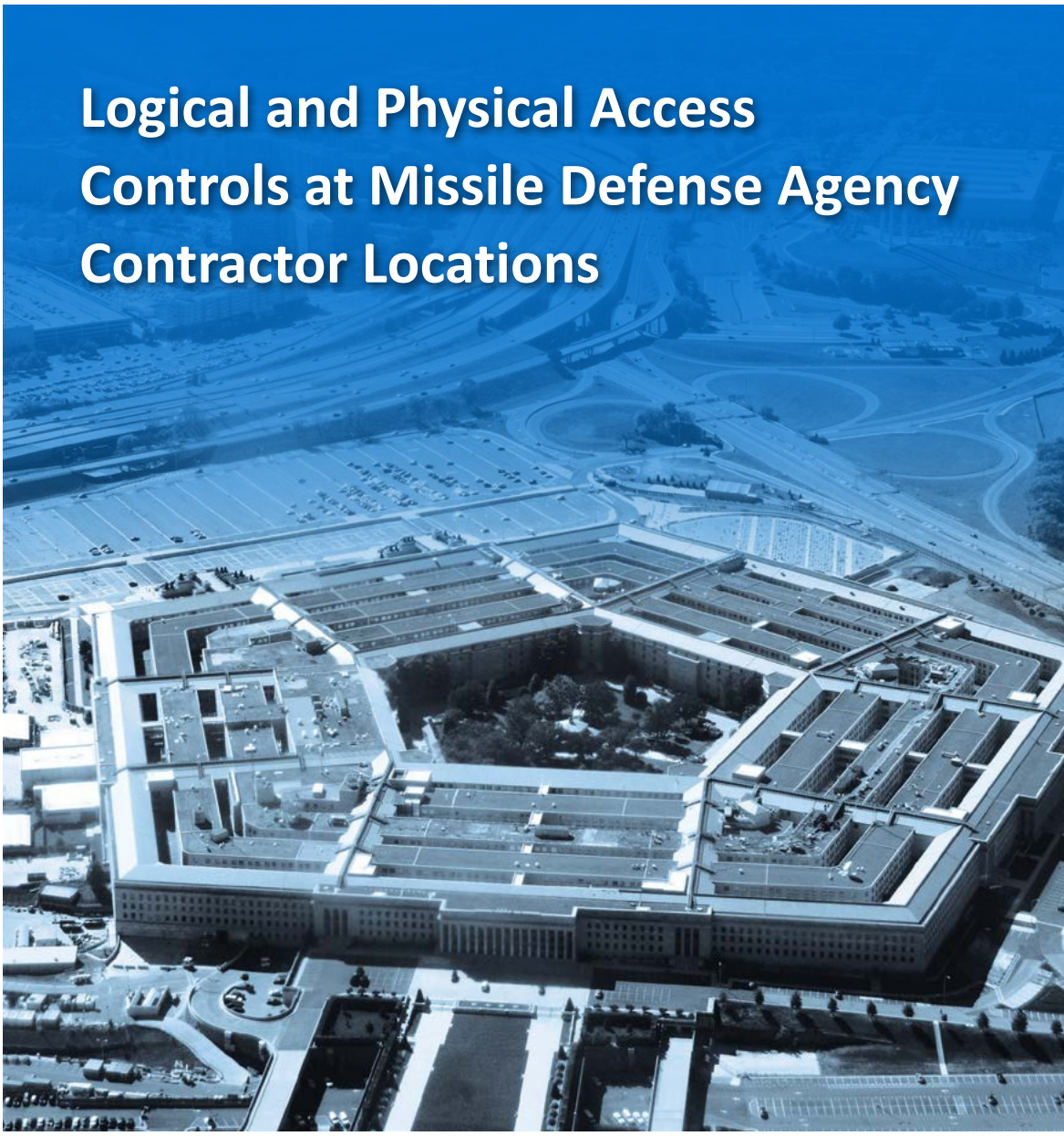
Report No. DODIG-2018-094

INSPECTOR GENERAL

U.S. Department of Defense

MARCH 29, 2018

Logical and Physical Access Controls at Missile Defense Agency Contractor Locations



INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

Mission

Our mission is to provide independent, relevant, and timely oversight of the Department of Defense that supports the warfighter; promotes accountability, integrity, and efficiency; advises the Secretary of Defense and Congress; and informs the public.

Vision

Our vision is to be a model oversight organization in the Federal Government by leading change, speaking truth, and promoting excellence-a diverse organization, working together as one professional team, recognized as leaders in our field.

For more information about whistleblower protection, please see the inside back cover.

Results in Brief

Logical and Physical Access Controls at Missile Defense Agency Contractor Locations

March 29, 2018

Objective

We determined whether Missile Defense Agency (MDA) contractors implemented security controls and processes to protect classified and unclassified ballistic missile defense system (BMDS) technical information from internal and external threats. This audit focused on security controls at seven MDA contractor facilities.

We conducted this audit in response to a congressional requirement to audit the controls in place to protect classified and unclassified ballistic missile defense technical information, whether managed by cleared Defense contractors or by the Government. This is the first of two audits to determine whether the MDA effectively protects BMDS technical information from unauthorized access and disclosure.

Background

On April 14, 2016, the MDA Director provided testimony to the House Armed Services Subcommittee on Strategic Forces expressing concern about the potential threat to systems containing BMDS technical information, especially technical information present on cleared Defense contractors' systems. A cleared Defense contractor is a private company that is given clearance by the DoD to access, receive, or store classified information for the purpose of bidding for a contract or conducting activities in support of any DoD program. The MDA Director stated that cleared Defense contractors may be subject to cyber attacks that allow unauthorized individuals to obtain access to controlled technical information.

Findings

The seven MDA contractors that we audited did not consistently implement security controls and processes to protect classified and unclassified BMDS technical information.[1] Specifically, system and network administrators at the seven contractors that managed BMDS technical information on their classified and unclassified networks did not consistently implement system security controls in accordance with Federal and DoD requirements for safeguarding Defense information. Specifically, we identified issues with:

- the use of multifactor authentication to access networks;
- password configurations;
- the assessment of risk to information systems and assets;
- identifying and mitigating network and system vulnerabilities;
- overseeing network and boundary protection services provided by a third-party company;
- transferring controlled technical information to personal electronic devices, such as home computers;
- restricting the use of removable media;
- configuring systems to automatically lock;
- granting system access; and
- maintaining and reviewing system activity logs.

Contractor system security controls were ineffective because the MDA did not oversee the contractors' current or planned actions to protect BMDS technical information on classified and unclassified networks and systems before contract award or during the contract period of performance. If the MDA does not verify and monitor compliance with Defense

[1] For this report, we use the term "contractor" to mean private entities or individual facilities.

Results in Brief

Logical and Physical Access Controls at Missile Defense Agency Contractor Locations

Findings (cont'd)

Federal Acquisition Regulation Supplement (DFARS) and National Industrial Security Program Operating Manual requirements, contractors could inadvertently disclose critical technical details of the DoD's BMDS components to U.S. adversaries and allow them to potentially circumvent the BMDS capabilities, leaving the United States vulnerable to deadly missile attacks.

Recommendations

We recommend, among other recommendations, that the MDA Director for Acquisition:

- Establish a separate technical evaluation factor in the source selection process to evaluate whether an offeror's approach to securing its networks and systems complied with DFARS clause 252.204-7012.
- Include penalty clauses in awarded contracts to levy monetary sanctions on contractors that fail to implement physical and logical security controls for protecting classified and unclassified BMDS technical information.
- Provide oversight to ensure that contractors comply with the National Institute of Standards and Technology requirements for protecting controlled unclassified information throughout the lifecycle of the contract.

Management Comments and Our Response

The MDA Director partially agreed with our finding and recommendations, stating that he disagreed that the MDA plays a role in the contractors' inability to effectively protect BMDS technical information. However, the Under Secretary of Defense, Acquisition, Technology, and Logistics issued a memorandum related to the implementation of DFARS clause 252.204-7012 that states if an agency determines that oversight related to security requirements is necessary, they may add requirements to the terms of the contract. The significant weaknesses identified in this report support the need for the MDA to oversee the contractors' compliance with DFARS clause 252.204-7012 and National Institute of Standards and Technology requirements to ensure that the BMDS technical information maintained on contractor systems is protected against unauthorized access and disclosure. Therefore, the MDA Director should provide comments describing how the MDA plans to provide oversight of contractors to ensure compliance with DFARS clause 252.204-7012 and National Institute of Standards and Technology requirements for protecting BMDS technical information.

Although the MDA Director agreed with three recommendations, the comments did not address the specifics of the recommendations to:

- submit system security plans and associated plans of action and milestones to verify compliance with DFARS clause 252.204-7012;
- establish a separate technical evaluation factor in the source selection process; and
- take corrective actions against contractors that fail to meet Federal and DoD requirements for protecting classified and unclassified.

In addition, the MDA Director disagreed with recommendations to:

- conduct risk assessments;
- include penalty clauses in awarded contracts; and
- provide oversight to ensure that contractors.

Because the MDA Director did not address the specifics of three recommendations and disagreed with three others, the recommendations are unresolved. Please see the Recommendations Table on the next page.

Recommendations Table

Management	Recommendations Unresolved	Recommendations Resolved	Recommendations Closed
Director for Acquisition, Missile Defense Agency	1, 2, 3, 4, 5, 6	None	None

Please provide Management Comments by April 30, 2018.

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
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

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

March 29, 2018

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY, AND LOGISTICS
DIRECTOR, MISSILE DEFENSE AGENCY

SUBJECT: Logical and Physical Access Controls at Missile Defense Agency Contractor Locations (Report No. DODIG-2018-094)

We are providing this report for your review and comment. We conducted this audit in accordance with generally accepted government auditing standards.

DoD Instruction 7650.03 requires that recommendations be resolved promptly. Comments from the MDA Director did not address the recommendations. Therefore, we request additional comments on Recommendations 1, 2, 3, 4, 5, and 6. Please send a PDF file containing your comments to audcso@dodig.mil by April 30, 2018. Copies of your comments must have the actual signature of the authorizing official for your organization. We cannot accept the /Signed/ symbol in place of the actual signature. If you arrange to send classified comments electronically, you must send them over the SECRET Internet Protocol Router Network (SIPRNET).

We appreciate the courtesies extended to the staff. Please direct questions to me at (703) 699-7331 (DSN 499-7331).

Carol N. Gorman
Assistant Inspector General
Cyberspace Operations

Contents

Introduction

Objective

The objective of this audit was to determine whether Missile Defense Agency (MDA) contractors implemented security controls and processes to protect classified and unclassified ballistic missile defense system (BMDS) technical information from internal and external threats.[2] This is the first of two audits to determine whether the MDA effectively protects BMDS technical information from unauthorized access and disclosure.[3]

We selected a nonstatistical sample of 12 of 631 MDA contracts awarded to 10 different contractors. Of the 10 contractors selected, we visited 7 contractors to assess the security controls that were implemented to protect BMDS technical information. We did not visit the remaining three contractors because they either did not use BMDS technical information or the contracts had ended. All seven contractors managed unclassified BMDS technical information and five of the seven contractors managed classified BMDS technical information. We assessed controls over classified systems of only three of the five contractors because the classified systems for two contractors were not operational. See Appendix A for a discussion on the scope and methodology and Appendix B for testing methodology. See the Glossary for the technical term definitions.

Background

On April 14, 2016, the MDA Director provided testimony to the House Armed Services Subcommittee on Strategic Forces expressing concern about the potential threat to systems containing BMDS technical information, especially technical information stored on cleared Defense contractors' systems. A cleared Defense contractor is a private entity that is given clearance by the DoD to access, receive, or store classified information for the purpose of bidding for a contract or conducting activities in support of any DoD program. The MDA Director stated his belief that cleared Defense contractors may be subject to cyber attacks that allow unauthorized access to controlled technical information. As a result of the Director's testimony, the National Defense Authorization Act of FY 2017 directed the DoD Inspector General to audit the controls in place to protect classified and unclassified ballistic missile defense technical information, whether managed by cleared Defense contractors or by the Government.[4]

[2] For this report, we use the term "contractor" to mean private entities or individual facilities.

[3] For this report, "effective" means that security controls were implemented and operated as defined by the National Institute of Standards and Technology Special Publication 800-171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations," December 2016.

[4] Public Law 114-328, "National Defense Authorization Act for Fiscal Year 2017," December 23, 2016.

Ballistic Missile Defense System

The MDA's mission is to develop, test, and field a BMDS to defend the United States, its deployed forces, and its allies against enemy ballistic missiles. The BMDS is designed to destroy hostile missiles of all ranges—short, medium, intermediate, and long—and their warheads before reaching their intended targets. The BMDS architecture contains the following elements:

- networked sensors and radars (ground- and sea-based) that detect and track potential targets;
- interceptor missiles (ground- and sea-based) that destroy ballistic missiles using either direct impact or explosion; and
- a command, control, battle management, and communications network that provides operational commanders with information on the sensors and interceptor missiles.

U.S. military personnel from the U.S. Pacific Command, the U.S. European Command, the U.S. Forces Japan, the U.S. Northern Command, and the U.S. Strategic Command operate the BMDS elements.

Protecting Ballistic Missile Defense System Information

The Defense Procurement and Acquisition Policy Office, a component within the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, establishes DoD contracting and procurement policy, including Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012.[5] This DFARS clause requires contractors handling unclassified controlled technical information (UCTI) to implement security controls specified in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations" (NIST SP 800-171), by December 31, 2017.[6] NIST SP 800-171 lists security requirements created to safeguard sensitive information on non-Federal systems. These requirements include controls for user authentication, access controls, media protection, incident response, vulnerability management, and confidentiality of information. The DFARS provides examples of UCTI, such as military or space research and engineering data, engineering drawings, algorithms, specifications, technical reports, and source codes. For this report, UCTI is considered unclassified BMDS technical information.

[5] DFARS Clause 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting," October 2016.

[6] National Institute of Standards and Technology Special Publication 800-171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations," December 31, 2016.

The DoD requires Government and Defense contractor personnel to safeguard and disseminate UCTI in accordance with government-wide and DoD policies and regulations. DFARS clause 252.204-7012 requires that contractors comply with NIST SP 800-171 established security requirements for protecting the confidentiality of UCTI when such information is located on non-Federal systems, and the MDA includes DFARS clause 252.204-7012 in all new contracts related to BMDS. Although not required to, MDA officials stated that the MDA was modifying existing contracts to include the DFARS clause. For contractors handling classified information, the MDA also includes a contract requirement that contractors comply with DoD 5220.22-M, "National Industrial Security Program Operating Manual" (DoD 5220.22-M), February 28, 2006, Incorporating Change 2, May 18, 2016, to prevent the unauthorized disclosure of classified information. The DoD 5220.22-M prescribes requirements, restrictions, and other safeguards to prevent unauthorized disclosure of classified information in the hands of contractors. These requirements include controls similar to NIST SP 800-171 but tailored to classified systems and networks.[7] DoD 5220.22-M also outlines additional requirements for the handling and disposition of classified information.

