Report No. DODIG-2019-034

INSPECTOR GENERAL

U.S. Department of Defense

DECEMBER 10, 2018

(U) Security Controls at DoD Facilities for Protecting Ballistic Missile Defense System Technical Information

~~Classified By: Carol N. Gorman, Assistant Inspector General for Cyberspace Operations~~
~~Derived From: Multiple Sources~~
~~Declassify On: 20490628~~

INTEGRITY ★ INDEPENDENCE ★ EXCELLENCE


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

Results in Brief

(U) Security Controls at DoD Facilities for Protecting Ballistic Missile Defense System Technical Information

December 10, 2018

(U) Objective

(U) We determined whether DoD Components implemented security controls and processes at DoD facilities to protect ballistic missile defense system (BMDS) technical information on classified networks from insider and external cyber threats.

(U) We conducted this audit in response to a congressional requirement to audit the controls in place to protect BMDS technical information, whether managed by cleared Defense contractors, or by the Government. Cleared contractors are entities granted clearance by the DoD to access, obtain, or store classified information, to bid on contracts, or conduct activities in support of DoD programs.

(U) We analyzed only classified networks because BMDS technical information was not managed on unclassified networks. The classified networks processed, stored, and transmitted both classified and unclassified BMDS technical information. This is the second of two audits to determine whether the DoD protected BMDS technical information from unauthorized access and disclosure. On March 29, 2018, we issued a report on the effectiveness of logical and physical access controls in place to protect BMDS technical information at Missile Defense Agency (MDA) contractor locations. The report identified systemic weaknesses at the contractor locations concerning network access, vulnerability management, and the review of system audit logs.

(U) Background

(U) 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. Examples of technical information include, but are not

(U) Background (cont'd)

(U) limited to, military or space research and engineering data, engineering drawings, algorithms, specifications, technical reports, and source codes.

(U) Findings

(U) We determined that officials from the [redacted] did not consistently implement security controls and processes to protect BMDS technical information. Specifically, [redacted] network administrators and data center managers did not:

- (U) require the use of multifactor authentication to access BMDS technical information at the [redacted];
- (U) identify and mitigate known network vulnerabilities at three of the five Components visited;
- (U) lock server racks at the [redacted];
- (U) protect and monitor classified data stored on removable media at the [redacted];
- (U) encrypt BMDS technical information transmitted between [redacted];
- (U) implement intrusion detection capabilities on [redacted] classified network; and
- (U) require written justification as a condition to obtain and elevate system access for users at the [redacted].

Results in Brief

(U) Security Controls at DoD Facilities for Protecting Ballistic Missile Defense System Technical Information

(U) Findings (cont'd)

(U) In addition, facility security officers did not consistently implement physical security controls to limit unauthorized access to facilities that managed BMDS technical information at the [redacted].

(U) Security control weaknesses existed because officials at the [redacted] did not consistently verify the effectiveness of implemented security controls and assess the impact of missing security controls. Without well-defined, effectively implemented system security and physical access controls, the MDA and its business partners, [redacted], may disclose critical details that compromise the integrity, confidentiality, and availability of BMDS technical information. The disclosure of technical details could allow U.S. adversaries to circumvent BMDS capabilities, leaving the United States vulnerable to deadly missile attacks. Increasing threats of long-range missile attacks from adversaries requires the effective implementation of system security controls to help reduce the number of exploitable weaknesses that attackers could use to exfiltrate BMDS technical information.

(U) Recommendations

(U) We recommend that the [redacted] develop and implement a plan to correct the systemic weaknesses identified in this report at facilities that manage BMDS technical information related to, among other issues:

- (U) using multifactor authentication;
- (U) mitigating vulnerabilities in a timely manner;
- (U) protecting data on removable media; and
- (U) implementing intrusion detection capabilities.

