPAWAR Audit Liaison POC: 
						SPAWAR Audit Liaison POC: 

DD FORM 818-1, AUG 2016

SELECT A CLASSIFICATION

7



## Deputy Assistant Secretary of the Navy (Research, Development, Test, and Evaluation) (cont'd)

**Final  
Report Reference**

**Item 15  
on page 32**

~~UNCLASSIFIED//FOUO~~

**CONSOLIDATED DoD ISSUANCE COMMENT MATRIX**

DoDIG Draft Report D2018-D000CR-0171, Audit of Protection of DoD Controlled  
Unclassified Information on Contractor-Owned Networks and Systems

Space and Naval Warfare Systems Command (SPAWAR) Comments

CLASS	#	PAGE	PARA	BASIS FOR NON- CONCUR?	COMMENTS, JUSTIFICATION, AND ORIGINATOR JUSTIFICATION FOR RESOLUTION	COMPONENT AND POC NAME, PHONE, AND E-MAIL
						SPAWAR Audit Liaison POC:

DD FORM 818-1, AUG 2016

SELECT A CLASSIFICATION

8

## Deputy Assistant Secretary of the Navy (Research, Development, Test, and Evaluation) (cont'd)

<del>UNCLASSIFIED//FOUO</del>						
CONSOLIDATED DoD ISSUANCE COMMENT MATRIX						
DoDIG Draft Report D2018-D000CR-0171, Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems						
Space and Naval Warfare Systems Command (SPAWAR) Comments						
CLASS	#	PAGE	PARA	BASIS FOR NON- CONCUR?	COMMENTS, JUSTIFICATION, AND ORIGINATOR JUSTIFICATION FOR RESOLUTION	COMPONENT AND POC NAME, PHONE, AND E-MAIL

DD FORM 818-1, AUG 2016

SELECT A CLASSIFICATION

9

## Assistant Secretary of the Air Force (Acquisition, Technology & Logistics)



DEPARTMENT OF THE AIR FORCE  
WASHINGTON DC

21 JUN 2019

OFFICE OF THE ASSISTANT SECRETARY

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL

FROM: SAF/AQ

SUBJECT: Air Force Response to DoD Office of Inspector General, "(FOUO) Draft Report  
Protection of CUI on Contractor-Owned Networks and Systems"

This is the Air Force feedback to the DoDIG Draft Report, "(FOUO) Draft Report -  
Protection of CUI on Contractor-Owned Networks and Systems." SAF/AQ non-concurs to the  
draft report with non-concur comments identified within Tab 2.

A handwritten signature in cursive script, reading "Darlene J. Costello".

DARLENE J. COSTELLO  
Principal Deputy Assistant Secretary of the Air  
Force (Acquisition, Technology & Logistics)

Tab  
CRM DoDIG Draft Report-Protection CUI on CON-S

## Assistant Secretary of the Air Force (Acquisition, Technology & Logistics) (cont'd)

~~FOR OFFICIAL USE ONLY~~  
Template

Item #	Org/ Reviewer	Type C/S/A	Page	Para	Comment	Rationale	Resolution (A/R/P)
1.							
2.							
3.							
4.							
5.							
6.							
7.							
8.							
9.							
10.							
11.							

~~FOR OFFICIAL USE ONLY~~

1

Final  
Report Reference

Item 1  
on page 42

Item 2  
on page 42

Item 3  
on page iv

## Assistant Secretary of the Air Force (Acquisition, Technology & Logistics) (cont'd)

~~FOR OFFICIAL USE ONLY~~

Template

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

~~FOR OFFICIAL USE ONLY~~

2

## U.S. Transportation Command Chief of Staff



### UNITED STATES TRANSPORTATION COMMAND

OFFICE OF THE CHIEF OF STAFF  
508 SCOTT DRIVE  
SCOTT AIR FORCE BASE, ILLINOIS 62225-5357

04 June 2019

#### MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL

FROM: TCCS

SUBJECT: DOD OIG Draft Report for Project No. D2018-D000CR-0171.000, "Audit of the Protection of Controlled Unclassified Information on Contractor-Owned Networks and Systems," dated May 2, 2019.

1. The United States Transportation Command has reviewed the Draft Report and concurs with comments to recommendations A3a, b, and e. United States Transportation Command non-concurs with recommendation A3c. Recommendations A3d, f, g, and h do not contain any findings for a United States Transportation Command contractor.

2. For additional information or assistance, please contact [REDACTED], [REDACTED], at [REDACTED] or DSN [REDACTED] or email: [REDACTED] or [REDACTED].

FLOURNOY,JOHN.C.JR. Digitally signed by  
FLOURNOY,JOHN.C.JR.  
Date: 2019.06.04 08:24:52  
-05'00'  
JOHN C. FLOURNOY, JR.  
Major General, USAF  
Chief of Staff

cc:  
TCAQ  
TCJ6  
TCJA

## U.S. Transportation Command Chief of Staff (cont'd)

2

### DOD IG DRAFT REPORT DATED MAY 2, 2019 D2018-D000CR-0171.000

#### “AUDIT OF PROTECTION OF DOD CONTROLLED UNCLASSIFIED INFORMATION ON CONTRACTOR OWNED NETWORKS AND SYSTEMS”

**RECOMMENDATION A.3:** *We recommend that the Director of Acquisitions for the Missile Defense Agency; and Contracting Officers for the U.S. Army, U.S. Navy, U.S. Air Force, U.S. Cyber Command, U.S. Transportation Command, Defense Contract Management Agency, and Defense Microelectronics Activity, in coordination with DOD requiring activities, develop and implement a plan to verify that contractors correct the weakness identified in this report related to:*

- a. Using multifactor authentication;*
- b. Mitigating vulnerabilities in a timely manner;*
- c. Protecting and monitoring data on removable media;*
- d. Documenting and tracking cybersecurity incidents;*
- e. Utilizing an automatic system lock after inactivity or unsuccessful logon attempts;*
- f. Implementing physical security controls;*
- g. Generating system activity reports; and*
- h. Requiring and maintaining justification for accessing systems that contain controlled unclassified information.*

**USTRANSCOM Response:** Actions taken to date, and those planned in response, are outlined below according to each sub-recommendation.