The Office of the DoD Chief Information Officer develops strategy and policy for operating and protecting DoD information technology and systems and serves as the approving authority when contractors request deviations from NIST SP 800-171 requirements. According to the DoD Office of the Chief Information Officer, the MDA should include DFARS clause 252.204-7012 in all contracts to ensure the protection of BMDS technical information.

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.[8] We identified internal control weaknesses related to verifying whether contractors implemented effective physical and logical controls on networks and systems that contained BMDS technical information. Specifically, the MDA did not implement processes to verify that contractors complied with Federal and DoD requirements for protecting classified and unclassified BMDS technical information in non-Federal systems and organizations. We will provide a copy of the report to the senior official responsible for internal controls at the MDA.

[7] A network is a collection of interconnected information systems and components that transmit, receive, and exchange data.

[8] DoD Instruction 5010.40, "Managers' Internal Control Program Procedures," May 30, 2013.

Finding

Contractor Security Controls for Networks and Systems Containing Ballistic Missile Defense System Information Were Not Consistently Implemented

MDA contractors did not consistently implement security controls and processes to protect classified and unclassified BMDS technical information. Specifically, system and network administrators at three contractors that managed BMDS technical information on classified networks did not identify and mitigate vulnerabilities on classified networks and systems.[9] In addition, two contractors did not conduct risk assessments associated with systems that contained classified BMDS technical information.

Furthermore, the system and network administrators of the seven contractors that managed BMDS technical information on their unclassified networks did not consistently implement system security controls in accordance with DoD requirements for safeguarding Defense information. Specifically:

- five contractors did not enforce the use of multifactor authentication to access networks;
- four contractors did not configure systems to meet password length and complexity requirements;
- three contractors did not periodically assess the risk on information systems and assets;
- seven contractors did not always identify and mitigate network and system vulnerabilities;
- one contractor did not oversee network and boundary protection services provided by a third-party company;
- one contractor allowed users to transfer UCTI from its document management system to personal electronic devices, such as home computers;
- five contractors did not restrict the use of removable media;
- five contractors did not configure systems to automatically lock after either 15 minutes of inactivity or after three unsuccessful logon attempts;

[9] For this report, "mitigate" means to identify and implement a solution to prevent identified vulnerabilities from being exploited by malicious actors.

- five contractors did not grant system access based on the user's assigned duties and apply the principle of least privilege when granting system privileges; and
- four contractors did not maintain and review system activity logs.[10]

The DoD took steps to require contractors to protect BMDS technical information, to include requiring compliance with NIST SP 800-171 by December 31, 2017, for unclassified systems, and DoD 5220.22-M for classified systems. However, the MDA did not establish a process to verify that contractors complied with requirements to implement security controls on classified and unclassified BMDS networks and systems. If the MDA does not verify, monitor, and enforce compliance with DFARS clause 252.204-7012 and the DoD 5220.22-M requirements, contractors may be subject to cyber attacks that result in inadvertent disclosure of critical technical details of the DoD's BMDS elements to U.S. adversaries. The disclosure of technical details could allow U.S. adversaries to circumvent the BMDS capabilities, leaving the United States vulnerable to deadly missile attacks. Increasing threats of long-range missile attacks from adversaries require the effective implementation of system security controls to help reduce the number of exploitable weaknesses that attackers can use to steal and download classified and unclassified technical information.

Contractors Did Not Implement Effective System Security Controls to Protect BMDS Technical Information

MDA contractor controls and processes over systems that store, process, and transmit classified and unclassified BMDS technical information did not effectively protect against the potential unauthorized access to, or disclosure of, BMDS technical information. To determine whether contractors protected classified and unclassified BMDS technical information, we analyzed logical security controls and processes, such as authentication, vulnerability management, and the protection of stored data on the contractors' networks and systems and physical security controls, such as facility access and security at the seven contractor facilities. Based on our analyses of the seven contractors we selected, we identified control deficiencies at all seven contractors. This report contains information that may be considered contractor proprietary data. Public release of contractor proprietary

[10] Multifactor authentication combines two or more independent credentials: what the user knows (password), what the user has (security token), and what the user is (biometric verification). The goal of multifactor authentication is to create a layered defense and make it more difficult for an unauthorized person to access a computing device, network, or system. Boundary protection services include monitoring and control of communications of the logical perimeter of an information system to prevent and detect malicious and unauthorized communications.

data violates criminal provisions in title 18, United States Code 1905, "Disclosure of confidential information generally." As a result, we identify the seven contractors we reviewed as Contractors A through G to ensure that the contractors and their proprietary information are not identified. Table 1 identifies the control deficiencies at each contractor facility.

Table 1. Control Deficiencies Identified at Contractor Facilities Visited

Control Deficiencies	Contractor						
	A	B	C	D	E	F	G
Multifactor Authentication Was Not Consistently Used		X	X	X	X	X	
System Passwords Were Not Always Strong		X	X	X	X		
Contractors Did Not Periodically Conduct System Risk Assessments			X	X	X	X	X
Network and System Vulnerabilities Were Not Consistently Mitigated	X	X	X	X	X	X	X
No Oversight of Third Party Service Provider's Network Protection Activities				X			
Contractor Allowed Users to Process and Store UCTI on Personal Electronic Devices				X			
Removable Media Was Not Properly Protected	X	X		X		X	X
Systems Did Not Automatically Lock After Inactivity or Unsuccessful Logon Attempts	X	X	X		X	X	
System Access and User Privileges Were Not Consistently Granted	X		X	X	X	X	
System Activity Reports Were Not Properly Maintained and Reviewed	X	X		X		X	

Source: The DoD OIG.

Multifactor Authentication Was Not Consistently Used

Of the seven contractors we analyzed, we found that Contractors B, C, D, E, and F did not always or consistently use multifactor authentication to access unclassified networks that contained BMDS technical information.[11] 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.[12] NIST SP 800-171 requires the use of multifactor authentication to access unclassified networks for non-privileged accounts for users who do not perform security-related functions. Although two contractors configured their unclassified

[11] DoD 5220.22-M only requires single-factor authentication to access classified systems. Contractors D, E, and G complied with this requirement for its classified systems.

[12] A token is a physical object, such as an access card, used to authenticate a user's identity.

systems to support the use of multifactor authentication, the contractors did not enforce the use of multifactor authentication to access unclassified networks. For example, Contractor B partially enforced the requirement for users to access its network using multifactor authentication. Users at Contractor B accessed the network using single-factor authentication and were only required to use multifactor authentication when accessing the network remotely. The information technology director at Contractor B could not provide a reason for limiting the use of multifactor authentication to remote network access but stated that the contractor planned to fully implement multifactor authentication by December 31, 2017.[13]

Contractor E configured its laptops to use multifactor authentication; however, the desktop computers that connect to the contractor's network required only single-factor authentication, such as a username and password. Single-factor authentication is the least stringent form of authentication and presents a greater risk of unauthorized access to UCTI. The program manager at Contractor E stated that the contractor did not require the use of multifactor authentication at the time of our review because they planned to deploy a company-wide multifactor authentication solution by December 2018, a year after the December 2017 DFARS deadline.

In addition, Contractors C, D, and F did not use multifactor authentication to access networks that contained UCTI and, instead, allowed users to access networks using single-factor authentication. The security director at Contractor C and the information technology director at Contractor D stated that they did not require the use of multifactor authentication because they planned to deploy multifactor authentication solutions by the December 2017 deadline. The facility security officer at Contractor F stated that there was only one workstation that would house UCTI and that workstation would not connect to the contractor's network. Because NIST requires multifactor authentication to access contractor networks and this workstation will process and store BMDS technical information, the contractor should configure the workstation to require the use of multifactor authentication for access. NIST SP 800-171 also requires the use of multifactor authentication for privileged accounts when accessing workstations. Privileged accounts authorize privileged users to perform security related functions, such as enforcing system security policy. All users of the workstation at Contractor F are privileged account holders. Therefore, Contractor F needs to implement multifactor authentication for the workstation. The information technology administrator at Contractor F stated that it had not conducted the research necessary to identify a multifactor authentication solution.

[13] We confirmed that Contractor B began using multifactor authentication in December 2017 to access BMDS technical information.

Of the seven contractors analyzed, we found that system and network administrators at four contractors did not enforce the use of strong passwords for accessing unclassified systems.[14] Specifically, system and network administrators at Contractors B, C, and E configured systems that contain UCTI to require only an 8-character password, and Contractor D required only a 10-character password. Although the DoD requires DoD system passwords to be at least 15 characters in length, industry best practices state that the minimum password length should be set to 14 characters.[15] Contractors B, C, D, and E should have, at a minimum, configured password lengths to be at least 14 characters.

Officials from Contractors B, C, D, and E stated that they did not configure passwords to meet DoD password requirements because they considered existing password complexity configurations sufficient to control access to systems that contain UCTI. Specifically,

- the information technology director at Contractor B stated that an 8-character password was a best practice and that users are required to change passwords every 90 days;
- a program manager at Contractor C stated that the 8-character minimum password length, combined with at least three of the four complexity requirements, provided the necessary access security to its systems;
- the information systems security engineer at Contractor D stated that it believed the 10-character password would prevent users from creating simple passwords; and
- the senior security representative at Contractor E stated that the 8-character password was driven by industry standards and best practices.

Allowing users to access individual systems without using strong passwords that meet minimum industry standards increases the potential that cyber attackers could guess passwords and gain access to sensitive BMDS technical information. Cyber attackers use several methods to exploit weak passwords and gain unauthorized access to systems, such as dictionary attacks, phishing, and brute force attacks.[16] 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

[14] Defense Security Service, "Baseline Technical Security Configuration of Microsoft Windows 7 and Microsoft Server 2008 R2," Version 1.0, July 2013, updated August 7, 2015, requires passwords for classified systems to be at least 14 characters. Contractors D and E required 14 characters to access their classified systems.

[15] Application Security and Development Security Technical Implementation Guide, version 4, release 4, October 27, 2017.

[16] Phishing is a method malicious actors use to masquerade as a reputable entity or person to obtain sensitive information, such as passwords and financial information. Brute force attack is a trial and error method used to guess passwords.

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 protected by passwords. A longer, more complex password decreases the ability of hackers and others performing cyber attacks to obtain a system password.

Contractors Did Not Periodically Conduct System Risk Assessments

Of the seven contractors we analyzed, we found that Contractors C, F, and G did not assess risks associated with unclassified systems that contained BMDS technical information. NIST SP 800-171 requires periodic assessments of risk on information systems associated with processing, storing, and transmitting controlled unclassified information. Risk assessments analyze threats and vulnerabilities of information systems and potential impacts that could result in data loss and disclosure. Organizations use risk assessment results as a basis for identifying system security countermeasures needed to protect sensitive organizational missions and business processes. Contractor C performed risk assessments only at the corporate level and did not assess risks on individual unclassified systems that actually contained BMDS technical information at non-corporate facilities. Although Contractor C developed procedures for conducting risk assessments on unclassified systems, it did not actually conduct a risk assessment and continued to use the system. In addition, Contractors F and G worked with BMDS technical information on their unclassified systems (beginning in April 2016 and August 2011, respectively) without conducting systems assessments to determine the impact of threats and vulnerabilities that, if exploited, could result in the loss of BMDS technical information. The security director at Contractor C stated that he was still developing processes and procedures that would measure the likelihood of harm from the disclosure of BMDS technical information. He also stated that Contractor C would complete risk assessment worksheets as part of its system authorization packages for authentication, physical access controls, network boundary protection, and vulnerability management by October 2017. The facility security officer at Contractor F stated that he was still drafting procedures for conducting risk assessments on unclassified systems. Lastly, Contractor G did not conduct risk assessments but stated it planned to conduct a risk assessment by the end of November 2017.

Contractors D and E did not assess risks associated with classified systems that contained BMDS technical information. DoD 5220.22-M requires contractors to categorize the potential impact level for confidentiality based on the system's classification level. DoD 5220.22-M also requires contractors to monitor information systems changes that may adversely impact the security status of the

information. Although Contractor D developed a corporate policy for assessing risk on its unclassified system, it did not assess risk on its classified system. According to a security engineer, Contractor D is still developing a process for addressing risk on the systems that contain BMDS technical information.

In addition, Contractor E did not assess the risk on its classified network. According to the information system security manager, Contractor E did not perform risk assessments on its classified network because this network did not connect to the Internet. The information system security manager for Contractor E stated that its classified network relied on the annual Defense Security Service inspections to assess the risk.[17] Risk assessments include determining how adverse circumstances or events could affect an enterprise.[18]

Network and System Vulnerabilities Were Not Consistently Mitigated

Network and system administrators for the seven contractors we analyzed did not consistently mitigate known vulnerabilities on classified and unclassified networks. DoD 5220.22-M requires contractors to identify and mitigate new threats and vulnerabilities.[19] Contractors D and G did not scan workstations that stored classified BMDS technical information to identify vulnerabilities and only assessed the workstations for compliance with software baselines.[20] The system administrator at Contractor D and the information system security manager at Contractor G did not believe they needed to scan the classified workstations for vulnerabilities because the workstations did not connect to the corporate network or the Internet and because the workstations were inspected annually by the Defense Security Service to verify compliance with DoD 5220.22-M. Without a process to identify and mitigate vulnerabilities on workstations, the contractors expose workstations, including those workstations not connected to the network, to disgruntled employees who could potentially connect an infected device to the workstation and execute malicious activities.

Contractor E did not consistently scan classified workstations that contained BMDS technical information. Specifically, the contractor scanned the workstations that connected to the MDA's secure classified network but did not scan other workstations that contained classified BMDS technical information. We compared

[17] The Defense Security Service serves as an interface between the Government and cleared Defense contractors by overseeing and assisting cleared Defense contractors in protecting classified DoD information. This includes performing periodic security reviews on all cleared contractor facilities to ensure that classified information is adequately protected.

[18] An enterprise is an organization with a defined mission that uses information systems to execute that mission and that is responsible for managing its own risks and performance.

[19] DoD 5220.22-M, "National Industrial Security Program Operating Manual," February 28, 2006, Incorporating Change 2, May 18, 2016.

[20] Software baselines identify each version of software applications and facilitate the detection and correction of configuration errors.

classified vulnerability scan results from June 2017 and September 2017 at Contractor E for classified workstations that connect to the MDA's classified network and determined that Contractor E did not mitigate 483 of 1,346 network vulnerabilities. Of these 483 unmitigated vulnerabilities, 14 were high and 76 were medium vulnerabilities.[21] The information system security officer at Contractor E stated that the 14 high vulnerabilities were false-positives, but did not provide evidence that the identified vulnerabilities were actually false-positives.[22]

NIST SP 800-171 requires contractors to periodically scan systems and applications to identify vulnerabilities, mitigate those vulnerabilities, and develop plans of action and milestones when contractors are unable to mitigate vulnerabilities in a timely manner.[23] We compared unclassified network scan results from April through August 2017 for Contractors A, B, C, E, and G and found that server and workstation vulnerabilities were not mitigated in a timely manner. Table 2 lists the number of unmitigated vulnerabilities at the five contractors.