(U) We also recommend that the [redacted], among other actions:

- (U) enforce the use of multifactor authentication to access systems that process, store, and transmit BMDS technical information or obtain a waiver from using multifactor authentication from the DoD Chief Information Officer;
- (U) develop plans and take appropriate and timely steps to mitigate known vulnerabilities;
- (U) encrypt BMDS technical information stored on removable media; and
- (U) assess gaps in physical security coverage and install security cameras with [redacted] to monitor personnel movements throughout [redacted] facilities.

(U) In addition, we recommend that the [redacted] Chief Information Officer enforce the use of multifactor authentication to access systems that process, store, and transmit BMDS technical information or obtain a waiver from using multifactor authentication; and implement intrusion detection capabilities on networks that maintain BMDS technical information. Furthermore, we recommend that the [redacted] Chief Information Officer develop and implement procedures to secure server racks and control server rack keys; and maintain access request forms that include written justification to support the need for access to networks and systems that contain BMDS technical information.

Results in Brief

(U) Security Controls at DoD Facilities for Protecting Ballistic Missile Defense System Technical Information

(U) Recommendations (cont'd)

(U) Lastly, we recommend that the [redacted] Chief Information Officers:

- (U) encrypt BMDS technical information stored on removable media;
- (U) develop and implement a process to identify individuals who are authorized to use removable media as well as procedures to monitor the type and volume of data transferred to and from removable media; and
- (U) assess gaps in security coverage and install security cameras with [redacted] to monitor personnel movements throughout their facilities.

(U) Management Comments

(U) The [redacted], and Chief Information Officers for [redacted] did not provide comments on the draft report. Therefore, we request comments on the final report from the Director, Commanding General, Commander, and Chief Information Officers.

(U) Please see the Recommendations Table on the next page.

(U) Recommendations Table

Unclassified Management	Recommendations Unresolved	Recommendations Resolved	Recommendations Closed
Director, [redacted]	1.a, 1.b, 1.c, 1.d, 1.e, 1.f, 1.g, 2.a, 2.b, 2.c, 2.d, 2.e, 2.f, 2.g, 2.h, 2.i, 2.j	None	None
Commanding General, [redacted]	1.a, 1.b, 1.c, 1.d, 1.e, 1.f, 1.g	None	None
Commander, [redacted]	1.a, 1.b, 1.c, 1.d, 1.e, 1.f, 1.g	None	None
Chief Information Officer, [redacted]	3.a, 3.b, 4.a, 4.b, 4.c	None	None
Chief Information Officer, [redacted]	4.a, 4.b, 4.c, 5.a, 5.b, 5.c	None	None

Unclassified

(U) Please provide Management Comments by January 8, 2019.

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

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

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

December 10, 2018

MEMORANDUM FOR DIRECTOR, [redacted]
COMMANDING GENERAL, [redacted]
COMMANDER, [redacted]
NAVAL INSPECTOR GENERAL
AUDITOR GENERAL, DEPARTMENT OF THE ARMY

SUBJECT: (U) Security Controls at DoD Facilities for Protecting Ballistic Missile Defense System Technical Information (Report No. DODIG-2019-034)

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

(U) DoD Instruction 7650.03 requires that recommendations be resolved promptly. The [redacted]; and the Chief Information Officers for the [redacted] did not respond to the draft report. Therefore, we request that the Director, Commanding General, Commander, and Chief Information Officers comment on the final report by January 8, 2019.

(U) Please send a PDF file containing your comments on the recommendations to [redacted] and [redacted]. 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. Comments provided on the final report must be marked and portion-marked, as appropriate, in accordance with DoD Manual 5200.01.

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

Carol N. Gorman
Assistant Inspector General
Cyberspace Operations

Contents

(U) Introduction

(U) Objective

(U) The audit objective was to determine whether DoD Components implemented security controls and processes at DoD facilities to protect ballistic missile defense system (BMDS) technical information from insider and external threats.[1] This is the second of two audits to determine whether the DoD protected BMDS technical information from unauthorized access and disclosure. On March 29, 2018, we issued a report on the effectiveness of logical and physical access controls at Missile Defense Agency (MDA) contractor locations.[2]

(U) We selected a nonstatistical sample of 5 of 104 DoD locations at four military installations that manage BMDS elements and technical information. The five locations included [redacted]. One military installation maintained a separate facility for [redacted]. Therefore, we assessed physical security controls at all facilities visited and cybersecurity controls at only the data centers and labs. The data centers and labs managed BMDS technical information.[3] See Appendix for a discussion on the scope and methodology. See the Glossary for definitions of the technical term.