Note, insofar as the definition of the word “verify” contained in footnote 9 on page 6 of the Draft Report can only be manifested as an on-site visit to the contractor’s facility to make the stated determination, USTRANSCOM disagrees with this definition. While DOD guidance regarding implementation of DFARS 252.204-7012 issued on 6 November 2018 permits on-site government assessment of contractors’ internal unclassified information systems for compliance with NIST SP 800-171, the current terms of the clause do not provide a contractual means to access the contractor’s systems until a cyber-incident has occurred. In fact, any such on-site verification was previously explicitly rejected by DOD in its 23 June 2017 “Industry Information Day” regarding DFARS clause 252.204-7012. Current USTRANSCOM contracts have been written following this guidance. Because these are new requirements, and our strategic transportation contracts are IDIQ contracts, any such modification requiring verification will have to be agreed to by all contractors involved. If the DFARS clause changes to require on-site visits, USTRANSCOM will take actions necessary to comply. However, at present, USTRANSCOM is not resourced to conduct on-site visits of this type or magnitude.

**a. RECOMMENDATION A3a.** *Using multifactor authentication;*

**Response:** USTRANSCOM concurs with this recommendation.

On 4 March 2019, USTRANSCOM provided a memo to Contractor F identifying the weaknesses found during the inspection. Contractor F enforces the off-premise use of



## U.S. Transportation Command Chief of Staff (cont'd)

3

multifactor authentication across the company's network. However, Contractor F does not require end users working within physically secure contractor on-premise locations to use multifactor authentication because Contractor F views physical access controls as a compensating control to system access. As a result of (and as noted in) the draft report, Contractor F is reviewing the practicality and impact of fully implementing multifactor authentication use on-premise. A pilot is currently underway in one of Contractor F's on-premise locations, wherein management is reviewing the impact of implementing this control. The Contracting Officer will follow up on the outcome of this pilot and compliance with NIST control 3.5.3 with Contractor F NLT 1 July 2019.

**b. RECOMMENDATION A3b.** *Mitigating vulnerabilities in a timely manner;*

**Response:** USTRANSCOM concurs with this recommendation.

This recommendation was not included in the memorandum received from DOD IG on 7 Dec 2018; therefore, USTRANSCOM has not yet approached Contractor F with this concern. The Contracting Officer will follow up with Contractor F NLT 1 July 2019.

**c. RECOMMENDATION A3c.** *Protecting and monitoring data on removable media;*

**Response:** USTRANSCOM non-concurs with this recommendation.

The DODIG report noted that Contractor F stated it could not encrypt removable media devices because the equipment used with the devices did not support encryption. However, on 4 March 2019, Contractor F clarified that its USB devices are scanned when connected to ensure the network and data are protected from the introduction of malware. In addition, Contractor F's current Plan of Action and Milestones state they have a Media Protection Policy and Media Protection Standard in place. DOD put forth guidance on 6 November 2018 which annotates the following implementation standard is appropriate for NIST control 3.8.7, "A policy and process on allowable use of removable media (e.g., thumb drives, DVDs), including monitoring for compliance, would address this requirement." Absent specific direction from the DOD Chief Information Officer (CIO), through Defense Pricing and Contracting, in the form of an updated clause or mandate, Contractor F's mitigation approach fits the intent of the NIST SP 800-171 control for protection of removable media.

**d. RECOMMENDATION A3d.** *Documenting and tracking cybersecurity incidents;*

**Response:** There were no documented findings for Contractor F (USTRANSCOM contractor) in the report.

**e. RECOMMENDATION A3e.** *Utilizing an automatic system lock after inactivity or unsuccessful logon attempts;*

**Response:** USTRANSCOM concurs with this recommendation.

## U.S. Transportation Command Chief of Staff (cont'd)

4

The report notes that NIST SP 800-171 requires user sessions to lock after a period of inactivity, but does not specify the period. Contractor F made a risk-based decision to configure systems to lock after 20 minutes of inactivity because locking the systems after 15 minutes did not allow personnel adequate time to complete their job tasks. Similarly, the report requires contractors that maintain CUI to limit unsuccessful logon attempts, but does not specify the maximum number of logon attempts. Contractor F again made a risk-based decision to lock user accounts after five unsuccessful logon attempts based on a study of the business impact for unlocking user accounts. Thereafter, the report concludes that because Contractor F assessed the risks and associated impacts of unsuccessful logon attempts, the contractor complied with the intent of NIST SP 800-171. The recommendation was subsequently made to the CIO to revise policy to require all systems and networks that maintain DOD information to configure systems and networks to align with DOD requirements to lock automatically after defined periods of inactivity and logon attempts. Once this guidance is received, USTRANSCOM will incorporate the revised requirement and monitor compliance. In the interim, there is no contractual requirement to go above and beyond what is required by NIST SP 800-171 as incorporated through DFARS 252.204-7012.

**f. RECOMMENDATION A3f.** *Implementing physical security controls;*

**Response:** There were no documented findings for Contractor F (USTRANSCOM contractor) in the report.

**g. RECOMMENDATION A3g.** *Generating system activity reports;*

**Response:** There were no documented findings for Contractor F (USTRANSCOM contractor) in the report.

**h. RECOMMENDATION A3h.** *Requiring and maintaining justification for accessing systems that contain controlled unclassified information.*

**Response:** There were no documented findings for Contractor F (USTRANSCOM contractor) in the report.

## U.S. Cyber Command Chief of Staff

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

DEPARTMENT OF DEFENSE  
UNITED STATES CYBER COMMAND  
9800 SAVAGE ROAD, SUITE 6171  
FORT GEORGE G. MEADE, MARYLAND 20755

Reply to:  
Chief of Staff

JUN 13 2019

### MEMORANDUM FOR DOD INSPECTOR GENERAL

Subject: USCYBERCOM Response to DOD OIG Report; Project No. D2018-D000CR-0171.000

1. USCYBERCOM is in receipt of subject DOD OIG Draft Report and concurs with the recommendation captured in section A.3.
2. The report identified only one USCYBERCOM contractor as having deficiencies (the report identified two deficient areas). The USCYBERCOM J9 Acquisition and Program Management Divisions worked with the contractor and corrected those deficiencies as of March 22, 2019 (see Attachment).
3. (FOUO) The POC for this effort is [REDACTED] [REDACTED] [REDACTED]

*Ross A. Myers*  
ROSS A. MYERS  
Vice Admiral, U.S. Navy  
Chief of Staff

Attachment:  
Enclosure A – Corrective Action Correspondence

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

## Principal Deputy Chief Information Officer



CHIEF INFORMATION OFFICER

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

JUN - 7 2019

MEMORANDUM FOR INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE

SUBJECT: Review and Comment of DoD Inspector General "Audit of Protection of Controlled Unclassified Information on Contractor-Owned Networks and Systems" (D2018-D000CR-0171.000) Proposed Report

This is the Department of Defense (DoD) Chief Information Officer (CIO) response to the DoD Inspector General Proposed Report, "Audit of Protection of Controlled Unclassified Information on Contractor-Owned Networks and Systems" (D2018-D000CR-0171.000).