Table 2. Unmitigated Unclassified Network Vulnerabilities at Contractors A, B, C, E, and G

Contractor	Vulnerability Scan Dates	Number of Vulnerabilities Identified	Number of Unmitigated Vulnerabilities
Contractor A	April and June 2017	3,230	347
Contractor B	June and July 2017	821	9
Contractor C	May and June 2017	16	13
Contractor E	June and August 2017	600	47
Contractor G	June and July 2017	305	267

Source: The DoD OIG.

At Contractor A, we found that 347 of the 3,230 vulnerabilities identified on an April 2017 network scan remained unmitigated based on a June 2017 network scan. The 347 vulnerabilities included 61 critical and 187 high vulnerabilities. Critical vulnerabilities, if exploited, would likely result in privileged access to servers and information systems and, therefore, require immediate patches.[24] For example, an unmitigated SharePoint vulnerability identified on Contractor A's network,

[21] High vulnerabilities, if exploited, could result in elevated privileges and significant loss or downtime. Elevated privileges allow full administrative access to system resources outside of the standard user access. Medium vulnerabilities manipulate individual victims and could result in an attacker obtaining access to user privileges.

[22] A false-positive is a result from a vulnerability scan in which an identified vulnerability does not actually exist.

[23] NIST SP 800-171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations," December 2016 and NIST SP 800-171 aligns with controls described in NIST SP 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," Revision 4, April 2013, which requires organizations to define response times for mitigating vulnerabilities.

[24] Privileged access allows users to set access rights for other users.

identified in April 2017, could allow cyber attackers to execute malicious software code.[25] This would then allow the attacker to take control of the affected system.

At Contractor B, we found that 9 of the 821 vulnerabilities identified on a June 2017 network scan remained unmitigated in a July 2017 network scan. The nine vulnerabilities included seven medium and two low vulnerabilities. Medium vulnerabilities, if exploited, could result in the execution of a denial of service attack, which prevents legitimate users from accessing information and services on the contractor's system. For example, an unmitigated network vulnerability, identified in June 2017, could allow a cyber attacker to obtain password lengths, which can be used to obtain user passwords.

At Contractor C, we found that 13 of the 16 vulnerabilities identified on a May 2017 network scan remained unmitigated, based on the results from a June 2017 network scan. The 13 vulnerabilities included 5 critical vulnerabilities. For example, an unmitigated Microsoft vulnerability could allow an attacker to gain access to the system and install programs; view, change, or delete data; and create new accounts with full user privileges. Contractor C's vulnerability management program requires the contractor to mitigate critical vulnerabilities within 30 days.[26] However, 56 days after the May 2017 network scan, five critical vulnerabilities remained in the contractor's network.

At Contractor E, we found that 47 of the 600 vulnerabilities identified on a June 2017 network scan remained unmitigated in an August 2017 network scan. The 47 vulnerabilities included 22 high vulnerabilities. For example, an unmitigated Microsoft vulnerability, identified in June 2017, could allow cyber attackers to entice a user to open a malicious file, which would provide the attacker with unauthorized access to the contractor's system.

At Contractor G, we found that 267 of the 305 vulnerabilities identified on a June 2017 network scan remained unmitigated in a July 2017 network scan. The 267 vulnerabilities included 51 critical and 216 high vulnerabilities. For example, an unmitigated Microsoft vulnerability, identified in June 2017, could allow cyber attackers to remotely access files on the contractor's network, which would degrade the confidentiality and integrity of BMDS technical information.

In addition, during the audit, Contractor D conducted its first vulnerability scan on unclassified servers on May 17, 2017, even though it had worked with BMDS technical information since March 2011. The contractor also did not scan its workstations for vulnerabilities. The information technology director at

[25] SharePoint is a document management system used by Contractor A to store UCTI.

[26] Critical vulnerabilities, if exploited, could result in the compromise of servers and network devices.

Contractor D stated that, prior to the release of NIST SP 800-171, he was not aware that scanning the unclassified network and workstations for vulnerabilities was a requirement. Additionally, the information system security officer at Contractor F stated that it did not conduct vulnerability scans on the unclassified workstation that processed and stored UCTI because the contractor was still testing tools for managing vulnerabilities.

The unmitigated vulnerabilities identified at Contractors A, B, C, E, and G show they are not effectively mitigating network vulnerabilities. In addition, the contractors did not develop plans of action and milestones for vulnerabilities they were not able to mitigate. Contractor B's information technology director stated that he did not fully remediate the vulnerabilities because the only way to exploit the unmitigated vulnerability was from inside the contractor's network.[27] However, an employee with malicious intent could easily exploit these vulnerabilities and disclose BMDS technical information. Contractor E's network administrators stated that they mitigate vulnerabilities based on contractor priorities, not severity levels. This means that vulnerabilities with lower severity levels could be mitigated before those with higher severity levels. Without an effective process to ensure that vulnerabilities are identified and mitigated quickly, cyber attackers could exploit the vulnerabilities and compromise the confidentiality and integrity of BMDS technical information.

No Oversight of Third-party Service Provider's Network Protection Activities

In 2008, Contractor D contracted out 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 D 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.

The information technology director at Contractor D stated that a former company official was the only individual with the knowledge of why Contractor D entered into a contract without establishing a mutual understanding for services. The information technology director further stated that, after the official left the company, management from Contractor D requested details of the services

[27] Remediation is the act of correcting vulnerabilities or eliminating the threat by either installing a patch, adjusting configuration settings, or uninstalling a software application.

provided by the third-party service provider. However, also according to the information technology director, the third-party service provider would not provide details on the type and level of service because the third-party provider considered this to be proprietary information. The information technology director stated that contract obligations with the service provider through April 2019 prevent Contractor D from changing service providers. Contactor D expressed concerns that, if the third-party service provider experienced a breach of its networks, the third-party provider would not be obligated to notify Contractor D of the breach or whether the breach had an impact on Contractor D's networks and systems. Without proper oversight on the network protection services provided by the third-party service provider, the MDA and contractor officials have no assurance that contractor networks are properly protected.

Contractor Allowed Users to Process and Store UCTI on Personal Electronic Devices

Contractor D allowed users to process and store UCTI on contractor-managed devices without ensuring that security controls on the devices met NIST requirements. NIST SP 800-171 requires contractors to protect the confidentiality of UCTI. Contractor D allowed users to process and store UCTI on personal devices, such as laptops, tablets, and mobile phones, which are not subject to the same level of protection required by NIST. Specifically, the contractor issued software licenses to users, which they installed on personal electronic devices, allowing the users to download the BMDS technical information necessary to analyze the algorithms from the contractor's document management system. Contractor D did not require users to certify that the personal devices maintained a level of device security commensurate with NIST requirements. The MDA and Contractor D lost control of UCTI and its storage location when they allowed users to process and store UCTI on personal devices that were not configured to protect technical information.

Removable Media Was Not Properly Controlled

Of the seven contractors we analyzed, we found that officials at five contractors did not control the use of removable media on systems that contained BMDS technical information. NIST SP 800-171 requires organizations to control the use of removable media on systems that process, store, and transmit controlled unclassified information. Contractors B, D, and F allowed users to export data from systems and workstations using removable media including compact discs (CDs), universal serial bus drives (commonly known as USB drives), external hard drives, and digital versatile discs (commonly known as DVDs) without implementing safeguards to protect the information on the devices. Safeguards include restricting or limiting the use of removable media by, among other actions:

- disabling external ports used to connect the devices,
- allowing only organization-approved and -issued devices, and
- denying "write" access to the devices.

NIST SP 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," April 2013, states that organizations can use technical and nontechnical safeguards to restrict the use of removable media. An example of a technical safeguard that restricts the use of removable media is disabling ports that allow the connection of removable media.

The information technology director at Contractor B stated that instead of implementing technical safeguards to control the use of removable media, it physically controlled CDs by storing them in a locked cabinet. In addition, the facility security officer at Contractor B stated that personnel were not authorized to use USBs. However, Contractor B did not implement safeguards to restrict the use of the devices. The information technology director at Contractor D stated that it issued policy that restricted the use of removable media to contractor-issued devices. However, Contractor D did not implement controls that would prevent personnel from using unapproved removable media. Contractor F officials stated that, although they allowed personnel to use removable media, the contractor planned to install software that would allow it to control the use of removable media; however, officials did not provide a date of the installation or any evidence that the software was available.

Although Contractors A and G did not restrict the use of removable media, they implemented compensating controls to protect the information stored on the devices. For example, an official at Contractor A stated that it encrypted data copied to CDs, USBs, and DVDs instead of spending $5,000 annually to control removable media. Contractor G also encrypted data copied to USBs and planned to fully deploy software to track those devices by November 27, 2017. Although encryption does not prevent users from exporting UCTI onto removable media, it is effective at preventing unauthorized individuals from accessing specific information. Workstations that allow the use of removable media introduce opportunities for cyber attackers to execute malicious code that could infect networks and workstations and corrupt data. In addition, removable media allows individuals to easily steal and disclose critical BMDS technical information. Implementing safeguards that prohibits or restricts the use of removable media provides an added layer of protection over the confidentiality of BMDS data.

Systems Did Not Automatically Lock After Inactivity or Unsuccessful Logon Attempts

Of the seven contractors we analyzed, we found that system administrators for Contractors A, B, C, E, and F did not configure networks and systems containing BMDS technical information to lock user sessions after 15 minutes of inactivity. NIST SP 800-171 requires user sessions to lock after a predetermined time period of inactivity. Although NIST does not specify the time period, industry standards recommend locking user sessions after 15 minutes of inactivity, which aligns with the Defense Information Systems Agency Security Technical Implementation Guide for Application Security that limits inactivity to 15 minutes.[28] Contractors A, B, E, and F did not configure their networks to lock after 15 minutes of inactivity. Contractor C configured its network to lock after 30 minutes of inactivity. Automatically locking systems and user accounts within required timeframes limits the potential for unauthorized access and prevents malicious action that could jeopardize the security of BMDS technical information.

NIST SP 800-171 requires contractors handling BMDS technical information to limit unsuccessful logon attempts. Although NIST does not specify the maximum number of logon attempts, industry standards recommend locking user accounts after three unsuccessful logon attempts, which aligns with the Defense Information Systems Agency Security Technical Implementation Guide for Application Security that limits unsuccessful logon attempts to three. However, we found that system administrators for Contractors A and C did not configure user accounts to lock after three unsuccessful logon attempts. Contractor A locked user accounts only after five failed logon attempts. In addition, although Contractor C developed policy regarding terminating user sessions, a program manager at Contractor C stated that the policy did not include locking user accounts after any specific number of failed logon attempts. Contractor C's policy for terminating user sessions only applied to periods of system inactivity. Without a network configuration that locks user sessions, malicious cyber intruders would have unlimited attempts to access contractor systems. Automatically locking systems and user accounts limits the potential for unauthorized access and prevents malicious actions that could jeopardize the confidentiality and integrity of BMDS technical information.

System Access and User Privileges Were Not Consistently Granted

Of the seven contractors we analyzed, we found that system administrators for Contractors A, C, D, E, and F did not consistently grant users access to systems

[28] Application Security and Development Security Technical Implementation Guide, version 4, release 4, October 27, 2017.

containing BMDS technical information based on defined roles that aligned with user responsibilities. NIST SP 800-171 requires contractors to limit system access to authorized users. However, these five contractors did not implement a process that would ensure that only authorized personnel gained access to systems that contain BMDS technical information. For example, Contractor A granted seven individuals access to a system that contained UCTI. However, the system administrator allowed users to request access without requiring a justification and did not retain the user's access request. The system administrator for Contractor C and the information system security officer for Contractor D both stated that they granted access based on e-mail requests from managers, but that the managers did not include justifications for access. Neither Contractor C nor D implemented a formal process for granting system access. A formal access request process includes completing a standard form that requires user roles, justification for access, supervisory approval, and data owner approval. Using a standard request form for granting user access allows contractors to validate the trustworthiness of individuals requesting access to networks and systems that contain UCTI. Inappropriately granting access could potentially result in the disclosure of BMDS technical information to unauthorized individuals.

At Contractor E, we tested user access to the system that contained UCTI and identified six instances where improvements to managing access were needed. Specifically, we selected a statistical sample of 44 of 575 users from the system to validate whether access was granted appropriately (see Appendix B for sampling methodology). System administrators did not provide system access request forms for 2 of the 44 users and could not justify whether the two users' access was granted appropriately. In addition, the system administrators incorrectly granted four users access to Contractor E's systems. Specifically, two users were given access to the wrong system and two did not justify the need for access. Furthermore, the information system security officer at Contractor F granted one user elevated privileges that did not align with the user's assigned duties.

Based on Contractors A, C, D, E, and F's ineffective processes for granting system access, they could not demonstrate that users had only the appropriate level of access required to perform user duties. NIST SP 800-171 requires contractors to limit system access to the types of functions that authorized users are permitted to execute. The system administrators for Contractors A, C, D, E, and F could not ensure that users' level of access was appropriate because they did not implement a formal process to validate and grant user access. Inappropriately managing user privileges within systems containing sensitive BMDS technical information could result in assigning unauthorized elevated privileges and intentionally and unintentionally disclosing technical information.

System Activity Reports Were Not Properly Maintained and Reviewed

System administrators for Contractors A, B, D, and F did not consistently review system activity reports to assess user activity, failed login attempts, and possible data exfiltration attempts. NIST SP 800-171 requires contractors to create audit records that allow the contractors to monitor, analyze, investigate, and report unauthorized system activity. In addition, NIST SP 800-53 requires audit logs to include descriptions of user activity and all login and data exfiltration attempts. Audit logs provide automated and chronological records of system user's activity. Although Contractors A and B configured their networks to generate system activity reports, the system administrators only reviewed the reports irregularly. Contractor D did not develop a process for generating and reviewing system activity reports. In addition, although Contractor F configured the workstation to generate system activity reports, the information system security officer stated that the contractor did not review the reports for anomalies because only one individual used the workstation. However, the number of users should not determine whether system activity reviews are performed. 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.

MDA Did Not Assess Contractors' Actions for Protecting Information

The MDA did not assess the contractors' security controls or planned actions for protecting BMDS technical information on classified and unclassified networks and systems. The MDA also did not include penalty clauses in contracts to levy sanctions on contractors that did not implement required security controls to protect BMDS technical information. Significant weaknesses, as discussed in this report, show the security controls at the seven contractor locations we visited were ineffective in protecting BMDS technical information on classified and unclassified networks and systems. In October 2016, the DoD issued DFARS clause 252.204.7012, which requires contractors to protect BMDS technical information, to include requiring compliance with NIST SP 800-171 by December 31, 2017. The Under Secretary of Defense for Intelligence also issued DoD 5220.22-M in February 2006, updated in May 2016, which requires contractors to implement restrictions and safeguards for protecting classified information.