(U) Background

(U) On April 14, 2016, the MDA Director testified before the House Armed Services Subcommittee on Strategic Forces, expressing concern about the potential threat to systems containing BMDS 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 BMDS technical information managed by the Government.[4] Examples of technical information include, but are not limited to, military or space research and engineering data, engineering drawings, algorithms, specifications, technical reports, and source codes. In addition, system and network owners must, at a minimum, comply with DoD configuration standards in applicable Defense Information Systems Agency Security Technical Implementation Guides.

[1] (U) We assessed only classified networks because BMDS technical information was not maintained on unclassified networks. However, the classified networks processed, stored, and transmitted both classified and unclassified BMDS technical information.
[2] (U) Report DODIG-2018-094, "Logical and Physical Access Controls at Missile Defense Agency Contractor Locations," March 29, 2018.
[3] (U) Although we visited [redacted], we did not assess security controls at [redacted]-managed facilities. Instead, we assessed security controls at the [redacted] located at [redacted]. For this report, "facility" means the physical building.
[4] (U) Public Law 114-328, "National Defense Authorization Act for Fiscal Year 2017," December 23, 2016.

(U) Missile Defense Agency

(U) The MDA manages, directs, and executes the development of the BMDS in accordance with DoD Directive 5134.09, "Missile Defense Agency," September 17, 2009, and National Security Presidential Directive 23, "National Policy on Ballistic Missile Defense," December 16, 2002. DoD Directive 5134.09 requires the MDA to support DoD priorities to:

- (U) defend the United States, deployed forces, and allies from ballistic missile attacks of all ranges in all phases of flight;
- (U) develop, test, deploy, and field BMDS elements; and
- (U) improve the effectiveness of the fielded elements.

(U) Ballistic Missile Defense System

(U) The BMDS is designed to destroy hostile missiles of all ranges—short, medium, intermediate, and long—and their warheads before the missiles reach their intended targets. The BMDS is a system of elements that enable the DoD to execute a layered defense to defend against hostile missiles in all phases of flight: boost, midcourse, and terminal.[5] The elements are:

- (U) Aegis Ballistic Missile Defense – the naval component of BMDS that builds upon the existing Aegis Weapon System, Standard Missile, and Navy and joint forces command, control, and communication systems and which detects and tracks ballistic missiles of all ranges.
- (U) Ground-based Midcourse Defense – the communications networks, fire control systems, sensors, and interceptors that allow combatant commanders to engage and destroy intermediate- and long-range ballistic missile threats in space.
- (U) PATRIOT Advanced Capability-3 – a land-based element that provides simultaneous air and missile defense capabilities.
- (U) Terminal High Altitude Area Defense – a globally-transportable, rapidly-deployable capability that intercepts and destroys ballistic missiles inside or outside of the atmosphere during their final phase of flight.

[5] (U) The boost phase is the firing stage of the missile, the midcourse phase is when the missile begins coasting towards its target, and the terminal phase is the missile's last opportunity to intercept warheads before reaching its target.

(U) The BMDS architecture contains the following support elements:

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

(U) According to the MDA, ballistic missiles have different ranges, speeds, sizes, and performance characteristics. The BMDS architecture provides multiple opportunities to destroy missiles and warheads before reaching the intended target. 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.

(U) Protecting BMDS Information

(U) On March 14, 2014, the DoD Chief Information Officer directed the DoD to implement National Institute of Standards and Technology (NIST) security controls to protect networks and systems as part of the DoD's Risk Management Framework.[6] Although BMDS is a weapons system, the technical information used to manage BMDS is maintained on DoD and cleared Defense contractor networks and systems.[7] As such, DoD Components and MDA contractors must implement security controls and processes to protect classified and unclassified BMDS technical information.