**DoD IG RECOMMENDATION A.1.a:** The DoD Chief Information Officer, in coordination with Defense Pricing and Contracting, implement or revise policy to require all systems and networks that maintain DoD information, including those owned by contractors that maintain DoD information to use strong passwords that, at a minimum, meet DoD password length and complexity requirements.


**DoD IG RECOMMENDATION A.1.b:** The DoD Chief Information Officer, in coordination with Defense Pricing and Contracting, implement or revise policy to require all systems and networks that maintain DoD information, including those owned by contractors that maintain DoD information to configure their systems and networks to align with DoD requirements for locking after 15 minutes of inactivity and 3 unsuccessful logon attempts.

**DoD CIO RESPONSE to A.1.a and A.1.b:** DoD CIO disagrees with the DoD IG recommendations. The DoD IG recommendations are added parameter values that are required for National Security Systems (NSS) and outlined in the Committee on National Security Systems Instruction 1253, "Security Categorization and Control Selection for National Security Systems." These requirements are based on protecting the information systems and not about Controlled Unclassified Information (CUI). A privately owned contractor system is not a NSS and therefore these specifications are inappropriate. Contractors are contractually required to implement the requirements outlined in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information (CUI) in Nonfederal Information Systems and Organizations." Additionally, the DoD IG recommendations conflict with 32 Code of Federal Regulation (CFR) 2002, "Controlled Unclassified Information," which states that adding agency specific requirements, as this report recommends, is not allowed to ensure that a single standard is applied for safeguarding CUI. Contractor internal IT systems are used for many U.S. Government agency contracts, so allowing each agency to specify unique, ad hoc requirements cannot be supported by the contractors. This also defeats the stated purpose of CUI Executive Order 13556 (and the implementing Federal Regulation) to "establish an open and uniform program for managing information that requires safeguarding or dissemination controls" and eliminates "ad hoc, agency-specific policies, procedures, and markings to safeguard and control this information."

## Principal Deputy Chief Information Officer (cont'd)

A security review to verify "FOR OFFICIAL USE ONLY" (FOUO) markings in the report has been completed and there are no additional recommendations.

The point of contact for this matter is Ms. [REDACTED].

  
Essye B. Miller  
Principal Deputy

## Office of the Director of Operational Test and Evaluation, Principal Deputy Director



OPERATIONAL TEST  
AND EVALUATION

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~  
**OFFICE OF THE SECRETARY OF DEFENSE**  
1700 DEFENSE PENTAGON  
WASHINGTON, DC 20301-1700

MAY 29 2019

MEMORANDUM FOR OFFICE OF THE INSPECTOR GENERAL, DEPARTMENT  
OF DEFENSE

SUBJECT: Project Number D2018-D000CR-0171.000, Audit of Protection of DOD Controlled  
Unclassified Information on Contractor-Owned Networks and Systems, 2-May-2019

Thank you for the opportunity to review and provide comments for Project Number  
D2018-D000CR-0171.000, Audit of Protection of DOD Controlled Unclassified Information on  
Contractor-Owned Networks and Systems, dated 2-May-2019.

I have attached comments from our review of the draft report pertaining to the findings  
for the DOT&E support contractor, "Contractor G," as they are identified in the report. If you  
have any additional questions, please contact [REDACTED] at [REDACTED] or at  
[REDACTED]

David W. Duma  
Principal Deputy Director

Attachment:  
As stated



~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

## Office of the Director of Operational Test and Evaluation, Principal Deputy Director (cont'd)

Project Number D2018-D000CR-0171.000

### OSD/DOT&E Comments

Recommendation A.1 – Recommend that the DoD Chief Information Officer, in coordination with Defense Pricing and Contracting, implement or revise policy to require all systems and networks that maintain DoD information, including those owned by contractors that maintain DoD information to:

- a. Use strong passwords that, at a minimum, meet DoD password length and complexity requirements.
- b. Configure their system and networks to align with DoD requirements for locking after 15 minutes of inactivity and 3 unsuccessful logon attempts.

DOT&E Response: Concur with recommendation. No action required from DOT&E.

Recommendation A.2 - Recommend that the Principal Director for Defense Pricing and Contracting, in coordination with the appropriate DoD Component responsible for developing policy:

- a. Revise its current policy to require DoD Component contracting offices, as part of the Request for Proposal and source selection processes, and requiring activities, during the performance of the contract, to assess whether contractors comply with the National Institute of Standards and Technology requirements for protecting controlled unclassified information before contract award and throughout the contracts' period of performance.
- b. Develop and implement policy requiring DoD Component contracting offices and requiring activities to maintain an accurate accounting of contractors that access, maintain, or develop controlled unclassified information as part of their contractual obligations.
- c. Revise its current policy to include language that will require DoD Component contracting offices and requiring activities to validate contractor compliance with National Institute of Standards and Technology Special Publication 800-171 requirements.
- d. Require DoD Component contracting offices, in coordination with DoD requiring activities, to develop and implement a risk-based process to verify that contractors comply with the Defense Federal Acquisition Regulation Supplement clause 252.204-7012 for protecting controlled unclassified information.
- e. Require DoD Component contracting offices, in coordination with DoD requiring activities, to take corrective actions against contractors that fail to meet the National Institute of Standards and Technology and contract requirements for protecting controlled unclassified information.

DOT&E Response: Concur with the above recommendations, with comment. DOT&E agrees that an assessment for contractor compliance with NIST requirements during source selection and throughout contract execution is a reasonable component for safeguarding CUI. However, DOT&E, like many others, is a small organization that is not staffed with the manpower or required skillsets to conduct actual on-site compliance audits of contractor networks. A process that would include an independent organization, such as Defense Security Services (DSS), that has the skillsets to conduct such audits, would be a reasonable approach. DOT&E is amenable to evaluating the results of recurring independent

1



## Office of the Director of Operational Test and Evaluation, Principal Deputy Director (cont'd)

Project Number D2018-D000CR-0171.000

audits to assess a support contractor's network compliance and to put in place corrective action plans, as required.

**Recommendation A.3** - Recommend that the Director of Acquisitions for the Missile Defense Agency; and Contracting Officers for the U.S. Army, U.S. Navy, U.S. Air Force, U.S. Cyber Command, U.S. Transportation Command, Defense Contract Management Agency, Director, Operational Test and Evaluation, and Defense Microelectronics Activity, in coordination with DoD requiring activities, develop and implement a plan to verify that contractors correct the weaknesses identified in this report related to:

- a. using multifactor authentication;

**DOT&E Response:** Concur. No action required from DOT&E.

- b. mitigating vulnerabilities in a timely manner;

**DOT&E Response:** Concur. Contractor G is developing a formalized process to document and track outstanding vulnerability plans of action and remediation plans. Contractor G will correct existing deficiencies and will reduce or eliminate existing vulnerabilities by August 15, 2019. DOT&E and the COR will receive regular updates regarding IDA's progress throughout the remediation process.