We determined that the MDA included the DFARS clause in the contracts for Contractors A, B, C, D, F, and G. The MDA attempted in 2015 and 2016 to modify the contract for Contractor E to include the DFARS requirement. However,

Contractor E stated that complying with the DFARS requirement would cost the Government approximately $10.53 million. According to MDA contracting officials, the MDA could not absorb that cost without significant impact to its budget. Therefore, the MDA did not make further attempts to include the DFARS clause in Contractor E's contract. Although the MDA did not include the clause in Contractor E's contract, the DFARS program manager at Contractor E stated that the company planned to implement security controls and processes outlined in NIST SP 800-171.

We met with the MDA's acquisitions director to determine the MDA's role in validating contractor compliance with DFARS clause 252.204.7012 and NIST SP 800-171 requirements. The MDA acquisitions director stated that the MDA planned to establish procedures during its acquisition process that would, in the future, verify whether contractors developed a plan to comply with the DFARS clause. However, the MDA did not provide a timeline for when it would deploy the procedures. In addition, according to the MDA Deputy Chief Information Officer, the MDA does not have the resources to verify whether contractors that handle BMDS technical information properly implement NIST SP 800-171 security controls and processes.

On September 21, 2017, the Director of Defense Pricing/Defense Procurement and Acquisition Policy issued guidance outlining, in part, how DoD organizations can leverage the contractor's system security plan (SSP) and associated plans of action in the contractor formation, administrations, and source selection process.[29] Although the guidance states that the DoD will not certify a contractor's compliance with the NIST SP 800-171 security requirements, contracting agencies are allowed to add requirements to contract terms if the agency determines that oversight related to security requirements is necessary. The guidance also states that during the source selection process, contracting agencies may use a potential contractor's SSP and associated plans of action and milestones (POA&Ms) to evaluate the overall risk introduced by the condition of the contractor's internal information system and network.[30] For example, a POA&M that identifies persistent weaknesses may indicate an offeror's inability to effectively implement certain security controls and, by extension, protect BMDS technical information. Together, SSPs and POA&Ms could provide critical details to the MDA regarding contractors' ability to protect BMDS technical information. The guidance further states that contracting agencies may establish a separate technical evaluation factor in the source selection process to determine compliance, or planned compliance, with the DFARS clause requirements.

[29] SSPs provide an overview of security requirements and describe security controls in place or planned for meeting those requirements.

[30] POA&Ms identify tasks and resources needed to accomplish an element of a plan and provide scheduled completion dates for meeting the tasks.

Although the MDA notified each contractor that the MDA reserved the right to conduct inspections to verify whether contractors complied with requirements for protecting UCTI, the MDA did not establish a process to execute inspections.[31] The process should include assessments of security controls for contract awardees and contract offerors that verify whether the contractor has implemented the appropriate NIST and DoD 5220.22-M controls. The process should also include imposing monetary sanctions on contractors that fail to meet Federal and DoD requirements for protecting BMDS technical information and on contractors that experienced network and system breaches as a result of ineffective security controls. Without a process for assessing the effectiveness of security controls on potential and current contractor networks and systems, the MDA risks transferring critical technical details on BMDS components and capabilities to companies whose networks and systems are vulnerable to malicious activities, including data exfiltration, unauthorized access, and disclosure of sensitive information.

Increased Risk of Unauthorized Disclosure of BMDS Classified and Unclassified Technical Information

Cleared Defense contractors use classified and unclassified BMDS technical information to produce services or products for the MDA. The DFARS requires Defense contractors to secure contractor information systems using the applicable security requirements outlined in NIST SP 800-171. Security measures, such as multifactor authentication, complex passwords, and data encryption, decrease the risk of unauthorized access to classified and unclassified BMDS technical information. In addition, identification and mitigation of vulnerabilities and regular monitoring of system activity decreases the risk that cyber attackers and unauthorized individuals will exploit system and network vulnerabilities. Furthermore, limiting access to BMDS technical information to users with a mission need to know reduces the risk of intentional or unintentional disclosures of UCTI. Defense contractors that do not implement the proper security controls to protect BMDS technical information risk disclosing critical technical details of BMDS components to U.S. adversaries. Inadequate security controls may allow U.S. adversaries to circumvent the BMDS capabilities, leaving the United States vulnerable to missile attacks that threaten the safety of U.S. citizens and critical infrastructure.

As of September 30, 2017, the MDA had awarded 198 of 578 active contracts that included classified and unclassified BMDS technical information. There are 280 contractors developing products, such as algorithms and threat

[31] DD Form 254, "DoD Contract Security Classification Specification," December 1999.

scenarios, which are critical to the success of the BMDS program. When security requirements are not applied or are ineffective, systems and networks that store, process, and transmit classified and unclassified BMDS technical information are vulnerable to data breaches, data loss and manipulation, and unauthorized disclosure of technical information. The MDA and the Defense contractors share the responsibility for ensuring that security controls are implemented to protect critical BMDS data. The MDA should assess contractors' ability to effectively protect systems that contain BMDS technical information. This includes conducting risk assessments prior to contract award and throughout the contract's lifecycle. In addition, the MDA should implement processes for evaluating a contractor's compliance with NIST and DoD security requirements and take corrective actions against contractors that fail to meet these requirements.

Management Comments to the Finding and Our Response

Management Comments to Contractor Security Controls to Protect BMDS Information

The MDA Director, responding for the MDA Director for Acquisition, disagreed with the report finding, stating that security controls at the seven contractor locations were ineffective in protecting BMDS technical information because the contractors failed to properly implement the existing security controls. The Director stated that the contractors are responsible for protecting their networks and systems that maintain critical BMDS data, and that no Federal government agency is responsible for assessing unclassified nonfederal systems. The Director also stated that DFARS clause 252.204-7012 only requires contractors to self-attest compliance with NIST SP 800-171 controls. In addition, citing a memorandum issued by the Under Secretary of Defense, Acquisition, Technology, and Logistics on September 21, 2017, the Director stated that the DoD would not certify a contractor's compliance with NIST requirements.

The Director stated that the MDA took steps to provide awareness of the DFARS clause deadline for implementing the NIST security controls and believed the MDA should receive credit for its proactive efforts. Specifically, the Director stated that the MDA developed a partnership with four major MDA prime contractors to address requirements for protecting BMDS technical information. In addition, the Director stated that the MDA developed cyber assistance teams to assess cybersecurity concerns at contractor locations that voluntarily consented to an assessment. He also stated that the MDA developed a plan to review SSPs and associated POA&Ms after the December 31, 2017, DFARS clause deadline.

The Director stated that the Defense Security Service, not the MDA, is responsible for providing oversight of contractors that maintain classified networks and ensuring that the contractors comply with the National Industrial Security Program Operating Manual. He expressed concern that the report did not delineate the legal jurisdiction, authority, and boundaries of the Government when working with nonfederal classified and unclassified information systems.

Our Response

Although the MDA Director stated that the Under Secretary of Defense, Acquisition, Technology, and Logistics memorandum states that the DoD would not certify compliance with DFARS clause 252.204-7012 and NIST SP 800-171 requirements, the memorandum also states that if an agency determines that oversight related to security requirements is necessary, they may add requirements to the terms of the contract.[32] Clearly, the significant weaknesses identified in this report substantiate the need for the MDA to oversee the contractors' compliance with the DFARS clause and NIST requirements to ensure that the BMDS technical information maintained on contractor systems is protected.

We agree that partnering with contractors and conducting cyber assessments are positive steps; however, those activities are limited in scope. The MDA's partnership with 4 of its 280 contractors represents only 1 percent of the contractors that maintain BMDS technical information. In addition, the Director did not provide details on when the MDA began partnering with the four contractors, whether the MDA and contractors identified solutions to systemic issues with implementing the NIST controls, and if lessons learned were applied to the other MDA contractors. Furthermore, as the Director stated, the MDA cyber assistance teams only conduct assessments at contractor locations that voluntarily consent to an assessment, and the assessment is not a requirement or implemented using a risk-based selection process.

The Director's statement that the MDA "developed a plan to review SSPs and associated POA&Ms" does not align with his comments to Recommendations 1, 2, and 3, in which he states the MDA **may** [emphasis added] require contractors to submit SSPs and POA&Ms as part of its source selection process. Between FYs 2015 and 2017, the DoD Cyber Crime Center received reports of 50 cyber incidents involving 15 contractors that are currently included in the universe of the MDA contractors that maintain BMDS technical information. The cyber incidents included lost or stolen equipment, attempts to gain unauthorized access to data by exploiting ineffective security controls, and other insider threat

[32] Under Secretary of Defense, Acquisition, Technology, and Logistics memorandum, "Implementation of DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting," September 21, 2017.

activities. Review of SSPs and POA&Ms as part of the source selection process, could identify offerors that have ineffective security controls or vulnerabilities and potentially avoid breaches of contractor networks and systems. Therefore, the Director needs to specify whether submitting SSPs and POA&Ms will be an offeror requirement or not.

Lastly, although the Defense Security Service, in its role as DoD's Cognizant Security Office, is responsible for providing information technology security oversight of contractors that maintain classified networks, the National Industrial Security Operating Manual states that the Defense Security Service's responsibilities do not relieve the Government from protecting and safeguarding classified information or from reviewing contractors security controls.[33] Therefore, the MDA Director's concern that the report did not define the legal jurisdiction, authority, and boundaries of the Government when working with nonfederal classified and unclassified information systems is unfounded.

Recommendations, Management Comments, and Our Response

We recommend that the Director for Acquisition, Missile Defense Agency:

1. **Revise acquisition strategies for contract proposals involving ballistic missile defense system technical information to require contract offerors to submit a system security plan and associated plans of action that shows the condition of an offeror's internal information system and network that will process, store, and transmit classified and unclassified ballistic missile defense system technical information.**

Missile Defense Agency Comments

The MDA Director, responding for the MDA Director for Acquisition, agreed, stating that the MDA **may** [emphasis added] require contractors to submit SSPs and associated POA&Ms as part of the request for proposal's statements of work, which the MDA would evaluate during the source selection process to assess the contractor's proposed security compliance status. In addition, he stated that the MDA drafted an Information Management and Control Plan that was approved as a pilot for two new MDA acquisitions. According to the Director, the plan requires vendors to: (1) identify where UCTI is collected, developed, received, transmitted, used, and stored; (2) verify compliance with the DFARS clause; (3) monitor procedures for safeguarding information; and (4) assess risk based on the implementation of the DFARS clause.[34] He also stated that the MDA

[33] The Cognizant Security Office administers industrial security on behalf of the Department of Defense.

[34] For the purposes of the report, the MDA's use of the word "vendor" is the same as "contract offeror."

would include the Information Management and Control Plan in Federal Business Opportunities when posting draft requests for proposals in January and February 2018.[35] The Director stated that the Information Management and Control Plan will "evaluate a contractor's SSP and/or POA&M in support of a program risk mitigation strategy."

Our Response

Comments from the MDA Director did not address the specifics of the recommendation; therefore, the recommendation is unresolved. Although the Director agreed with the recommendation, he stated that the MDA **may** [emphasis added] require contractors to submit SSPs and associated POA&Ms as part of the request for proposal's statements of work. Use of the word "may" does not provide assurance that the MDA will require submission of SSPs and POA&Ms and, without those documents, the MDA will not have the information needed to determine whether a contractor is capable of protecting BMDS technical information before a contract is awarded. We agree that the Information Management and Control Plan, as described by the Director, would be useful in identifying where offerors' plan to receive, process, transmit, and store BMDS technical information. However, the plan would not be effective in assessing the condition of an offeror's internal information technology system and network security before contract award because it does not contain all of the information contained in the SSPs and POA&Ms. The SSPs and POA&Ms include: (1) description of the security controls in place or planned for meeting the DFARS and NIST requirements; (2) identification of the tasks and resources needed to implement the planned security controls; and (3) scheduled completion dates for the tasks. According to the Director's description of the Information Management and Control Plan, it does not include that same information. Furthermore, it is unclear how the Information Management and Control Plan will evaluate a contractor's SSP and/or POA&M if the contractor is not required to submit those documents. Therefore, the MDA Director should provide additional comments describing how the MDA will revise its acquisition strategy to require offerors to submit SSPs and POA&Ms.

2. Establish a separate technical evaluation factor in the source selection process to evaluate whether an offeror's approach to securing its networks and systems complied with Defense Federal Acquisition Regulation Supplement clause 252.204-7012.

[35] According to the MDA, the requirement to submit an Information Management and Control Plan was included in only one of those two postings.

Missile Defense Agency Comments

The MDA Director, responding for the MDA Director for Acquisition, agreed that a scan of security documents and an analysis of vulnerabilities would provide a critical look at the state of a contractor's system. However, the Director stated that the MDA does not own nonfederal (contractor) systems and, therefore, does not have the authority or responsibility to implement the recommendation. He stated that the contractors are responsible for ensuring compliance with the DFARS clause and the NIST controls. The Director further stated that the MDA has been developing source selection criteria related to an offeror's protection of controlled unclassified information since June 2017 in addition to a procedure for validating compliance with the DFARS clause. The Director stated that the MDA **may** [emphasis added] require contractors to submit SSPs and POA&Ms as part of the request for proposal, which the MDA would use to assess the contractor's security compliance status. The Director also reemphasized the MDA's initiation of the pilot program for the Information Management and Control Plan.

Our Response

Comments from the MDA Director did not address the specifics of the recommendation; therefore, the recommendation is unresolved. We disagree that the Director has no authority or responsibility to implement the recommendation and that it is solely incumbent upon the contractor to determine compliance with Defense Federal Acquisition Regulation Supplement clause 252.204-7012. The memorandum on the implementation of DFARS clause 252.204-7012 specifically states that contracting agencies can include a separate technical evaluation factor in proposals to determine compliance with the DFARS clause. Furthermore, the MDA Director's statement that the MDA developed source selection criteria related to the protection of controlled unclassified information indicates that the MDA is aware that it can establish a separate technical evaluation factor to evaluate compliance with the DFARS clause. A separate technical evaluation factor will allow the MDA to determine whether a contractor is capable of protecting BMDS technical information before the contract is awarded by requiring offerors to describe the actions they will employ to ensure compliance with the DFARS clause. Therefore, the MDA Director should provide additional comments describing how the MDA will establish a separate technical evaluation factor to evaluate whether an offeror's approach to securing its networks and systems complies with the DFARS clause.

3. Conduct risk assessments prior to awarding contracts to evaluate the overall risk introduced by the condition of an offeror's information system and network that will process, store, and transmit ballistic missile defense system technical information and perform periodic risk assessments throughout the lifecycle of the contract.