(U) DoD Components Responsible for Managing BMDS Technical Information

(U) As of October 2018, 104 DoD facilities worldwide managed BMDS technical information. MDA officials stated that they planned to operate 10 additional facilities in the future to support BMDS development and testing but did not identify a timeline for the additional facilities. We visited the following five locations, some with multiple facilities, and assessed the cybersecurity controls on networks and systems that processed, stored, and transmitted BMDS technical information.

[6] (U) DoD Instruction 8500.01, "Cybersecurity," March 14, 2014; NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," Revision 4, April 2013; and DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014 (Incorporating Change 2, July 28, 2017).
[7] (U) For this report, the security controls and processes must be applied to networks and information systems that process, store, and transmit BMDS technical information. A cleared defense contractor is a private entity granted clearance by the DoD to access, obtain, or store classified information for the purpose of bidding on a contract or conducting activities in support of a DoD program.

- (U) [redacted], supports BMDS research and development and system-level testing and evaluation. It also provides operational and training support to the combatant commands.
- (U) [redacted], supports BMDS research and development and manages [redacted].
- (U) [redacted], provides [redacted] capabilities for research, development, and lifecycle engineering solutions for BMDS. We visited [redacted] that maintained BMDS technical information.
- (U) [redacted], provides research development, test and evaluation, analysis, system engineering, integration, and certification of [redacted]. The [redacted] also supports BMDS test events.
- (U) [redacted], supports the [redacted] organization with modeling, simulation, and analysis services. The [redacted] primarily focuses on emerging concept technologies, which contribute to advancing BMDS capabilities.

(U) We also assessed physical security controls at the five locations as well as an [redacted].

(U) Review of Internal Controls

(U) DoD Instruction 5010.40 requires DoD organizations to implement a comprehensive system of internal controls that provides reasonable assurance that programs are operating as intended and to evaluate the effectiveness of the controls.[8] We identified internal control weaknesses related to protecting networks and systems that process, store, and transmit BMDS technical information. Specifically, [redacted] did not consistently implement security controls and processes to protect classified and unclassified BMDS technical information. We will provide a copy of the report to the senior official responsible for internal controls at the [redacted].

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

(U) Finding

(U) Security Controls for DoD Networks and Systems Containing BMDS Information Were Not Consistently Implemented

(U) [redacted] officials did not consistently implement security controls and processes to protect BMDS technical information. Specifically, [redacted] network and database administrators and data center managers did not:

- (U) require the use of multifactor authentication to access BMDS technical information at the [redacted];
- (U) identify and mitigate known network vulnerabilities at three of the five Components visited;
- (U) lock server racks at the [redacted];
- (U) protect and monitor the type and volume of classified data stored on removable media at the [redacted];
- (U) enforce the use of encryption when [redacted] BMDS technical information to [redacted];[9]
- (U) implement intrusion detection capabilities on [redacted]; and
- (U) require written justification as a condition to obtain and elevate system access privileges at the [redacted].

(U) In addition, facility security officers did not consistently implement physical security controls to limit unauthorized access to [redacted] facilities that managed BMDS technical information.

(U) Officials at the [redacted] neither verified that network and database administrators and physical security personnel consistently implemented security controls nor assessed the impact of missing security controls. Without well-defined, effectively implemented system security and physical access controls, the MDA and its business partners, [redacted], may disclose critical data that compromise the integrity, confidentiality, and availability of BMDS technical information. The disclosure of technical details could allow U.S. adversaries to circumvent the BMDS capabilities, leaving the United States vulnerable to deadly

[9] (U) For this report, "[redacted] that manage BMDS technical information.

(U) missile attacks. The increased threat of long-range missile attacks from U.S. adversaries requires the effective implementation of system security controls to help reduce the number of exploitable weaknesses that malicious actors could use to exfiltrate classified and unclassified technical information.