- c. protecting and monitoring data on removable media;

**DOT&E Response:** Non-concur. DOT&E has worked with Contractor G and has determined that they are compliant with NIST 800-171, as currently written, regarding the protection and monitoring of data on removable media. Contractor G utilizes encryption tools and has implemented procedures to properly safeguard data. However, they recognize that much of the compliance relies on staff adherence to policies, and as a result will strengthen staff training and communications to reinforce policies and maintain compliance. Contractor G policies will be recommunicated to their staff through corporate channels and updated staff training, with a target completion date of September 1, 2019.

- d. documenting and tracking cybersecurity incidents;

**DOT&E Response:** Non-concur. Contractor G complies with NIST 800-171 as currently written, including the reporting of all cyber incidents to the Defense Cyber Crime Center (DC3) that includes malware and disk images. Incidents are tracked through remediation in a local IT Service Management System. However both DOT&E and Contractor G agree that the process can be strengthened through a more formal reporting program that utilizes a consolidated, single repository, and includes comprehensive documentation. This program will be deployed over the coming months with a target date for full implementation of September 1, 2019.

- e. utilizing an automatic system lock after inactivity or unsuccessful logon attempts;

**DOT&E Response:** Non-concur. As currently written, NIST 800-171 does not specify a specific lockout period. Contractor G currently employs a 30 minute lockout period that is in compliance, as per current NIST 800-171 policy. DOT&E and Contractor G have discussed the specific finding, and based on physical and operational controls at the Contractor G facility, a 30 minute lockout properly balances the

## Office of the Director of Operational Test and Evaluation, Principal Deputy Director (cont'd)

Project Number D2018-D000CR-0171.000

risk of compromise, with business requirements and staff productivity. If future policy identifies an explicit lockout period for contractor networks, DOT&E will assess and track Contractor G's compliance.

- f. implementing physical security controls;

DOT&E Response: Concur. No action required from DOT&E.

- g. generating system activity reports;

DOT&E Response: Concur. No action required from DOT&E.

- h. requiring and maintaining justification for accessing systems that contain controlled unclassified information.

DOT&E Response: Concur. No action required from DOT&E.

Recommendation A.4 - Recommend that the Director of Acquisition, Missile Defense Agency, verify that Contractor H:

- a. transitioned to a 3<sup>rd</sup> Party service provider where oversight of the provider are feasible;
- b. configured all assets on its network to create system activity reports;
- c. configured all devices on its network to use multi-factor authentication.

DOT&E Response: Not Applicable to DOT&E.

Recommendation B.1 – Recommend that the Director for Contract Policy and Oversight, Defense Threat Reduction Agency:

- a. Revise its process for monitoring security incidents, including data spillages by contractors, to verify that contractors took the appropriate steps to identify, respond to, and report security incidents that involve DoD data.
- b. Review the performance of the contracting officer responsible for monitoring the 2016 security incident identified in this report and consider administrative action, as appropriate, for not ensuring that Contractor C took actions to remove the classified information from its corporate network and the contractor's commercial cloud environment.

DOT&E Response: Not Applicable to DOT&E

Recommendation B.2 – Recommend that the Director for Defense Security Services assess and document the risk of leaving classified data unprotected in unclassified environments and, based on the assessment, develop and implement controls to protect the information.

DOT&E Response: Not Applicable to DOT&E.

## Defense Threat Reduction Agency Chief Information Officer



DEFENSE THREAT REDUCTION AGENCY  
8725 JOHN J. KINGMAN ROAD, STOP 6201  
FORT BELVOIR, VA 22060-6201

June 3, 2019

MEMORANDUM FOR CYBERSPACE OPERATIONS, DOD OFFICE OF INSPECTOR  
GENERAL (ATTN: [REDACTED])

SUBJECT: Follow-up on Audit Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems, (Project No. D2018-D000CR-0171.000)

This is in response to the Audit of Protection of DoD Controlled Unclassified Information (CUI) on Contractor-Owned Networks and Systems published May 2, 2019, request for comments. The following is provided as an update:

**Recommendation B.1.a:** The DoD OIG recommended the Director for Contract Policy and Oversight, Defense Threat Reduction Agency revise its process for monitoring security incidents, including data spillages by contractors, to verify that contractors took the appropriate steps to identify, respond to, and report security incidents that involve DoD data.

**Management Update:** Partially Concur. The DTRA Chief of Security is responsible for monitoring security incidents, to include data spillages. That office is working with the DTRA Incident Response Team to revise the Negligent Disclosure of Classified Information (NDCI) Spillage form and DTRA NDCI Work instruction. These documents are used for coordinating security incidents, including data spillages by contractors. The changes will ensure notifications are made to the appropriate Contracting Officer for possible administrative actions and to assist with notification to the Defense Security Service. **This is expected to be completed by June 30, 2019.**

**Recommendation B.1.b:** The DoD OIG recommended the Director for Contract Policy and Oversight, Defense Threat Reduction Agency review the performance of the contracting officer responsible for monitoring the 2016 security incident identified in this report and consider administrative action, as appropriate, for not ensuring that Contractor C took actions to remove the classified information from its corporate network and the contractor's commercial cloud environment.

**Management Update:** Partially Concur. The Director for Contract Policy and Oversight reviewed the performance of the contracting officer related to these findings and found no reason to take administrative actions. Of note, there is no DOD policy that requires the contracting officer to "ensure the removal of classified information from a corporate network and the contractor's commercial cloud environment." Contracting officers are not trained to nor are they required to "validate contractor compliance with National Institute of Standards and Technology Special Publication 800-171 requirements."

## Defense Threat Reduction Agency Chief Information Officer (cont'd)

However, all procedures at DTRA related to the Security Incident process, as noted in the management update for Recommendation B.1.a, will be updated to ensure appropriate DTRA offices receive timely notification of incidents and that relevant information is provided to the Contracting Officer. **This is expected to be completed by June 30, 2019.**

REEVES-  
FLORES.NANCY.P [REDACTED]  
[REDACTED]

Digitally signed by REEVES-  
FLORES.NANCY.P [REDACTED]  
Date: 2019.06.03 07:59:37  
-04'00'

Nancy P. Reeves-Flores, SES  
Director, Information Integration & Technology  
Services and Chief Information Officer

## Defense Counterintelligence and Security Agency Executive Director

**DEFENSE SECURITY SERVICE**

27130 TELEGRAPH ROAD  
QUANTICO, VA 22134-2253

JUN 10 2019

MEMORANDUM FOR INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE  
(ATTN: [REDACTED])

SUBJECT: DoD OIG Draft Report, "Audit of the Protection of Controlled Unclassified Information on Contractor-Owned Networks and Systems" (Project No. D2018-D000CR-0171.000)

We reviewed the subject report and concur with no comments. We will include the aspects of Recommendation B2 into future incident responses and decisions. If you have any questions in the meantime, please contact [REDACTED] at [REDACTED] or [REDACTED].