Missile Defense Agency Comments

The MDA Director, responding for the MDA Director for Acquisition, disagreed, stating that the MDA did not have sufficient DoD authorizations or contractual authority to perform vulnerability scans on contractor-owned and -operated networks before contract award. In addition, the Director stated that the DFARS clause does not require the MDA to physically validate compliance with DFARS clause 252.204-7012 beyond the contractor's self-attestation; that the MDA was not resourced to do so; and that he did not believe it was practical to conduct cybersecurity risk assessments on contractor networks during the contract proposal and award cycle. He stated that conducting risk assessments of that magnitude would require an intensive effort that would impact cost, schedule, and performance and would require conducting comprehensive system vulnerability scans and analyses to determine risk on more than 500 prime and subcontractor networks per year. However, the Director reiterated the use of the MDA's cyber assistance team to review cybersecurity processes and operations and stated that the MDA would use the Information Management and Control Plan risk rating provided by the prime contractor to assess high-risk subcontractors.

Our Response

Comments from the MDA Director did not address the specifics of the recommendation; therefore, the recommendation is unresolved. As part of a risk assessment process, we do not expect MDA to perform vulnerability scans of contractor networks prior to contract award. The implementation memorandum for DFARS clause 252.204-7012 acknowledges that SSPs and POA&Ms may be used to provide the agencies the ability to evaluate the overall risk introduced by the condition of contractor networks and systems. Therefore, action taken in response to Recommendation 1 to require submission of SSPs and POA&Ms would provide the information needed to conduct a risk assessment of the offerors' ability to protect the systems that contain BMDS technical information. In addition, the MDA could use the SSPs and POA&Ms to periodically assess the contractors' continued ability to protect BMDS technical information.

Furthermore, while the use of the MDA cyber assistance teams may be useful in identifying security weaknesses, the visits by the teams are voluntary, and neither contractors nor subcontractors are required to consent to the MDA's review of

their processes and operations. The MDA Director should provide additional comments describing how the MDA plans to conduct risk assessments to evaluate the condition of offerors' networks and systems prior to contract award and periodically assess risk on contractors' networks and systems throughout the lifecycle of the contract.

4. **Include penalty clauses in awarded contracts to levy monetary sanctions on contractors that fail to implement physical and logical security controls for protecting classified and unclassified ballistic missile defense system technical information.**

Missile Defense Agency Comments

The MDA Director, responding for the MDA Director for Acquisition, disagreed, stating that the MDA is not focusing on punishing contractors financially but on strengthening network protections and business practices for improving information protection. The Director stated that a "liquidated damages" clause would be more appropriate than imposing fines for noncompliant contractors, which he stated would be counterproductive to the MDA's goal of protecting UCTI.[36] However, the Director stated that the MDA was working with contractors to ensure that preliminary controls were in place to protect BMDS technical information and that the MDA would continue to assess when and how to use penalty clauses, award fees, and incentive fees as a way to encourage future compliance with DoD policy.

Our Response

Comments from the MDA Director did not address the specifics of the recommendation; therefore, the recommendation is unresolved. We disagree that liquidating damages is appropriate for levying monetary sanctions against contractors that fail to implement the proper security controls. According to the Federal Acquisitions Regulation Subpart 11.5, "Liquidating Damages," agencies should use liquidating damages clauses only when timely delivery or performance is critical or when the extent or the amount of damages is difficult or impossible to estimate or prove. However, the Federal Acquisition Regulation allows agency heads to reduce or waive the amount of liquidating damages assessed under a contract. Penalty clauses are more appropriate because the MDA could impose the penalties when contractors default on contract requirements, such as, in this instance, complying with the DFARS clause and implementing NIST requirements. The significant security weaknesses identified at the seven contractors we assessed demonstrates a need to include penalty clauses in contracts to hold contractors accountable for failing to implement the proper security controls to protect BMDS

[36] Liquidated damages is a type of actual damage that often appears in contracts and is used when actual damages are difficult or impossible to prove.

technical information. The MDA Director should provide additional comments describing how the MDA will levy monetary sanctions on contractors that fail to comply with the DFARS clause.

5. Provide oversight to ensure that contractors comply with the National Institute of Standards and Technology requirements for protecting controlled unclassified information throughout the lifecycle of the contract.

Missile Defense Agency Comments

The MDA Director, responding for the MDA Director for Acquisition, disagreed, stating that incorporating continuous monitoring of contractor networks was cost prohibitive and not within DoD authorizations and contractual authority. The Director reiterated the contractors' self-attestation requirement and stated that the DFARS clause does not require the agencies to monitor compliance with DoD or NIST requirements. The Director also reiterated the use of its cyber assistance teams, based on availability of resources, to assess nonfederal (contractor) information systems it considers medium to high risk. In addition, the Director stated that the best cybersecurity practices memorandum issued on January 12, 2018, stresses the need for contractors to be vigilant in applying NIST controls to provide increased protection of BMDS information.

Furthermore, in the Director's response to Recommendation 4, he stated that the MDA **may** [emphasis added] initiate an evaluation requirement in the Contractor Performance Assessment Reporting System related to the implementation of the DFARS clause. According to the Director, during annual evaluations, agencies would be able to document contractors' performance in maintaining information security on their networks, and unsatisfactory performance evaluations would require contractors to explain corrective actions to meet statement of work requirements. He stated that using the Contractor Performance Assessment Reporting System would allow the MDA to provide reasonable oversight of contractor performance and take discretionary corrective action as needed. Likewise, the Director stated that the MDA issued a memorandum on January 12, 2018, discussing best cybersecurity practices that aligned with recurring NIST control shortfalls and that stressed the need for contractors to be vigilant in applying NIST security controls to provide increased protection of BMDS information.[37]

Our Response

Comments from the MDA Director did not address the specifics of the recommendation; therefore, the recommendation is unresolved. Without oversight, security weaknesses, such as the significant security weaknesses identified in

[37] MDA Memorandum, "MDA Cybersecurity Best Practices," January 12, 2018.

this report, leave critical BMDS technical information vulnerable to compromise. This should compel the Director to implement procedures that provide oversight of contractor efforts to ensure that contractors are properly protecting BMDS technical information from unauthorized access and disclosure. While the implementation memorandum for DFARS clause 252.204-7012 cited by the Director states that agencies were not required to monitor contractor compliance with the DFARS clause, the memorandum does state that agencies could add oversight requirements to the terms of the contract if an agency determines that oversight related to security requirements is necessary. In addition, while the use of the MDA cyber assistance teams may be useful in identifying security weaknesses, the visits by the teams are voluntary, and contractors are required to consent to the MDA's review of their processes and operations. If the MDA does not conduct oversight activities to verify whether contractors effectively implemented appropriate NIST controls, the MDA ignores the risks associated with weak security controls, such as the exfiltration of critical technical data to U.S. adversaries.

In addition, the best practices memorandum described by the Director does not offer suggestions for reducing the shortfalls in areas such as user access, external devices usage, and vulnerability management. The memorandum lists 15 technical items that, if not addressed, would result in high-impact issues. In this report, we determined that the contractors we assessed did not effectively implement 7 of the 15 technical items, with shortfalls in the following areas.

- Enabling multifactor authentication
- Enforcing password complexity
- Conducting risk assessments
- Controlling the use of removable media
- Limiting logon attempts and locking systems after period of inactivity
- Identifying system flaws (vulnerability management)
- Deploying security patching (vulnerability mitigation)

Providing guidance to contractors on how to address the identified shortfalls would be a more effective method of assisting contractors in protecting BMDS technical information.

Although the Director discussed using the Contractor Performance Assessment Reporting System annual evaluation process to oversee contractor performance to determine whether corrective actions are necessary in Recommendation 4, his comments are relevant to this recommendation. While the Director stated that the MDA could use the Contractor Performance Assessment Reporting System annual evaluation process as an oversight tool, the Director did not state that the MDA

took steps to do so. However, using the annual evaluation process as a sole source of oversight is problematic because it would only require contractors to address critical and high vulnerabilities once a year. The Director's suggested method for taking discretionary action against contractors only once per year will not address the need to take immediate actions to reduce the risk of cyber attackers exploiting those weaknesses and gaining unauthorized access to BMDS technical information that is critical to national security. The Director should provide additional comments describing the MDA's specific plans to provide oversight of contractors' compliance with NIST requirements for protecting controlled unclassified information throughout the lifecycle of the contract.

6. Take corrective actions against contractors that failed to meet the National Institute of Standards and Technology and DoD requirements for protecting classified and unclassified ballistic missile defense system technical information.

Missile Defense Agency Comments

The MDA Director, responding for the MDA Director for Acquisition, agreed, but reiterated that the DFARS clause only requires contractors to self-attest compliance with NIST controls and that the DFARS clause does not require the MDA to monitor compliance with DoD or NIST requirements. The Director also reiterated that the MDA **may** [emphasis added] initiate an evaluation requirement in the Contractor Performance Assessment Reporting System, which the Director stated would allow agencies to document whether contractors' successfully performed network security actions. In addition, the Director stated that unsatisfactory performance evaluations would require contractors to explain corrective actions and that the MDA would use the evaluation reporting as leverage for taking discretionary corrective action as needed.

Our Response

Comments from the MDA Director did not address the specifics of the recommendation; therefore, the recommendation is unresolved. While the Director stated that the MDA could use the Contractor Performance Assessment Reporting System annual evaluation process as a method for taking action against contractors that fail to meet the requirements of the DFARS clause, the Director did not state that the MDA took steps to do so. However, using the annual evaluation process as a sole source of taking action against contractors is problematic because it would only require contractors to implement corrective actions once a year. Providing oversight throughout the lifecycle of the contract is the only effective way of ensuring contractors take appropriate actions to protect BMDS technical information. In addition, while unsatisfactory performance evaluation

ratings could impact a contractor's ability to obtain future defense contracts, unsatisfactory evaluations would not always result in contractors correcting security weaknesses in a timely manner. We believe that contractor networks would remain vulnerable to unauthorized access or use and exploitation by cyber attackers if weaknesses are not corrected in a timely manner and if the MDA only assesses contractors' network security actions once a year. Allowing contractors to continue accessing BMDS technical information after they demonstrated an inability or unwillingness to protect the information properly is irresponsible. Therefore, the MDA should provide comments describing the MDA's additional plans to take corrective actions on contractors that do not correct, strengthen, or implement security controls in a timely manner.

Appendix A

Scope and Methodology

We conducted this performance audit from March through December 2017 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

To understand the process used to protect classified and unclassified BMDS technical information, we interviewed officials from the MDA, the DoD Office of the Chief Information Officer, and the Office of Defense Procurement and Acquisition Policy. We also interviewed system owners, chief information officers, system administrators, developers, and users at select contractor locations to identify security protocols implemented to protect classified and unclassified BMDS technical information. Additionally, we reviewed Federal laws and DoD and MDA policy concerning DFARS clause 252.204-7012 and requirements for security controls on unclassified and classified systems and networks to protect BMDS technical information.

Personnel from the MDA's contracting office provided a universe of 631 active MDA Defense contracts as of January 30, 2017. We nonstatistically selected 12 contracts awarded to 10 contractors based on the number of past cyber incidents reported to the Defense Cyber Crime Center, contract face value, and the contractor size (small businesses and medium to large businesses). Of the 10 contractors selected, we visited 7 contractors to assess security controls implemented to protect BMDS technical information. The remaining three contractors either did not use BMDS technical information or the contracts had ended. Therefore, we did not visit those three contractors (see Appendix B for more details on the sampling methodology).

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

- boundary defense;
- 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;
- protection of BMDS technical information from unauthorized modification and deletion;
- audit logging;
- security incident handling and response;

- risk assessment;
- system maintenance; and
- workforce security.

The contractors were provided the opportunity to review and comment on relevant portions of the draft report. Comments provided by the contractors were considered in preparing the final report.

Use of Computer-Processed Data

We used computer-processed data that MDA contract personnel extracted from the Federal Procurement Data System and provided to us in Excel spreadsheets. We used the data to develop a universe of active contracts. We used the list of contracts to select individual contractors that managed BMDS technical information to visit. However, the list of contracts was not sufficiently reliable to determine whether contractors had active MDA contracts and worked with unclassified and classified BMDS technical information. To assess the reliability of the data, we contacted the 10 contractors to verify that the contract was active and that the contractor worked with BMDS technical information. Two contracts ended in October 2016 and one contract did not use the MDA or BMDS technical information. Therefore, we did not visit those three contractors. Subsequently, our audit focused on the remaining seven contractors on the list.

We also used computer-processed data from unclassified and classified systems to generate a universe of users at each site visited. System administrators from the contractors provided us with extracts of active and inactive users from the systems as NotePad and Adobe Acrobat files. We used the universe of users to select a sample of users to verify the appropriateness of users' access and privileges. We compared system access requests for the selected users, when available, to the user lists to verify that system account administrators granted access only to personnel with a documented need for access to networks and systems that contained classified and unclassified BMDS technical information. In addition, we verified that the selected users' access within contractor systems and networks aligned with their assigned duties. When formal system access requests were not available, we interviewed system account administrators at each contractor site to determine whether users' system access aligned with assigned duties.

Use of Technical Assistance

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

Prior Coverage

No prior coverage has been conducted on the security controls and processes to protect classified and unclassified BMDS technical information during the last 5 years.

Appendix B

The audit used two different sampling approaches: one approach to select a sample of contractors to analyze and one approach to select a sample of users at each contractor facility visited to test system access and privileges. The audit team used non-statistical sampling to ensure representation of different types of contracts across the population of active MDA contracts.

The MDA provided the audit team a list of 631 contracts that the MDA identified as active as of January 30, 2017. The request for the contracts list specified all contracts handling BMDS technical information, whether classified or unclassified. The MDA classified each contract using several criteria including whether the contractor was a "Small Business" or "Other than Small Business."

The audit team also requested and received mandatory cyber incident reports, which contractors self-reported from FYs 2015 through 2017 in the Defense Cyber Crime Center. We then established three cyber incident categories which we coded as follows:

- "1" if the contractor did not report any cyber incidents in FYs 2015 through 2017;
- "5" if the contractor reported one cyber incident in FYs 2015 through 2017; and
- "10" if the contractor reported more than one cyber incident in FYs 2015 through 2017.

We identified each contract by the contractor's cyber incident category. Table 3 provides the breakdown of the type of contractor selected based on cyber incident categories.

Table 3. Contract Universe by Incident Rating and Business Category

Cyber Incident Rating	Small Business	Other Than Small Business	Total
None	393(2)	149(2)	542(4)
One	5(3)	12(2)	17(5)
More Than One	1(1)	71(2)	72(3)
Total	399(6)	232(6)	631(12)

*Numbers in parentheses indicate the number of contractors selected.
Source: The DoD OIG.

We considered resources, time available, and project objectives and selected a non-statistical sample of 12 contracts.[38] We selected the two contracts with the highest and lowest value in each business size category. There was only one Small Business contract with more than one cyber incident report so we selected an additional low value Small Business contract in its place to have six Small Business contracts to include in the sample.