(U) Security Controls Were Not Effective or Consistently Implemented

(U) [redacted] officials did not consistently implement cybersecurity controls and processes to protect against the potential unauthorized access to, or disclosure of, BMDS technical information. To determine whether the Army, Navy, and MDA protected BMDS technical information, we analyzed cybersecurity controls, processes, and technology used for managing network and system authentication, vulnerabilities, and data storage and transfers. In addition, we analyzed physical security controls, such as facility access. Based on our analyses and testing, we identified security weaknesses at all five locations visited. Table 1 identifies the security weaknesses identified by facility.

(U) Table 1. Security Weaknesses Identified at [redacted] Facilities Visited

Unclassified Security Weakness	Facility Visited*				
	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Multifactor Authentication Was Not Consistently Used	X		X		X
Network Vulnerabilities Were Not Consistently Mitigated	X	X			X
Server Racks Were Not Consistently Secured	X			X	
Data on Removable Media Was Not Consistently Protected and Monitored		X	X	X	
Intrusion Detection Was Not Implemented			X		
Administrators Did Not Require or Maintain Justification for Access	X	X	X	X	X
Physical Security Controls Were Not Implemented			X	X	X

Unclassified

*(U) The [redacted] maintained separate facilities for administrative activities at the [redacted]. Therefore, checkmarks in those columns could indicate issues at either an administrative facility, a lab, or both. For details, see the discussion section of this report.

Source: The DoD OIG.

(U) Multifactor Authentication Was Not Consistently Used

(U) [redacted] users did not consistently use multifactor authentication to access networks and systems that maintained BMDS technical information. Authentication verifies the identity of a user and is a prerequisite to allowing access to an information system. Multifactor authentication requires using something in a

(U) user's possession, such as a token, in combination with something known only to the user, such as a personal identification number.[10] DoD Instruction 8520.03 requires DoD Components to use multifactor authentication mechanisms, such as a Common Access Card (CAC) or a Rivest-Shamir-Adleman token (commonly known as RSA tokens), to access DoD networks and systems.[11] Although the [redacted] configured their respective networks to use CACs, officials did not enforce the use of CACs to access BMDS technical information. Instead, [redacted] officials used single-factor authentication, such as a username and password, to access classified networks at the [redacted] as well as the [redacted] at the [redacted]. Single-factor authentication is less stringent and presents a greater risk of malicious actors compromising systems and networks.

(U) Users at the [redacted] accessed the [redacted] without using multifactor authentication because the domain administrator did not configure the network to allow only CAC-holding users access. [redacted] officials stated that they issued guidance that allows new users to access the [redacted] using single-factor authentication instead of a CAC for up to 14 business days from the time of account creation. [redacted] personnel stated that the [redacted] used this practice during the on-boarding process because users needed immediate access to the [redacted] to complete assigned responsibilities. Although the [redacted] complied with the DoD's password length and complexity requirements for accessing a classified network, we found that 34 users accessed the [redacted] using single-factor authentication well past 14 business days, with some users not using CACs to access the [redacted] for up to 7 years. The [redacted] domain administrator changed 33 of the 34 user accounts to require the use of CACs to access the [redacted], but he could not explain why those user accounts had not been previously changed and he did not provide additional details on why the one account was not changed.

(U) We found that 34 users accessed the [redacted] using single-factor authentication well past 14 business days, with some users not using CACs to access the [redacted] for up to 7 years.

(U) In addition, the system administrator at the [redacted] stated that the operating system used to access an enclave on the [redacted] did not support the use of CACs.[12] [redacted] personnel considered single-factor authentication, such as user name and password, sufficient for accessing the workstations in the lab. However, the system administrator stated that the [redacted] planned to use RSA tokens to enforce

[10] (U) Multifactor authentication uses two or more factors to achieve authentication by using something you know (password/personal identification number), something you have (cryptographic identification device), or something you are (biometric). A token authenticates a user's identity.
[11] (U) DoD Instruction 8520.03, "Identity Authentication for Information Systems," May 13, 2011, incorporating Change 1, July 27, 2017.
[12] (U) An enclave is a set of system resources that operate in the same security domain and that shares the protection of a single, common, continuous security perimeter.