  
Troy L. Littles  
Executive Director

## Missile Defense Agency Director



IR

DEPARTMENT OF DEFENSE  
MISSILE DEFENSE AGENCY  
5700 18<sup>TH</sup> STREET  
FORT BELVOIR, VIRGINIA 22060-5573

JUN 05 2019

MEMORANDUM FOR ASSISTANT INSPECTOR GENERAL FOR CYBERSPACE  
OPERATIONS, DEPARTMENT OF DEFENSE INSPECTOR  
GENERAL

SUBJECT: Missile Defense Agency Response to the Department of Defense Inspector General  
Draft Report for the Audit of the Protection of Controlled Unclassified Information  
on Contractor-Owned Networks and Systems (Project No. D2018-D000CR-  
0171.000)

Thank you for providing the Missile Defense Agency (MDA) the opportunity to review  
the Draft Report for the Audit of the Protection of Controlled Unclassified Information on  
Contractor-Owned Networks and Systems (Project No. D2018-D000CR-0171.000). MDA is  
providing the attached response to the Draft Report and the requested Security Marking Review  
document. If you have any questions, please contact my POCs [REDACTED] [REDACTED]

[REDACTED] or [REDACTED]  
[REDACTED]

J. A. HILL  
Vice Admiral, USN  
Director

Attachments:  
As stated

## Missile Defense Agency Director (cont'd)

**Final  
Report Reference**

**MDA Response to Recommendations  
DoD IG Audit of Protection of DoD Controlled Unclassified Information on  
Contractor-Owned Networks and Systems (Project No. D2018-D000CR-  
0171.000)  
DRAFT REPORT**

Rec #	Response
A.3	<p><b>Recommendation:</b> We recommend that the Director for Acquisition for the Missile Defense Agency (and others) in coordination with DoD requiring activities, develop and implement a plan to verify that contractors correct the weaknesses identified in this report related to:</p> <ul style="list-style-type: none"> <li>a. Using multifactor authentication (MFA);</li> <li>b. Mitigating vulnerabilities in a timely manner;</li> <li>c. Protecting and monitoring data on removable media;</li> <li>d. Documenting and tracking cybersecurity incidents;</li> <li>e. Utilizing an automatic system lock after inactivity or unsuccessful logon attempts;</li> <li>f. Implementing physical security controls;</li> <li>g. Generating system activity reports; and</li> <li>h. Requiring and maintaining justification for accessing systems that contain controlled unclassified information.</li> </ul> <p><b>Response:</b> MDA concurs with this recommendation.</p> <p><b>Reason:</b> As stated in the report (pp. 2-3), Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012 requires contractors that maintain controlled unclassified information (CUI) on their non-federal system(s) to implement security controls specified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171. Currently, neither DFARS 252.204-7012 nor any supplemental DoD Policy mandate on-site reviews of non-federal systems by Government personnel, including DoD Component contracting office personnel. The current policy requires contractors to self-assess their network/system(s), develop a system security plan to addresses their system(s) compliance with NIST SP 800-171 requirements, and, where non-compliant with any of the NIST requirements, develop a plan of action and milestones (POA&amp;M) to address and schedule implementation of remaining applicable security requirements. Notwithstanding prevailing policy guidance, MDA is directly engaged with Contractor H to support their improved DFARS -7012 compliance status, with respect to Control Deficiencies a-c, e, g and h listed above. These six items were identified as the deficiencies of Contractor H per the DoD IG report page 7, Table 2.</p> <p><b>Corrective Actions Taken to Date:</b> The MDA contract Procuring Contracting Officer (PCO) for Contractor H is directly and regularly engaged with the contractor. The contractor has been diligently and consistently working on improving their compliance status and reporting their progress to MDA since the DoD IG visit. Contractor H developed a comprehensive corrective action plan (Attachment 1) in March 2019 to address the DoD IG audit findings. As confirmed by the contract PCO, Contractor H is on schedule to complete implementation of identified</p>

**Page 3 and 4**

Page 1 of 4

Attachment 1



## Missile Defense Agency Director (cont'd)

Rec #	Response
	<p>enhancements by June 2019. Specific actions for Control Deficiencies a-c, e, g, and h completed by Contractor H include:</p> <ul style="list-style-type: none"> <li>a. Contractor H has incorporated MFA for all users in Huntsville and will complete company-wide MFA by June 2019. Contractor H is also incorporating a public key infrastructure (PKI) for Key Management Personnel for non-repudiation, including email encryption.</li> <li>b. Contractor H is increasing storage capacity and adding end-point scanning to the core infrastructure scans in order to generate records to analyze, monitor and report unauthorized system activity on all devices, ultimately in order to find and fix vulnerabilities. Estimated Completion Date (ECD): June 2019</li> <li>c. Contractor H is completing infrastructure-wide disabling of USB port usage by non-approved USB devices through Active Directory Group Policy. ECD: June 2019</li> <li>e. Contractor H is updating their Active Directory Group Policy for password lock-out after three invalid attempts. This is being accomplished with the USB port lockout update. Additionally, this Policy update will require 15-character passwords. ECD: June 2019</li> <li>g. As discussed for A.3.b., Contractor H is adding further scanning, monitoring and analyzing scans on the servers and client systems to ensure reports are generated and reviewed, as well as action taken to find and fix vulnerabilities.</li> <li>h. Contractor H requires all users to receive prior Data Content Owners' approval for access to their respective areas. No access is provided without verifying a need-to-know and without written approval from content owner. Additionally, Contractor H is implementing more formal procedures, including standardized web forms and automated workflow, that will be documented in the System Security Plan.</li> </ul> <p>In addition, Contractor H has also agreed to an on-site visit by the MDA Cyber Assistance Team (CAT) to review/assess their "improved systems and processes as soon as these enhancements are completed." The MDA PCO has confirmed in writing (Attachment 2) that the improved cybersecurity status of Contractor H has the full attention of their senior management, who is committed to automate and hasten the identification and remediation of vulnerabilities. To date, Contractor H has completed the requested actions in Control Deficiencies a, b, and c, with other actions in process.</p> <p><b>Near-Term and Planned Future Actions:</b> The Under Secretary of Defense for Acquisition and Sustainment (USD(A&amp;S)) memo "Guidance for Assessing Compliance and Enhancing Protections Required by DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting", issued November 6, 2018, provides guidance for conducting on-site reviews of nonfederal systems. MDA is actively participating in DoD working groups chartered to develop holistic Department procedures to conduct on-site contractor assessments and assign associated ratings, as applicable. These DoD activities are</p>