The audit team also used statistical testing to test contractor compliance for system access controls. Among the sampled contracts, there were only seven contractor systems that met our criteria for testing system access controls. We used internal controls testing standards to determine the sample sizes to use: if there were no errors observed, we could conclude, with 90 percent confidence, that the error rate was under five percent (pass).[39] If the error rate exceeded the pass rate of five percent, the system was considered a failure. Table 4 shows the results of our compliance testing.

Table 4. Internal Controls Test of User Access Controls

System	Number of Users	Users Tested	Result
1	7	7	Fail
2	22	22	Pass
3	22	22	Fail
4	575	44	Fail
5	126	33	Fail
6	168	36	Fail
7	3	3	Fail
Total	923	167	Fail

Source: The DoD OIG.

[38] The 12 contracts involved 10 different contractors. When we contacted the 10 contractors to set up site visits, we found that two of the contracts had ended and one other contract did not involve BMDS technical information. We therefore conducted seven site visits involving nine contracts.

[39] Council of the Inspector General on Integrity and Efficiency, "The Journal of Public Inquiry," Fall/Winter 2012-2013.

Management Comments

Missile Defense Agency Comments

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

IR

FEB 01 2018

MEMORANDUM FOR PROGRAM DIRECTOR FOR READINESS AND CYBER OPERATIONS, DEPARTMENT OF DEFENSE INSPECTOR GENERAL

SUBJECT: Missile Defense Agency Response to Logical and Physical Access Controls at Missile Defense Agency Contractor Locations (Project No. D2017-D000RF-0097.000, dated December 19, 2017)

Thank you for the opportunity to review the draft report "Logical and Physical Access Controls at Missile Defense Agency Contractor Locations (Project No. D2017-D000RF-0097.000)." Attached is the Missile Defense Agency comments to include the Security Marking Review Response. My point of contact for this effort is Ms. Carolyn Frye, 571-231-8286, carolyn.frye@mda.mil.

SAMUEL A. GREAVES 2/1/18
Lieutenant General, USAF
Director

Attachments:
As stated

MDA COMMENTS MATRIX: DoD IG Audit of the Effectiveness of Logical and Physical Access Controls Over BMDS Information (Project No. D2017-D000RF-0097.000) – DRAFT REPORT
(Please read instructions on back before completing form.)

#	Class	Component and POC Name, Phone, and E-mail	Page #	Para #	Comment Type (A/C/S)	Comments, Justification, and Originator Justification for Resolution	A/R/P
1	U		21	Rec. No. 1	N/A	**Coordinator Comment**: **AGREE** with recommendation 1. Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, requires contractors to implement National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171r1, Protecting Controlled Unclassified Information in Nonfederal Information Systems and requires only contractor self-attestation to confirm compliance with the DFARS and NIST SP 800-171r1 controls. Office of the Undersecretary of Defense (OUSD)-Acquisition Technology and Logistics (AT&L)-Defense Procurement and Acquisition Policy (DPAP) memo (Sep 21, 2017), Implementation of DFARS Clause 252.204-7012, confirms that contractors need only self-attest to meeting the DFARS 252.204-7012 requirements and implement NIST 800-171r1 controls. The September DPAP memo includes six (6) pages of detailed guidance, developed cooperatively by DPAP, DoD Chief Information Officer (CIO), and Deputy Assistant Secretary of Defense-Digital Engineering (DASD-DE), to help support successful implementation of the DFARS and the associated NIST 800-171r1 controls by contractors in their nonfederal systems. It also addresses the use and preparation of a System Security Plan (SSP) and Plan of Action and Milestone (POA&M), referenced in DFARS 252.204-7012, for documenting how a contractor will implement the NIST 800-171r1 controls on its network; the SSP and any POA&M should be in place on awarded contracts as of Dec 31, 2017. The POA&M should detail a contractor's plan to mitigate its non-compliance of any of the NIST 800-171r1 controls as addressed in its SSP and self-attestation. The DPAP guidance does not require submission of the SSP and POA&M, although it encourages requiring activities to use SSPs and POA&Ms in the evaluation process as a means to assess overall risk of a proposal and the state of the offeror's internal information system and network. **Coordinator Justification**: Contractors had until December 31, 2017 to implement NIST SP 800-171r1, included in DFARS 252.204-7012, and to prepare a SSP and POA&M, to document compliance and any mitigation, as applicable, with the DFARS and NIST SP 800-171r1 requirements. As part of its information security planning, MDA drafted an Information Management and Control Plan (IMCP). The IMCP	

MDA FORM 100 JUL 2017 PREVIOUS VERSIONS OBSOLETE 1

Attachment 1

MDA COMMENTS MATRIX: DoD IG Audit of the Effectiveness of Logical and Physical Access Controls Over BMDS Information (Project No. D2017-D000RF-0097.000) – DRAFT REPORT
(Please read instructions on back before completing form.)

#	Class	Component and POC Name, Phone, and E-mail	Page #	Para #	Comment Type (A/C/S)	Comments, Justification, and Originator Justification for Resolution	A/R/P
						requires the vendor to: identify full supply chain where Controlled Unclassified Information (CUI) is collected, developed, received, transmitted, used or, or stored; verify flow down of DFARS 252.204-7012 to all applicable subcontractors; verify NIST SP 800-171r1 compliance; verify and monitor information safeguarding procedures throughout the supply chain; assess risk based upon DFARS 252-204.7012 implementation. The Draft IMCP is currently approved as a pilot for two new Agency acquisitions and will be included in the respective Draft Request for Proposals (RFPs) (Federal Business Opportunities (FBO) postings planned in January and February 2018). MDA may require contractor submission of a SSP and POA&M as part of the RFP Statement of Work (SOW)/Performance Work Statement (PWS), those documents will be evaluated during source selection to assess the contractor's proposed security compliance status. Under DFARS 252.204-7012, the government, MDA in this case, is not required and not resourced to validate a contractor's actual or physical compliance beyond its self-attestation of compliance with DFARS 252.204-7012. As stated in the Sept 21 DPAP implementation memo, "DFARS clause 252.204-7012 does not add any other unique or additional requirements for the government to monitor contractor implementation of NIST SP 800-171r1 or to monitor compliance with any other requirement of that clause." As a result, the MDA IMCP, in draft status, will evaluate a contractor's SSP and/or POA&M in support of a program risk mitigation strategy.	
2	U		21	Rec. No. 2	S	**Coordinator Comment**: **AGREE** with recommendation 2. MDA does not own nonfederal systems and does not have the authority or responsibility to implement Recommendation 2, evaluating whether an offeror's approach to securing its networks and systems complies with DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, requires contractors to implement NIST SP 800-171r1, Protecting Controlled Unclassified Information in Nonfederal Information Systems. Contractor Self-Attestation for meeting NIST SP 800-171r1 controls is the standard required by OSD-AT&L/Defense	

MDA FORM 100 JUL 2017 PREVIOUS VERSIONS OBSOLETE 2

Attachment 1

MDA COMMENTS MATRIX: DoD IG Audit of the Effectiveness of Logical and Physical Access Controls Over BMDS Information (Project No. D2017-D000RF-0097.000) – DRAFT REPORT
(Please read instructions on back before completing form.)

#	Class	Component and POC Name, Phone, and E-mail	Page #	Para #	Comment Type (A/C/S)	Comments, Justification, and Originator Justification for Resolution	A/R/P
						Procurement and Acquisition Policy (DPAP). The System Security Plan (SSP) and Plan of Action and Milestone (POA&M) referenced in DFARS clause 252.204-7012 addresses how the contractor will implement the NIST 800-171r1 controls on their network. The POA&M will detail mitigation steps and schedule for non-compliant controls as addressed in the contractor SSP. As stated in the Sept 21 DPAP implementation memo, "DFARS clause 252.204-7012 does not add any other unique or additional requirements for the government to monitor contractor implementation of NIST SP 800-171r1 or to monitor compliance with any other requirement of that clause." **Coordinator Justification**: Contractors who self-attest had until December 31, 2017 to implement NIST SP 800-171r1. MDA may require SSPs and POA&Ms as part of the SOW/PWS within the associated RFP and at source selection. Contractors cannot assume that compliance with NIST SP 800-171r1 means they are fully protected from unauthorized disclosure of technical information. The vendors will also need to control information flow throughout the supply chain, distributing only the necessary data for subcontractors to complete necessary work and minimize impacts of any unauthorized disclosure or data loss. Since June 2017, MDA has been developing specific source selection criteria related to the contractor's protection of Controlled Unclassified Information (CUI) in addition to a procedure to validate compliance with the DFARS 252.204-7012 clause. As part of its information security planning, MDA drafted an Information Management and Control Plan (IMCP). The IMCP requires the vendor to: identify full supply chain where Controlled Unclassified Information (CUI) is collected, developed, received, transmitted, used or, or stored; verify flow down of DFARS 252.204-7012 to all applicable subcontractors; verify NIST SP 800-171r1 compliance; verify and monitor information safeguarding procedures throughout the supply chain; assess risk based upon DFARS 252-204.7012 implementation. The Draft IMCP is currently approved as a pilot for two new Agency acquisitions and will be included in the respective Draft RFPs (FBO postings planned in February 2018). MDA may require contractor submission of a SSP and POA&M as part of the RFP SOW/PWS, those documents will	

MDA FORM 100 JUL 2017 PREVIOUS VERSIONS OBSOLETE 3

Attachment 1

MDA COMMENTS MATRIX: DoD IG Audit of the Effectiveness of Logical and Physical Access Controls Over BMDS Information (Project No. D2017-D000RF-0097.000) – DRAFT REPORT
(Please read instructions on back before completing form.)

#	Class	Component and POC Name, Phone, and E-mail	Page #	Para #	Comment Type (A/C/S)	Comments, Justification, and Originator Justification for Resolution	A/R/P
						be evaluated during source selection to assess the contractor's proposed security compliance status. MDA reserves the right to tailor each unique acquisition. Other than a contractor's self-attestation of DFARS 252.204-7012 compliance and agency review of a contractor's SSP and POA&M, a scan of artifacts and analysis of vulnerabilities would provide a critical look at the state of a contractor's system cybersecurity hygiene.	
3	U		21	Rec. No. 3	S	**Coordinator Comment**: **DISAGREE** with recommendation 3. Under DFARS 252.204-7012, the government, MDA in this case, is not required and not resourced to validate a contractor's actual or physical compliance beyond its self-attestation of compliance with DFARS 252.204-7012. Additionally, MDA does not have the DoD Agency authorizations or contractual authorities to conduct risk assessments on offerors before a contractor is selected and a contract is awarded. DFARS clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting requires contractors to implement NIST SP 800-171r1, Protecting Controlled Unclassified Information in Nonfederal Information Systems. Contractor self-attestation for meeting NIST SP 800-171r1 controls is the standard required by OSD-AT&L/Defense Procurement and Acquisition Policy (DPAP). The System Security Plan (SSP) and Plan of Action and Milestone (POA&M), referenced in DFARS clause 252.204-7012, addresses how the contractor will implement the NIST 800-171r1 controls on their network. The POA&M will detail mitigation steps of non-compliant controls based off the contractor self-attestation. As stated in the Sept 21 DPAP implementation memo, "DFARS clause 252.204-7012 does not add any other unique or additional requirements for the government to monitor contractor implementation of NIST SP 800-171r1 or to monitor compliance with any other requirement of that clause."	

MDA COMMENTS MATRIX: DoD IG Audit of the Effectiveness of Logical and Physical Access Controls Over BMDS Information (Project No. D2017-D000RF-0097.000) – DRAFT REPORT
(Please read instructions on back before completing form.)

#	Class	Component and POC Name, Phone, and E-mail	Page #	Para #	Comment Type (A/C/S)	Comments, Justification, and Originator Justification for Resolution	A/R/P
						Coordinator Justification: Contractors who self-attest had until December 31, 2017 to implement NIST SP 800-171r1. MDA may require SSPs and POA&Ms as part of the SOW/PWS within the associated RFP and at source selection. Conducting thorough cybersecurity risk assessments on actual networks is a work intensive effort that impacts cost, schedule, and performance. Actual live assessments require comprehensive system vulnerability scans and subsequent analysis to make an informed risk decision that are not practical in a proposal and award cycle. In addition, absent consent from an industry partner/contractor, MDA does not have sufficient DoD authorizations or contractual authorities to perform a vulnerability scan on contractor owned and contractor-operated networks prior to, or after, contract award. MDA contractors may volunteer for a MDA Cyber Assistance Team (CAT) visit and consent to the associated MDA review of their cybersecurity processes or operations, as applicable. However, as part of its information security planning, MDA drafted an Information Management and Control Plan (IMCP). The IMCP requires the vendor to: identify full supply chain where Controlled Unclassified Information (CUI) is collected, developed, received, transmitted, used or, or stored; verify flow down of DFARS 252.204-7012 to all applicable subcontractors; verify NIST SP 800-171r1 compliance; verify and monitor information safeguarding procedures throughout the supply chain; assess risk based upon DFARS 252-204.7012 implementation. The Draft IMCP is currently approved as a pilot for two new Agency acquisitions and will be included in the respective Draft RFPs (FBO postings planned in February 2018). MDA may require contractor submission of a SSP and POA&M as part of the RFP SOW/PWS, those documents will be evaluated during source selection to assess the contractor's proposed security compliance status. The magnitude of this task could mean testing over 500 contractor networks per year, including prime and subcontractor networks. In the interim, MDA will utilize the IMCP risk rating, provided by the prime, to focus our limited resources on the high-risk subcontractors, via Cyber Assistance Team (CAT) visits.	

Attachment 1

MDA COMMENTS MATRIX: DoD IG Audit of the Effectiveness of Logical and Physical Access Controls Over BMDS Information (Project No. D2017-D000RF-0097.000) – DRAFT REPORT
(Please read instructions on back before completing form.)