(U) multifactor authentication beginning in August 2018.[13] The Deputy DoD Chief Information Officer (CIO) approved the use of RSA tokens on April 14, 2017, to allow multifactor authentication on systems and networks that did not support the use of CACs. In September 2018, system administrators began testing authentication using RSA tokens on the [redacted].

(U) [redacted] officials stated that delays, sometimes up to 8 weeks, in obtaining access to the [redacted] prevented lab users from accessing the network using multifactor authentication. The [redacted] Deputy CIO stated that he was not aware of the delays and stated that it should take only a few days to receive access. The Deputy CIO took action during the audit to correct the delays. [redacted] officials stated that, as of July 2018, the time to obtain access to the [redacted] was reduced from 8 weeks to about 1 week because of the Deputy CIO's actions.

(U) DoD Instruction 8520.03 allows the use of single-factor authentication if the Component obtains a waiver.[14] However, the [redacted] did not obtain waivers exempting the use of CACs to access their networks. Allowing users to access networks using single factor authentication increases the potential that cyber attackers could exploit passwords and gain access to sensitive BMDS technical information. Cyber attackers use several methods to exploit passwords and gain unauthorized access to systems, such as dictionary attacks, phishing, and brute force attacks.[15] A dictionary attack uses a simple file that contains words found in a dictionary. A cyber attacker randomly groups potential words based on the words in the dictionary file in an effort to guess user passwords. Some programs try to gain access to information systems by guessing common words and phrases, using personal information associated with specific users, or using a combination of various methods and programs to repeatedly attempt to access sensitive information protected by passwords. Security protocols such as multifactor authentication reduce the risk of unauthorized access to, and disclosure of, BMDS technical information. The [redacted] CIO should either enforce the use of multifactor authentication to access systems that process, store, and transmit BMDS technical information or obtain a waiver that exempts the networks from using multifactor authentication.

[13] (U) RSA tokens are hardware tokens designed to provide two-factor authentication, encryption, and e-mail signing capabilities.
[14] (U) When Components receive a waiver that allows the use of single-factor authentication, users must comply with DoD password length and complexity requirements by creating passwords that are at least 14 characters for classified networks and 15 characters for unclassified networks; and include at least one of the following: uppercase letter, lower case letter, number, and special character.
[15] (U) 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.

(U) Network Vulnerabilities Were Not Consistently Mitigated

(U~~//FOUO~~) Network administrators at three of the five DoD facilities that managed BMDS technical information did not consistently mitigate known network vulnerabilities on classified networks. In addition, the [redacted] CIO did not develop plans of action and milestones (POA&Ms) for vulnerabilities that the [redacted] was not able to mitigate. Chairman of the Joint Chiefs of Staff Manual 6510.02 [redacted].[16] Information assurance vulnerability alerts, which are issued by U.S. Cyber Command, are notifications generated when vulnerabilities may result in an immediate and potentially severe threat to DoD systems and information that require corrective actions based on the severity of the risk. We compared classified network scan results from January through June 2018 for the [redacted], and found that network vulnerabilities were not mitigated at the [redacted] in accordance with DoD requirements.[17] Table 2 lists the number of unmitigated vulnerabilities at the five DoD facilities.

~~(S)~~ Table 2. Unmitigated Classified Network Vulnerabilities at the [redacted]

~~SECRET~~ DoD Facility	Vulnerability Scan Dates	Number of Vulnerabilities Identified	Number of Unmitigated Vulnerabilities	Number, by Category, of Vulnerabilities That Were Not Mitigated				
				Critical	High	Medium	Low	Informational*
[redacted]	January and March 2018	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	January and April 2018	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	January and May 2018	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	May and June 2018	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	April and June 2018	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Totals		[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted] ~~SECRET~~

* ~~(S)~~ Informational vulnerabilities do not have a significant impact on the network. We concluded that [redacted] mitigated vulnerabilities in a timely manner. The [redacted] medium and low unmitigated vulnerabilities, but included them on a POA&M; therefore, we concluded that the [redacted] managed risk in a timely manner.