## Missile Defense Agency Director (cont'd)

**Final  
Report Reference**

Rec #	Response
	ongoing at this time (in coordination with the Defense Contract Management Agency (DCMA), the Defense Counterintelligence and Security Agency (DCSA) (formerly the Defense Security Service (DSS)), and associated Office of the Secretary of Defense (OSD) offices) to address and assess contractor cybersecurity implementation status. Pending any subsequent DoD-approved policy or regulation updates, MDA will fully support the implementation as provided in DoD policy.
A.4	<p><b>Recommendation:</b> We recommend that the Director for Acquisition, Missile Defense Agency, verify that Contractor H:</p> <ol style="list-style-type: none"> <li>Transitioned to a third-party service provider where the oversight activities of the provider are feasible.</li> <li>Configured all assets on its network to create system activity reports.</li> <li>Configured all devices on its network to use multi-factor authentication.</li> </ol> <p><b>Response:</b> MDA concurs with this recommendation.</p> <p><b>Reason:</b> As stated in the report (pp. 2-3), DFARS clause 252.204-7012 requires contractors that maintain CUI on their non-federal system(s) to implement security controls specified in NIST SP 800-171. Currently, neither DFARS 252.204-7012 nor any supplemental DoD Policy mandate on-site reviews of non-federal systems by Government personnel, including DoD Component contracting office personnel. The current policy requires contractors to self-assess their network/system(s), develop a system security plan to addresses their system(s) compliance with NIST SP 800-171 requirements, and, where non-compliant with any of the NIST requirements, develop a POA&amp;M to address and schedule implementation of remaining applicable security requirements. Notwithstanding prevailing policy guidance, MDA is directly engaged with Contractor H to support their improved DFARS -7012 compliance status.</p> <p><b>Corrective Actions Taken to Date:</b> The MDA PCO is monitoring Contractor H's DFARS 252.204-7012 compliance status and has confirmed that Contractor H performed the required DFARS self-assessment, developed a System Security Plan and developed a POA&amp;M that supports the Contractor's Corrective Action Plan for complete DFARS 252.204-7012 compliance by June 2019. Contractor H has completed the actions requested in A.4.a., with other actions in process as stated in Contractor H's Corrective Action Plan. Contractor H has also agreed to an external review by the MDA CAT as soon as practicable. Specific actions completed by Contractor H include:</p> <ol style="list-style-type: none"> <li>Contractor H was not able to terminate the contract with their existing network carrier (through April 2019) without severe penalties. In May 2019, network equipment installation and transition to Voice-Over-IP phones was completed. This brought oversight of network perimeter protections in-house. Contractor H deployed a software-defined Wide Area Network to increase monitoring and logging of network traffic.</li> <li>Contractor H is increasing storage capacity and adding end-point scanning to the core infrastructure scans in order to generate records to analyze, monitor and report unauthorized system activity on all devices. ECD: June 2019</li> </ol>

**Page 3 and 4**

Page 3 of 4

Missile Defense Agency Director (cont'd)

Rec #	Response
	<p>c. Contractor H has incorporated MFA for all users in Huntsville and will complete company-wide MFA by June 2019. Contractor H is also incorporating a PKI for Key Management Personnel for non-repudiation, including email encryption. ECD: June 2019</p> <p><b>Near-Term and Planned Future Actions:</b> The USD(A&amp;S) memo “Guidance for Assessing Compliance and Enhancing Protections Required by DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting”, issued November 6, 2018, provides guidance for conducting on-site reviews of nonfederal systems. MDA is actively participating in DoD working groups chartered to develop holistic Department procedures to conduct on-site contractor assessments and assign associated ratings, as applicable. These DoD activities are ongoing at this time (in coordination with DCMA, DCSA (formerly DSS), and associated OSD offices) to address and assess contractor cybersecurity implementation status. Pending any subsequent DoD-approved policy or regulation updates, MDA will fully support the implementation as provided in DoD policy.</p>

## Defense Contract Management Agency Director



### DEFENSE CONTRACT MANAGEMENT AGENCY

3901 A. AVENUE, BUILDING 10500  
FORT LEE, VIRGINIA 23801-1809

JUN 07 2019

MEMORANDUM FOR DEPARTMENT OF DEFENSE, INSPECTOR GENERAL

SUBJECT: DCMA management comments to DOD OIG draft report: "Audit of the Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems" dated April 30, 2019" (Project No. D2018-D000CR-0171.000)

Attached is the Defense Contract Management Agency's management comments for subject report.

The point of contact for this response is [REDACTED] at [REDACTED] or [REDACTED].

David H. Lewis  
VADM, USN  
Director

Attachment(s):

TAB A. DCMA's Management Comments

TAB B. OUSD Memorandum: Strategically Implementing Cybersecurity Contract Clauses

Link(s):

None

## Defense Contract Management Agency Director (cont'd)

ACQUISITION  
AND SUSTAINMENTTHE UNDER SECRETARY OF DEFENSE  
3010 DEFENSE PENTAGON  
WASHINGTON, DC 20301-3010

FEB - 5 2019

MEMORANDUM FOR COMMANDER, U.S. CYBER COMMAND  
(ATTN: ACQUISITION EXECUTIVE)  
COMMANDER, U.S. SPECIAL OPERATIONS  
COMMAND (ATTN: ACQUISITION EXECUTIVE)  
COMMANDER, U.S. TRANSPORTATION  
COMMAND (ATTN: ACQUISITION EXECUTIVE)  
ASSISTANT SECRETARY OF THE ARMY FOR ACQUISITION,  
LOGISTICS, AND TECHNOLOGY  
ASSISTANT SECRETARY OF THE NAVY FOR RESEARCH,  
DEVELOPMENT, AND ACQUISITION  
ASSISTANT SECRETARY OF THE AIR FORCE FOR  
ACQUISITION, TECHNOLOGY, AND LOGISTICS  
DIRECTORS OF THE DEFENSE AGENCIES  
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Strategically Implementing Cybersecurity Contract Clauses

Implementing Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012 across all Department of Defense (DoD) contracts, with the exception of those for commercially available off-the-shelf items, is vital to the future security of the United States. DFARS 252.204-7008 requires contractors to represent on a contract-by-contract basis that their implementation of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 is complete. To document the implementation of NIST SP 800-171, companies must develop, document, and periodically update a system security plan that describes system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems. If implementation of the security requirements is not complete, companies must develop and implement plans of action to describe how and when any unimplemented security requirements will be met.