#	Class	Component and POC Name, Phone, and E-mail	Page #	Para #	Comment Type (A/C/S)	Comments, Justification, and Originator Justification for Resolution	A/R/P
4			21	Rec. No. 4	S	**Coordinator Comment**: **DISAGREE** with recommendation 4. DFARS clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, requires contractors to implement NIST SP 800-171r1, Protecting Controlled Unclassified Information in Nonfederal Information Systems and requires only contractor self-attestation to confirm compliance with the DFARS and NIST SP 800-171r1 controls. OUSD-AT&L-Defense Procurement and Acquisition Policy (DPAP) memo (Sep 21, 2017), Implementation of DFARS Clause 252.204-7012, confirms that contractors need only self-attest to meeting the DFARS 252.204-7012 requirements and implement NIST 800-171r1 controls. The September DPAP memo includes six (6) pages of detailed guidance, developed cooperatively by DPAP, DoD CIO, and DASD-DE, to help support successful implementation of the DFARS and the associated NIST 800-171 r1 controls by contractors in their nonfederal systems. As stated in the Sept 21 DPAP implementation memo, "DFARS clause 252.204-7012 does not add any other unique or additional requirements for the Government to monitor contractor implementation of NIST SP 800-171r1 or to monitor compliance with any other requirement of that clause." **Coordinator Justification**: As the requirements of NIST SP 800-171r1 continue to evolve, MDA will maintain an open dialogue with its Contractor base on the implementation, use and improvement of these controls. Asking vendors to conduct an assessment and then "Fining" them for non-compliance after completing the voluntary assessment would be counterproductive to our goal of protecting CUI. As the controls mature and we have clearer implementation guidance a "Liquidated Damages" type of clause would be appropriate. However, at this stage of initial implementation, we are working with our industry partners to get preliminary controls in place to protect the information throughout the supply chain. MDA may initiate a special evaluation requirement in CPARS related to cybersecurity and the implementation of DFARS clause 252.204-7012. As part of each contractor's annual evaluation of performance, the agency will evaluate and document contractor performance in maintaining information security within their networks and supply	

MDA COMMENTS MATRIX: DoD IG Audit of the Effectiveness of Logical and Physical Access Controls Over BMDS Information (Project No. D2017-D000RF-0097.000) – DRAFT REPORT
(Please read instructions on back before completing form.)

#	Class	Component and POC Name, Phone, and E-mail	Page #	Para #	Comment Type (A/C/S)	Comments, Justification, and Originator Justification for Resolution	A/R/P
						chain. Unsatisfactory CPARS evaluations require vendor responses and corrective action plans to meet SOW/PWS requirements. Use of the CPARS tool as the initial evaluation of performance will provide reasonable oversight and evaluation of contractor performance as well as leverage for taking discretionary corrective action when needed. MDA is not focusing on punitive measures to punish, even financially, the contractors who support the BMDS while the most significant cyber threat to MDA is an attack to its industrial base. Rather, MDA is focused on working with our program and industry partners to strengthen network protections and associated business practices to improve information protection to mitigate or prevent its loss. The MDA Director, Lt Gen Greaves, recently signed a MDA Cybersecurity Best Practices memorandum (Attachment 1a) to all MDA prime contractors to share key best practices and lessons learned related to cybersecurity standards and hygiene. The memo aligns frequently recurring NIST SP 800-171r1 control shortfalls to identified threat vectors within the DIB (spear phishing, credential harvesting, and unsecure perimeter infrastructure); the memo encapsulates the need for increased focus and vigilance when applying NIST SP 800-171r1 controls and therefore provide increased protection of MDA's BMDS information across the DIB. The Best Practices memo is the second of two memos issued from the MDA Director to prime contractors as a means to spread cybersecurity awareness, assist with translation, timelines, and expectations from MDA contractors regarding DFARS 252.204-7012 compliance. The agency will continue to assess when and how the use of a penalty clause or award fee or incentive fee, as applies, may be appropriate to incentivize contractor compliance in the future or as required by DoD policy.	
5	U		22	Rec. No. 5	S	**Coordinator Comment**: **DISAGREE** with recommendation 5. DFARS clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, requires contractors to implement NIST SP 800-171r1, Protecting	

MDA FORM 100 JUL 2017 PREVIOUS VERSIONS OBSOLETE 7

Attachment 1

MDA COMMENTS MATRIX: DoD IG Audit of the Effectiveness of Logical and Physical Access Controls Over BMDS Information (Project No. D2017-D000RF-0097.000) – DRAFT REPORT
(Please read instructions on back before completing form.)

#	Class	Component and POC Name, Phone, and E-mail	Page #	Para #	Comment Type (A/C/S)	Comments, Justification, and Originator Justification for Resolution	A/R/P
						Controlled Unclassified Information in Nonfederal Information Systems and requires only contractor self-attestation to confirm compliance with the DFARS and NIST SP 800-171r1 controls. OUSD-AT&L-Defense Procurement and Acquisition Policy (DPAP) memo (Sep 21, 2017), Implementation of DFARS Clause 252.204-7012, confirms that contractors need only self-attest to meeting the DFARS 252.204-7012 requirements and implement NIST 800-171 controls. The September DPAP memo includes six (6) pages of detailed guidance, developed cooperatively by DPAP, DoD CIO, and DASD-DE, to help support successful implementation of the DFARS and the associated NIST 800-171 r1 controls by contractors in their nonfederal systems. As stated in the Sept 21 DPAP implementation memo, "DFARS clause 252.204-7012 does not add any other unique or additional requirements for the Government to monitor contractor implementation of NIST SP 800-171r1 or to monitor compliance with any other requirement of that clause." **Coordinator Justification**: MDA will oversee contractor implementation of the requirements of DFARS 7012, NIST SP 800 171r1, only in accordance with OSD guidance and policies for safeguarding covered defense information. Over the past year, the agency modified many of the MDA contracts, as applicable, by adding the DFARS Clause 252.204-7012. The DFARS requirements include submitting a System Security Plan, and a Plan of Action and Milestones for achieving compliance with NIST SP 800-171r1, Protecting Controlled Unclassified Information within their information systems. To meet this recommendation effectively, MDA would need to incorporate continuous monitoring/oversight of the contractor networks, which is both cost prohibitive, and not within DoD authorizations or contractual authority. The agency will continue deploying, as in FY17, Cyber Assistance Teams (CAT) to assess nonfederal information systems that are considered medium or high risks. Based on availability and limited resources in this area, the agency will focus on the high-risk subcontractors for Cyber Assistance Team (CAT) assist visits. Moreover, the MDA Director, Lt Gen Greaves, recently signed a MDA Cybersecurity Best Practices memorandum (Attachment 1a) to all MDA prime contractors to share key best practices and lessons learned related to cybersecurity standards and hygiene. The memo aligns	

MDA COMMENTS MATRIX: DoD IG Audit of the Effectiveness of Logical and Physical Access Controls Over BMDS Information (Project No. D2017-D000RF-0097.000) – DRAFT REPORT
(Please read instructions on back before completing form.)

#	Class	Component and POC Name, Phone, and E-mail	Page #	Para #	Comment Type (A/C/S)	Comments, Justification, and Originator Justification for Resolution	A/R/P
						frequently recurring NIST SP 800-171r1 control shortfalls to identified threat vectors within the DIB (spear phishing, credential harvesting, and unsecure perimeter infrastructure); the memo encapsulates the need for increased focus and vigilance when applying NIST SP 800-171r1 controls and therefore provide increased protection of MDA's BMDS information across the DIB. The Best Practices memo is the second of two from MDA Directors, in the past two years, to prime contractors as a means to spread cybersecurity awareness, assist with translation, timelines, and expectations from MDA contractors regarding DFARS 252.204-7012 compliance.	
6	U		22	Rec. No. 6	N/A	**Coordinator Comment**: **AGREE** with recommendation 6. DFARS clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, requires contractors to implement NIST SP 800-171r1, Protecting Controlled Unclassified Information in Nonfederal Information Systems and requires only contractor self-attestation to confirm compliance with the DFARS and NIST SP 800-171r1 controls. OUSD-AT&L-Defense Procurement and Acquisition Policy (DPAP) memo (Sep 21, 2017), Implementation of DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting includes six (6) pages of detailed guidance, developed cooperatively by DPAP, DoD CIO, and DASD-DE, to help support successful implementation of the DFARS and the associated NIST 800-171 r1 controls by contractors in their nonfederal systems. MDA may initiate a special evaluation requirement in the Contractor Performance Assessment Reporting System (CPARS) related to cybersecurity and the implementation of DFARS clause 252.204-7012. As part of each contractor's annual evaluation of performance, the agency will evaluate and document contractor performance in maintaining information security within their networks and supply chain. **Coordinator Justification**: Unsatisfactory CPARS evaluations require vendor responses and corrective action plans to meet SOW/PWS requirements. Use of the CPARS tool as the initial evaluation of performance will provide reasonable oversight	

MDA FORM 100 JUL 2017 PREVIOUS VERSIONS OBSOLETE 9

Attachment 1

MDA COMMENTS MATRIX: DoD IG Audit of the Effectiveness of Logical and Physical Access Controls Over BMDS Information (Project No. D2017-D000RF-0097.000) – DRAFT REPORT
(Please read instructions on back before completing form.)

#	Class	Component and POC Name, Phone, and E-mail	Page #	Para #	Comment Type (A/C/S)	Comments, Justification, and Originator Justification for Resolution	A/R/P
						and evaluation of contractor performance as well as leverage for taking discretionary corrective action when needed.	
7	U		All	All	C	**Coordinator Comment**: MDA has taken considerable steps to provide awareness and timing of imminent DPAP compliance requirements and corresponding cyber hygiene through pervasive Defense Industrial Base (DIB) meetings and implementation of MDA's Cyber Assistance Team (CAT) visits to DIB partners. The Draft Report makes no mention of notable MDA actions to improve cybersecurity awareness and protect BMDS information in the DIB: 1. MDA's efforts and partnership with our four (4) major primes (Lockheed, Northrop, Raytheon, and Boeing) to address the DFARs clause, protection of MDA data in the DIB, as well as a myriad of other proactive actions and engagements we have executed. 2. MDA's Cyber ASSISTANCE Teams (CAT) and our efforts with MDA DIB partners, on a purely voluntary basis, to address cybersecurity concerns at their locations. **Coordinator Justification**: MDA should be given due credit for the proactive efforts put forth to address the protection of data in the DIB. Partnerships with our DIB partners, DPAP, and DoD/CIO's office address the challenge of securing CUI on nonfederal systems and have been ongoing for two years. We continue to work with this group as we address the protection of CUI in the DIB."	
8	U		All	All	S	**Coordinator Comment**: All CLASSIFIED Cleared Defense Contractor (CDC) cybersecurity adherence to National Industrial Security Operating Manual (NISPOM) regulations are the responsibility of the Defense Security Service (DSS) to assess, not MDA. **Coordinator Justification**: DSS has the mission to assess CDC classified locations to NISPOM standards and issue Authority to Operate (ATO) authorizations	

MDA COMMENTS MATRIX: DoD IG Audit of the Effectiveness of Logical and Physical Access Controls Over BMDS Information (Project No. D2017-D000RF-0097.000) – DRAFT REPORT
(Please read instructions on back before completing form.)

#	Class	Component and POC Name, Phone, and E-mail	Page #	Para #	Comment Type (A/C/S)	Comments, Justification, and Originator Justification for Resolution	A/R/P
						and evaluation of contractor performance as well as leverage for taking discretionary corrective action when needed.	
7	U		All	All	C	**Coordinator Comment**: MDA has taken considerable steps to provide awareness and timing of imminent DPAP compliance requirements and corresponding cyber hygiene through pervasive Defense Industrial Base (DIB) meetings and implementation of MDA's Cyber Assistance Team (CAT) visits to DIB partners. The Draft Report makes no mention of notable MDA actions to improve cybersecurity awareness and protect BMDS information in the DIB: 1. MDA's efforts and partnership with our four (4) major primes (Lockheed, Northrop, Raytheon, and Boeing) to address the DFARs clause, protection of MDA data in the DIB, as well as a myriad of other proactive actions and engagements we have executed. 2. MDA's Cyber ASSISTANCE Teams (CAT) and our efforts with MDA DIB partners, on a purely voluntary basis, to address cybersecurity concerns at their locations. **Coordinator Justification**: MDA should be given due credit for the proactive efforts put forth to address the protection of data in the DIB. Partnerships with our DIB partners, DPAP, and DoD/CIO's office address the challenge of securing CUI on nonfederal systems and have been ongoing for two years. We continue to work with this group as we address the protection of CUI in the DIB."	
8	U		All	All	S	**Coordinator Comment**: All CLASSIFIED Cleared Defense Contractor (CDC) cybersecurity adherence to National Industrial Security Operating Manual (NISPOM) regulations are the responsibility of the Defense Security Service (DSS) to assess, not MDA. **Coordinator Justification**: DSS has the mission to assess CDC classified locations to NISPOM standards and issue Authority to Operate (ATO) authorizations	

MDA FORM 100 JUL 2017 PREVIOUS VERSIONS OBSOLETE 10

Attachment 1

MDA COMMENTS MATRIX: DoD IG Audit of the Effectiveness of Logical and Physical Access Controls Over BMDS Information (Project No. D2017-D000RF-0097.000) – DRAFT REPORT
(Please read instructions on back before completing form.)

#	Class	Component and POC Name, Phone, and E-mail	Page #	Para #	Comment Type (A/C/S)	Comments, Justification, and Originator Justification for Resolution	A/R/P
						information in the hands of industry. MDA provides these requirements by including the DD Form 254 in every classified contract.	
13	U		3	3	S	**Coordinator Comment**: The legal jurisdiction, authority, and boundaries of the Government, when dealing with nonfederal CLASSIFIED and UNCLASSIFIED information systems handling Unclassified Controlled Information (CUI), must be clearly delineated, codified, and established. **Coordinator Justification**: 1. DFARS 252.204-7012 (DFARS 7012) "Safeguarding Covered Defense Information and Cyber Incident Reporting" provides the DoD requirement for nonfederal systems to protect CUI. 2. The DoD/MDA has the jurisdiction, authority, and mandate to protect the federal systems that it owns. MDA has no jurisdiction, authority, or mandate over nonfederal systems. 3. The Defense Security Service (DSS) has the jurisdiction, authority, and mandate to assess CLASSIFIED nonfederal system. No federal agency has responsibility for UNCLASSIFIED nonfederal systems. 4. OSD/AT&L Memo 21 Sep 2017 "Implementation of DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting" states " DFARS Clause 252.204-7012 does not add any other unique or additional requirements for the Government to monitor contractor implementation of NIST SP 800-171r1 or to monitor compliance with any other requirement of that clause. As noted previously, third party assessments or certifications of compliance are not required, authorized, or recognized by DoD, nor will DoD certify that a contractor is compliant with the NIST SP 800-171r1 security requirements.... 5. A gap exists as to the clear delineation of the jurisdiction, authority, and mandate to evaluate, verify, and certify the compliance of nonfederal information systems to protect CUI and conform to DFARS 254.204-7012.	