Source: The DoD OIG.

[16] (U) Chairman of the Joint Chiefs of Staff Manual 6510.02, "Information Assurance Vulnerability Management (IAVM) Program," November 5, 2013.

[17] (U) Vulnerability scans are inspections of potential weaknesses that can be exploited on a computer or network. NIST SP 800-53, Revision 4, allows organizations to define response times for correcting vulnerabilities. The [redacted] Deputy CIO stated that the [redacted] required mitigation of critical vulnerabilities in 7 days and high vulnerabilities in 30 days.

~~(S)~~ At the [redacted], a March 2018 scan revealed that [redacted] of the [redacted] vulnerabilities identified on a January 2018 network scan remained unmitigated. The [redacted] vulnerabilities consisted of [redacted] critical and [redacted] high vulnerabilities. Critical vulnerabilities, if exploited by unauthorized users, would likely result in privileged access to servers and information systems and, therefore require immediate patches.[18] For example, an unmitigated critical vulnerability from January 2018 could allow [redacted] to networks and systems that maintain BMDS technical information [redacted]. The NIST assessment of this vulnerability concluded that it could be exploited multiple times by an attacker and that [redacted]. Although the vulnerability was initially identified in 2013, the [redacted] still had not mitigated the vulnerability by our review in April 2018. Of the [redacted] unmitigated vulnerabilities, the [redacted] included only [redacted] in a POA&M and could not provide an explanation for not including the remaining vulnerabilities in its POA&M.

~~(S)~~ An unmitigated critical vulnerability on the [redacted] could allow [redacted] BMDS technical information.

~~(S)~~ At the [redacted], an April 2018 scan revealed that [redacted] of the [redacted] vulnerabilities identified on a February 2018 network scan for the [redacted] remained unmitigated. The [redacted] vulnerabilities consisted of [redacted] critical and [redacted] high vulnerabilities. For example, an unmitigated critical vulnerability from February 2018, which included [redacted] could allow [redacted]. Although the vulnerability was initially identified in 2016, the [redacted] had neither mitigated the vulnerability nor included it in a POA&M by our review in April 2018. Of the [redacted] unmitigated vulnerabilities, the [redacted] accepted the risk for [redacted] vulnerabilities but did not provide documentation to justify the acceptance of risk or include the remaining [redacted] unmitigated vulnerabilities identified in our analysis in a POA&M and could not provide an explanation for not including them.[19]

~~(S)~~ In addition, at the [redacted], an April 2018 scan revealed that [redacted] of the [redacted] vulnerabilities identified on a January 2018 network scan for the [redacted] remained unmitigated. The [redacted] vulnerabilities consisted of [redacted] critical and [redacted] high vulnerabilities. For example, an unmitigated critical network vulnerability from January 2018 could allow [redacted]

[18] (U) High vulnerabilities, if exploited by unauthorized users, 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.
[19] (U~~//FOUO~~) Chairman of the Joint Chiefs of Staff Manual 6510.02 [redacted].

~~(S)~~ [redacted]. The NIST assessment of this vulnerability concluded that it could be exploited multiple times by an attacker, and that the vulnerability could [redacted]. Although the vulnerability was initially identified in 1990, the [redacted] had not mitigated the vulnerability by our review in April 2018. Of the [redacted] unmitigated vulnerabilities, the [redacted] included only [redacted] in a POA&M and could not provide an explanation for not including the remaining vulnerabilities in its POA&M.

~~(S)~~ At [redacted], a June 2018 scan revealed that [redacted] of the [redacted] vulnerabilities identified on an April 2018 network scan remained unmitigated. However, the [redacted] unmitigated vulnerabilities had a severity code as "informational," which Symantec describes as events that result from scans for malicious services and intrusion detection activities and do not have a significant impact on the network.[20] Therefore, [redacted] managed risk by mitigating all vulnerabilities that we identified in April 2018 that could impact its network security posture.