This individual contract approach is inefficient for both Industry and Government, and impedes the effective implementation of requirements to protect DoD's Controlled Unclassified Information for contracts containing DFARS clause 252.204-7012. Therefore, pursuant to this memorandum, I direct the Director, Defense Contract Management Agency (DCMA), to develop a proposed path ahead using its administration authority under Federal Acquisition Regulation Part 42 and 43 and DFARS 242.302 to modify contracts that are administered by DCMA to achieve the objectives below. Such authority will be limited to bilateral modifications that do not result in a change to any contract price, obligated amount, or fee arrangement. DCMA, in partnership with the Principal Director, Defense Pricing and Contracting (DPC); the DoD Chief Information Officer; the Deputy Director, Strategic Technology Protection and Exploitation; the Office of the Under Secretary of Defense for Intelligence; and the DoD Components, will:

## Defense Contract Management Agency Director (cont'd)

- Assess and recommend to the Under Secretary of Defense for Acquisition and Sustainment a set of business strategies to—
  - Obtain and assess contractor system security plans, and any associated plans of action, strategically (not contract-by-contract);
  - Propose a methodology to determine industry cybersecurity readiness, and a level of confidence in the readiness assessment, at the corporate, business sector (division) or facility level; and
  - Propose how to communicate (document and share) that cybersecurity readiness and confidence level to the DoD Components.
- Engage industry to discuss methods to oversee the implementation of DFARS Clause 252.204-7012 and NIST SP 800-171.
- Include within the business strategies above, consideration of leveraging DCMA's contracting officers authority to incorporate a repeatable strategic process/discussion to pursue a no-cost bilateral block change to:
  - Require submission of company's system security plan (or extracts thereof), and any associated plans of action, at a strategic level;
  - Document industry cybersecurity readiness at a strategic level;
  - Apply a standard methodology to recognize industry cybersecurity readiness at a strategic level and include a process to update this recognition as cybersecurity readiness changes over time; and
  - Negotiate inclusion of DFARS clause 252.204-7012 to existing contracts without the clause as part of the block change modification process.

To ensure a similar corporate approach may be taken with companies for which DCMA does not administer contracts (such as the Secretary of the Navy's shipbuilding contracts), DPC will work with representatives of those communities to implement a similar solution. DPC will host a meeting on Wednesday, February 6, 2019 to address the proposed methodology to recognize industry cybersecurity readiness, and address any concerns that you may have. Please contact Ms. Mary Thomas at 703-693-7895 or mary.s.thomas.civ@mail.mil with the name of any attendees. I have directed DCMA not to exercise this authority until after March 1, 2019. If you do not agree with the approach, please notify the action officers identified below before that date.

If you have any questions regarding this matter, my point of contact is Ms. Mary Thomas. The DCMA point of contact is Mr. John Ellis, at 804-734-0476 or john.a.ellis.civ@mail.mil.



Ellen M. Lord



## Defense Pricing and Contracts Acting Principal Director



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

JUN 06 2019

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

SUBJECT: Response to the Department of Defense Office of the Inspector General Draft Report  
on Audit of Protection of DoD Controlled Unclassified Information on  
Contractor-Owned Networks and Systems (Project No. D2018-D000CR-0171.000)

As requested, I am providing responses to the general content and recommendations for the Acting Principal Director for Defense Pricing and Contracting (DPC) action contained in the subject report.

Recommendation A.2: We recommend that DPC, in coordination with the appropriate Department of Defense (DoD) Component responsible for developing policy:

- a. Revise its current policy to require DoD Component contracting offices, as part of the Request for Proposal and source selection processes, and requiring activities, during the performance of the contract, to assess whether contractors comply with the National Institute of Standards and Technology requirements for protecting controlled unclassified information before contract award and throughout the contracts' period of performance.

Response for A.2.a: Concur. We concur with and are implementing the recommendation to assess whether contractors comply with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" during the performance of the contract with the following actions.

- Defense Federal Acquisition Regulation Supplement (DFARS) provision 252.204-7008, Compliance with Safeguarding Covered Defense Information Controls, requires that offerors represent that they will implement the security requirements specified by NIST SP 800-171 as part of the Request for Proposal and source selection processes.
- Under Secretary of Defense (Acquisition and Sustainment) memorandum, "Strategically Implementing Cybersecurity Contract Clauses," dated February 5, 2019, directed the Defense Contract Management Agency (DCMA) to assess contractor compliance with NIST SP 800-171 at a strategic (corporate-wide) level for companies for which they administer contracts. DCMA, in partnership with DPC, the Office of the Under Secretary of Defense for Research and Engineering (USD(R&E)), the Office of the DoD Chief Information Officer (CIO), the Defense Security Service (DSS), and the DoD Components, is piloting the strategic assessment approach with the Department's top seven defense contractors from June through September 2019.
- Upon completion of this pilot effort, DPC will work with DCMA, DoD CIO, USD(R&E), and the DoD Components to:



## Defense Pricing and Contracts Acting Principal Director (cont'd)

- Consider how assessment results may be used prior to contract award to update DFARS provision 252.204-7008.
- Revise current policy and/or regulations to document this strategic (corporate-wide) approach.

### Recommendation A.2.b:

Develop and implement policy requiring DoD Component contracting offices and requiring activities to maintain an accurate accounting of contractors that access, maintain, or develop controlled unclassified information as part of their contractual obligations.

Response for A.2.b: Concur. We concur with and are implementing the recommendation to maintain an accurate accounting of contractors that access, maintain, or develop controlled unclassified information as part of their contractual obligations. Using enterprise contract data, DPC tracks, and provides to the DoD Components on a quarterly basis, a listing of contracts that include DFARS clause 252.204-7012. This enterprise capability enables DPC to maintain an accounting of contractors DoD-wide.

### Recommendation A.2.c:

Revise its current policy to include language that will require DoD Component contracting offices and requiring activities to validate contractor compliance with National Institute of Standards and Technology Special Publication 800-171 requirements.

Response for A.2.c: Concur. As stated in response A.2.a., we concur with and are implementing the recommendation to validate contractor compliance with National Institute of Standards and Technology Special Publication 800-171 requirements. We will revise current policy and/or regulations to document the Department's approach upon completion of the pilot effort.