MDA COMMENTS MATRIX: DoD IG Audit of the Effectiveness of Logical and Physical Access Controls Over BMDS Information (Project No. D2017-D000RF-0097.000) – DRAFT REPORT (Please read instructions on back before completing form.)							
#	Class	Component and POC Name, Phone, and E-mail	Page #	Para #	Comment Type (A/C/S)	Comments, Justification, and Originator Justification for Resolution	A/R/P
14	U		4	3	A	**Coordinator Comment**: Original sentence: "Specifically, system and network administrators at three contractors that managed BMDS technical information on classified networks did not identify and mitigate vulnerabilities on classified networks and systems." **Change to**: "Specifically, system and network administrators at three contractor sites who managed BMDS technical information on classified networks did not identify and mitigate vulnerabilities on classified networks and systems." **Coordinator Justification**: Grammar.	
15	U		5	1	C	**Coordinator Comment**: 1. Per OSD/AT&L, "Implementation of DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting" memo dated September 21, 2017, contractors are to accomplish self-attestation and report to their DoD sponsor. Third party assessments or certifications of compliance are not required, authorized, or recognized by DoD, nor will DoD certify that a contractor is compliant with the NIST SP 800-171r1 security requirements." 2. DSS is responsible for all classified CDC networks and systems, not MDA. **Coordinator Justification**: DFARS 252.204-7012.	
16	U		18	2	C	**Coordinator Comment**: Coordinator Comment: MDA does not concur with the statement: "Security Controls at the seven contractor locations we visited were ineffective because the MDA did not assess the contractor's security actions or planned actions for protecting BMDS technical information on classified and unclassified networks and systems." **Coordinator Justification**: The security controls at the seven contractor locations are ineffective because the contractor failed to implement the controls properly. For clarification, MDA may require SSPs and POA&Ms as part of the SOW/PWS within the associated RFP and at source selection, which also will not necessarily guarantee proper implementation of 'said' controls. It is ultimately the contractor's responsibility to protect the network and systems that hold/contain MDA BMDS critical data. The	

MDA FORM 100 JUL 2017 PREVIOUS VERSIONS OBSOLETE 13

Attachment 1

MDA COMMENTS MATRIX: DoD IG Audit of the Effectiveness of Logical and Physical Access Controls Over BMDS Information (Project No. D2017-D000RF-0097.000) – DRAFT REPORT
(Please read instructions on back before completing form.)

#	Class	Component and POC Name, Phone, and E-mail	Page #	Para #	Comment Type (A/C/S)	Comments, Justification, and Originator Justification for Resolution	A/R/P
						contractor is required to accomplish a self-assessment, and send a letter to the MDA Contracting Officer stating compliance with NIST SP 800-171r1. Finally, Per OSD/AT&L, "Implementation of DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting" memo dated September 21, 2017, contractors are to accomplish self-attestation and report to their DoD sponsor. Third party assessments or certifications of compliance are not required, authorized, or recognized by DoD, nor will DoD certify that a contractor is compliant with the NIST SP 800-171r1 security requirements."	
17	U		18	2	C	**Coordinator Comment**: This paragraph should be updated to separate classified from unclassified and to delineate that the classified systems are not under the purview of the MDA. **Coordinator Justification**: MDA is not be held accountable for the oversight of classified information systems since those systems are under the security cognizance of the Defense Security Service. As previously stated, MDA provides a DD form 254 in every classified contract and the 254 calls out the requirement of the NISPOM for classified information system processing. DSS inspects the classified information systems on behalf of MDA.	
18	U		19	1	C	**Coordinator Comment**: Add the following as the last sentence "MDA does have a plan to review submitted System Security Plans (SSP) and associated, Plan of Action and Milestones (POA&Ms) after the December 31, 2017 mandated date for contractors to be compliant with NIST SP 800-171r1." **Coordinator Justification**: DFARS 252.204-7012.	
19	U		N/A	N/A	S	**Coordinator Comment**: EIR found no classified or controlled unclassified information based on MDA classification guidance. If the intent is to eventually publicly release the "DRAFT REPORT: Audit of the Effectiveness of Logical and	

MDA COMMENTS MATRIX: DoD IG Audit of the Effectiveness of Logical and Physical Access Controls Over BMDS Information (Project No. D2017-D000RF-0097.000) – DRAFT REPORT
(Please read instructions on back before completing form.)

#	Class	Component and POC Name, Phone, and E-mail	Page #	Para #	Comment Type (A/C/S)	Comments, Justification, and Originator Justification for Resolution	A/R/P
						Physical Access Controls Over Ballistic Missile Defense System Information (Project No. D2017-D000RF-0097.000)," the document must be submitted through the official OSD, Defense Office of Prepublication and Security Review (DOPSR) process for review and approval. Moreover, Official public release approval of MDA information must be provided by the MDA Public Affairs office. **Coordinator Justification**: Guidance is in accordance with DoD Directive 5230.09 "Clearance of DoD Information for Public Release," DoD Instruction 5230.29 "Security and Policy Review of DoD Information for Public Release" and MDA Directive 5400.03 "Security and Policy Review of Missile Defense Agency Information for Public Release."	
20	U		N/A	N/A	S	**Coordinator Comment**: It is incumbent on the originator(s) of the document to ensure that all FOUO portion and page markings are properly applied to the information and must determine at the time of origination whether the information may qualify for FOUO status by using the FOIA exemption criteria. Since the document was not produced/generated by MDA it does not meet the criteria of FOIA exemption (b) 5, "deliberative process," as it is not a product of MDA's internal decision-making process or operations. **Coordinator Justification**: Guidance is in accordance with the Department of Defense (DoD) Manual 5200.01, Volume 4 "DoD Information Security Program: Controlled Unclassified Information (CUI)."	

MDA FORM 100 JUL 2017 PREVIOUS VERSIONS OBSOLETE 15

Attachment 1

DEPARTMENT OF DEFENSE
MISSILE DEFENSE AGENCY
5700 18TH STREET
FORT BELVOIR, VA 22060-5573

DA

JAN 12 2018

MEMORANDUM FOR ALL MDA PRIME CONTRACTORS THROUGH THE COGNIZANT CONTRACTING OFFICERS

SUBJECT: MDA Cybersecurity Best Practices

The Missile Defense Agency (MDA) relies on its industry partners to help execute our mission, which requires the sharing and protection of sensitive data. MDA data is targeted and at risk for compromise across multiple domains, with significant cybersecurity vulnerabilities existing in the Defense Industrial Base (DIB). I am soliciting the continued commitment and assistance of all MDA DIB stakeholders to prevent adversary exfiltration of Ballistic Missile Defense System (BMDS) information from your systems and from systems throughout all levels of your sub-tier contractors and suppliers.

Effective October 21, 2016, revised DFARS 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting," clarified the definition of Covered Defense Information (CDI) and required compliance with security requirements in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 rev.1, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations." Covered Defense Information is defined in DFARS clause 252.227-7013, "Rights in Technical Data-Noncommercial items," Controlled Unclassified Information (CUI) and Department of Defense Manual (DoDM) 5200.01 Vol 4, "Controlled Unclassified Information." To safeguard CDI, contractors and subcontractors are required to implement NIST SP 800-171 rev.1 by December 31, 2017.

Based on feedback received from our industry partners, practices observed in the DIB, and lessons learned from MDA supply chain vulnerability assessments, we have identified a list of frequently recurring NIST 800-171 rev. 1 control shortfalls that you should consider as you take steps to improve cyber hygiene. We have aligned these frequently recurring shortfalls to identified threat vectors within the DIB (spear phishing, credential harvesting, and unsecure perimeter infrastructure). Although organizations are responsible for implementing all the controls outlined in NIST 800-171 rev. 1, I am requesting your assistance in providing increased focus and vigilance when applying the subset of controls, identified as 'MDA Cybersecurity Best Practices', in Attachment 1. These controls provide increased protection of MDA's BMDS information across the DIB.

Additional government resources are available to industry for improving your cybersecurity hygiene are provided in Attachment 2. These sites provide relevant and actionable cybersecurity information.

Attachment 1a

Our adversaries are engaged today, around the clock, working to infiltrate our networks. Cybersecurity is a team effort and a 24/7 activity that requires steadfast commitment from all stakeholders. It is imperative we continue to improve our cybersecurity protections.

My cybersecurity points of contact are Lieutenant Colonel Todd Cook, Chief, Network Warfare Division, Todd.Cook@mda.mil or 719-721-9997 and Mr. Tony Mesenbrink, MDA Senior Information Security Officer, Anthony.Mesenbrink@mda.mil or 719-721-8157. Please address your comments or questions regarding this subject matter to them.

SAMUEL A. GREAVES 1/12/18
Lieutenant General, USAF
Director

Attachments:
As stated

2

Cybersecurity Best Practices: Recommended Measures to Improve Cybersecurity Hygiene

Technical Focus Items		
Identified Threats in the DIB		
Spear Phishing	Credential Harvesting	Unsecure Perimeter Infrastructure
Measures	NIST SP 800-171 Rev.1 Control #	Impact level
Audit/Control - Administrator Privilege	3.1.5	1 – High
Limit logon attempts and lock after periods of inactivity	3.1.8 / 3.1.10	1 – High
Disable unlimited remote access	3.1.12 / 3.1.13	1 – High
Deploy network access control	3.1.20	1 – High
Remove stale/unused IT end of life systems	3.4.1 / 3.7.1	1 – High
Prohibit "Gray Market" IT procurements (EBay)	3.4.4	1 – High
Enable Two-/Multi-factor authentication	3.5.3	1 – High
Enforce a minimum password complexity	3.5.7	1 – High
Control use of removable media on system components	3.8.4 / 3.8.7	1 – High
Conduct system risk assessment and remediate	3.11.1	1 – High
Deploy Email filter	3.13.1	1 – High
Configure Category "None" blocking (web content filter)	3.13.1	1 – High
Harden Perimeter Networks	3.13.1 / 3.13.6	1 – High
Identify / report system flaws	3.14.1 / 3.14.3	1 – High
Deploy Security / Patching	3.14.4	1 – High

ATTACHMENT 1

3

Non-Technical Focus Items		
Identified Threats in the DIB		
Spear Phishing	Credential Harvesting	Unsecure Perimeter Infrastructure
Measures/Controls		
Distribution statements • Develop Controlled Unclassified Information (CUI) marking instruction (***3.1.22***) • Mandate Distribution Statements on CDRLs and program documents (non-deliverables) (***3.1.22***)		
Mandatory Government & Contractor Training • FOUO/CUI Marking & Safeguarding (***3.1.22***) • Cybersecurity Awareness (***3.2.2***) • Distribution Statement Markings (***3.1.22***)		
Supply Chain Operational Security (OPSEC) Practices • Restrict Information Flow-Down (Manufacturing need-to-know) (***3.1.3***) • Limit information listed on commodity Purchase Orders (***3.1.3***)		
Improve Cyber Intelligence Sharing between MDA & Industry • Known supplier issues (***3.11.3***)		
Information System Procurement • All network hardware should be cybersecurity approved – Prior to emplacement on production network (***3.4.4***)		

ATTACHMENT 1

Cybersecurity Resources

- United States Computer Emergency Readiness Team (US-CERT) http://www.us-cert.gov
- DoD Defense Industrial Base Cybersecurity program (DIB CS program) https://dibnet.dod.mil
- DoD Office of Small Business Programs http://business.defense.gov/
- FBI InfraGard https://www.infragard.org
- DHS Cybersecurity Information Sharing and Collaboration Program (CISCP) https://www.dhs.gov/ciscp
- DHS Enhanced Cybersecurity Services (ECS) https://www.dhs.gov/enhanced-cybersecurity-services
- Defense Security Information Exchange (DSIE) https://www.dsie.org/

Policy Resources

- DoD Procurement Toolbox, Cybersecurity Policy, Regulations, Frequently Asked Questions (FAQs) http://dodprocurementtoolbox.com/
- DPAP Website/DARS/DFARS and PGI http://www.acq.osd.mil/dpap/dars/dfarspgi/current/
  - DFARS Subpart 204.73 and PGI 204.73 - Safeguarding Covered Defense Information and Cyber Incident Reporting
  - SUBPART 239.76 and PGI 239.76-.Cloud Computing
  - 252.204-7008 Compliance with Safeguarding Covered Defense Information Controls.
  - 252.204-7009 Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information
  - 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting
  - 252.239-7009 Representation of Use of Cloud Computing
  - 252.239-7010 Cloud Computing Services
- National Institute of Standards and Technology SP 800-171
  - http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf
  - National Institute of Standards and Technology – Cybersecurity https://www.nist.gov/topics/cybersecurity
  - Cloud Computing Security Requirements Guide https://iase.disa.mil/cloud_security/Documents/u-cloud_computing_srg_v1r1_final.pdf

ATTACHMENT 2

Acronyms and Abbreviations

BMDS	Ballistic Missile Defense System
CD	Compact Disc
DFARS	Defense Federal Acquisition Regulation Supplement
DVD	Digital Versatile Disc
MDA	Missile Defense Agency
NIST	National Institute of Standards and Technology
POA&M	Plans of Action and Milestones
SP	Special Publication
SSP	System Security Plan
UCTI	Unclassified Controlled Technical Information
USB	Universal Serial Bus Drive

Glossary

Authentication. A process that verifies the identity of a user and is a prerequisite to allowing access to an information system.

Ballistic Missile Defense System. An integrated, layered architecture of sensors, radars, interceptor missiles, and communications network that is used to destroy hostile short, medium, intermediate, and long-range missiles before reaching their intended targets.

Cleared Defense Contractor. Private entity that is given clearance by the DoD to access, receive, or store classified information for the purpose of bidding for a contract or conducting activities in support of any DoD program.

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

Denial of Service. Prevents legitimate users from accessing information and services on systems.

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 elevated privileges, significant data loss, and network downtime.

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

Least Privilege. A security objective requiring access needed only to perform official duties.

Low Vulnerabilities. If exploited, would likely result in unauthorized local or physical system access.

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

Medium Vulnerabilities. If exploited, could result in a denial of service attack and provide attackers with limited access to the network.

Multifactor Authentication. Combines the use of what the user knows (e.g. password), what the user has (e.g. token), and what the user is (e.g. biometric verification) to prevent an unauthorized individual from accessing a device, system, or network.

Network and Boundary Protection. Monitoring the perimeter of an information system to prevent and detect malicious and unauthorized communication.

Non-privileged User. Is not authorized to perform security-related functions.

Patch. An update to an operating system, application, or other software issued to correct specific problems.

Plan of Action and Milestones (POA&M). A document that identifies tasks that need to be accomplished, resources required to accomplish tasks, milestones in meeting tasks, and scheduled completion dates for milestones.

Privileged User. Is authorized to perform security-related functions.

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.

Risk Assessment. A process of identifying risks to organizational operations, assets, and individuals from operating an information system.

System Audit Log. A chronological record of system activities performed in a given period.

Token. Used to authenticate a user's identity.

Unclassified Controlled Technical Information. Technical information with military or space application that is subject to access, use, reproduction, modification, performance, display, release, disclosure, or dissemination controls.

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

Whistleblower Protection
U.S. Department of Defense

The Whistleblower Protection Ombudsman's role is to educate agency employees about prohibitions on retaliation and employees' rights and remedies available for reprisal. The DoD Hotline Director is the designated ombudsman. For more information, please visit the Whistleblower webpage at www.dodig.mil/Components/Administrative-Investigations/DoD-Hotline/.

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

Congressional Liaison
703.604.8324

Media Contact
public.affairs@dodig.mil; 703.604.8324

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

Twitter
www.twitter.com/DoD_IG

DoD Hotline
www.dodig.mil/hotline

DEPARTMENT OF DEFENSE | OFFICE OF INSPECTOR GENERAL

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