### Recommendation A.2.d:

Require DoD Component contracting offices, in coordination with DoD requiring activities, to develop and implement a risk-based process to verify that contractors comply with the Defense Federal Acquisition Regulation Supplement clause 252.204-7012 for protecting controlled unclassified information.

Response for A.2.d: Concur. As stated in response A.2.a., we concur with and are implementing the recommendation to develop and implement a risk-based process to verify that contractors comply with DFARS clause 252.204-7012. The implementation of DoD's Procedures to Strategically Assess Compliance with NIST SP 800-171 will result in a risk-based process to verify that contractors comply with the security requirements in NIST SP 800-171 at the strategic (DoD and corporate-wide) level, and provides a common methodology that requiring activities/contracting offices may use on a contract-by-contract basis when appropriate.

## Defense Pricing and Contracts Acting Principal Director (cont'd)

Recommendation A.2.e:

Require DoD Component contracting offices, in coordination with DoD requiring activities, to take corrective actions against contractors that fail to meet the National Institute of Standards and Technology and contract requirements for protecting controlled unclassified information.

Response for A.2.e: Concur. We concur with the recommendation to require contracting offices, in coordination with DoD requiring activities, to take corrective actions against contractors that fail to meet NIST SP 800-171 and contract requirements for protecting controlled unclassified information. DoD Components are currently authorized in regulation to implement any or all of the penalties and remedies for non-compliance of Government terms and conditions in a contract, to include the requirements of DFARS clause 252.204-7012 and NIST SP 800-171. These penalties and remedies, when warranted, are based on risk to the Government or national security, and in accordance with FAR Parts 9, 17, 42, and 49, and DFARS Part 242. The implementation of DoD's Procedures to Strategically Assess Compliance with NIST SP 800-171 (addressed in A.2.a.) will provide added visibility to the contractors compliance with NIST SP 800-171 and enable DCMA (or the administering organization) to apply penalties and remedies as warranted.

Please contact [REDACTED] if additional information is required.



Kim Herrington  
Acting Principal Director  
Defense Pricing and Contracting

## Acronyms and Abbreviations

---

<b>CFR</b>	Code of Federal Regulations
<b>CUI</b>	Controlled Unclassified Information
<b>DCSA</b>	Defense Counterintelligence and Security Agency
<b>DFARS</b>	Defense Federal Acquisition Regulation Supplement
<b>DPC</b>	Defense Pricing and Contracting
<b>DTRA</b>	Defense Threat Reduction Agency
<b>DASN</b>	Deputy Assistant Secretary of the Navy
<b>FPDS</b>	Federal Procurement Data System
<b>DOT&amp;E</b>	Director of Operational Test and Evaluation
<b>GAO</b>	Government Accountability Office
<b>MDA</b>	Missile Defense Agency
<b>NIST</b>	National Institute of Standards and Technology
<b>OIG</b>	Office of Inspector General
<b>POA&amp;M</b>	Plan of Action and Milestones
<b>SP</b>	Special Publication
<b>USB</b>	Universal Serial Bus
<b>USTRANSCOM</b>	U.S. Transportation Command

## Glossary

---

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

**Audit Logs.** Chronological records of network and system activities, including records of system accesses and operations performed in a given period.

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

**Boundary Protection.** Monitoring and control of communications at the external boundary of a network or an information system to prevent and detect malicious and other unauthorized communications through the use of boundary protection devices (for example, proxies, gateways, routers, firewalls, and encrypted tunnels).

**Cloud Computing (Environment).** A model for enabling convenient, on-demand network access to a shared group of configurable computing resources (for example, networks, servers, storage, applications, and services) that can be rapidly provided and released with minimal management effort or service provider interaction.

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

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

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

**Controlled Unclassified Information (CUI) Registry.** The online repository for all information, guidance, policy, and requirements on maintaining CUI. Among other information, the CUI Registry identifies all approved CUI categories and subcategories, provides general descriptions for each, identifies the basis for controls, and establishes security markings.

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

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

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

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

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

**Integrity.** The property whereby an entity has not been modified in an unauthorized manner.

**Least Privilege.** The principle that a system should be designed so that users are granted the minimum system access needed to perform their duties.

**Local Access.** Access to an organizational system by a user (or process acting on behalf of a user) communicating through a direct connection without the use of a network.

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

**Media.** Physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, Large-Scale Integration memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within a system.

**Mobile Device.** A portable computing device that has a small form factor such that it can easily be carried by a single individual; is designed to operate without a physical connection (for example, wirelessly transmit or receive information); possesses local, non-removable or removable data storage; and includes a self-contained power source. Examples include smartphones, tablets, and electronic readers.

**Multifactor Authentication.** Authentication using two or more different factors to achieve authentication. Factors include something you know (for example, personal identification number or password), something you have (for example, cryptographic identification device or token), or something you are (for example, biometric).

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

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

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

**Remote Access.** Access to an organization's nonpublic information system by an authorized user (or information system) communicating through an external, non-organization-controlled network.

**Removable Media.** Portable electronic storage devices that can be inserted into and removed from a computer. Examples include hard disks, floppy disks, zip drives, compact discs, thumb drives, and similar universal serial bus storage devices.

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

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

**Service Level Agreement.** Defines the specific responsibilities of the service provider and sets the customer expectations.

**Token.** Used to authenticate a user's identity.

**Virtual Private Network.** A protected information system link using security controls to give the impression of a dedicated line.





## **Whistleblower Protection**

### **U.S. DEPARTMENT OF DEFENSE**

*Whistleblower Protection safeguards DoD employees against retaliation for protected disclosures that expose possible waste, fraud, and abuse in government programs. For more information, please visit the Whistleblower webpage at <http://www.dodig.mil/Components/Administrative-Investigations/Whistleblower-Reprisal-Investigations/Whistleblower-Reprisal/> or contact the Whistleblower Protection Coordinator at [Whistleblowerprotectioncoordinator@dodig.mil](mailto: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](mailto:public.affairs@dodig.mil); 703.604.8324 DoD OIG Mailing Lists  
[www.dodig.mil/Mailing-Lists/](http://www.dodig.mil/Mailing-Lists/)

**Twitter**

[www.twitter.com/DoD\\_IG](http://www.twitter.com/DoD_IG)

**DoD Hotline**

[www.dodig.mil/hotline](http://www.dodig.mil/hotline)

**~~FOR OFFICIAL USE ONLY~~**



DEPARTMENT OF DEFENSE | OFFICE OF INSPECTOR GENERAL

4800 Mark Center Drive  
Alexandria, Virginia 22350-1500 [www.dodig.mil](http://www.dodig.mil)  
Defense Hotline 1.800.424.9098

**~~FOR OFFICIAL USE ONLY~~**