~~(S)~~ At the [redacted], a June 2018 scan of its BMDS operating environment and enclave revealed that [redacted] of the [redacted] vulnerabilities identified on a May 2018 scan remained unmitigated. The [redacted] operating environment includes desktops, thin clients, support servers, domain controllers, backup servers, and security databases.[21] The [redacted] vulnerabilities consisted of [redacted] medium and [redacted] low vulnerabilities, and [redacted] vulnerabilities with a severity code of informational. The [redacted] included the [redacted] medium and low vulnerabilities on its POA&M with a completion date of July 30, 2019. Although the [redacted] did not immediately address the [redacted] vulnerabilities, it developed a plan that included a targeted completion date for mitigating the identified risks. Therefore, we determined that the [redacted] POA&M addressed the risks that could affect its network security.

~~(S//NF)~~ At the [redacted], a June 2018 scan revealed that [redacted] of the [redacted] vulnerabilities identified on an April 2018 network scan remained unmitigated. The [redacted] vulnerabilities included [redacted]. The [redacted] vulnerability from June 2017 included [redacted] that could allow an attacker [redacted]. This vulnerability includes flaws that could affect the confidentiality, integrity, and availability of networks and systems that maintain BMDS technical information. Although the information assurance vulnerability alert required components to mitigate the vulnerability or include it in a POA&M by June 6, 2017, the

[20] (U) Symantec is an industry leader in providing cybersecurity products and solutions.
[21] (U) The [redacted] developed an operating environment for managing BMDS technical information. The [redacted] also maintains an enclave that provides connectivity to the [redacted]. The [redacted] L scans the operating environment and enclave monthly for vulnerabilities.

~~(S//NF)~~ [redacted] had neither mitigated the vulnerability nor included it in a POA&M by our review in July 2018. In addition, the [redacted] did not include any of the [redacted] unmitigated vulnerabilities identified in our analysis in a POA&M and did not have an explanation for not including them.

(U) Although the five DoD facilities had vulnerability management programs that identified and mitigated some vulnerabilities, only [redacted] managed risk by mitigating known network vulnerabilities or developing POA&Ms to address the security risks. The [redacted] CIO did not meet the program's expectations to manage risk when [redacted] allowed critical and high vulnerabilities to remain unmitigated on their networks. The DoD CIO stated in July 2018 that countless cyber incident reports show that the overwhelming majority of incidents are preventable by implementing basic cyber hygiene and data safeguards, which include regularly patching known vulnerabilities. Without a rigorous and systematic process to mitigate vulnerabilities in a timely manner, the [redacted] CIO increased the risk that cyberattacks or other malicious actions could exploit the vulnerabilities. As a result, BMDS technical information that is critical to national security could be compromised through cyberattacks that are designed to exploit those weaknesses. The [redacted] should develop POA&Ms and take appropriate and timely steps to mitigate known vulnerabilities.

(U) The [redacted] CIO did not meet the program's expectations to manage risk when [redacted] allowed critical and high vulnerabilities to remain unmitigated on their networks.

(U) Server Racks Were Not Consistently Secured

(U) The [redacted] data center manager and the [redacted] security manager did not consistently secure server racks in their data centers. In addition, the [redacted] data center manager did not control the server rack keys. NIST SP 800-53 requires organizations to secure keys, combinations, and other physical devices. In addition, the Defense Information Systems Agency Network Infrastructure Security Technical Implementation Guide requires all network infrastructure devices to be located in a secure room with limited access, and DoD Components to physically secure network devices using locked cabinets.[22] The guide also requires organizations to control the keys to the locked cabinets, which could include requiring individuals to sign a log when they receive and return cabinet keys.

(U) The [redacted] data center manager stated that he was not aware of the requirement to secure the server racks and keys, but considered the existing security protocols to be sufficient because the [redacted] limited who had access to the data center. Although the [redacted] controlled who accessed the data center by using CACs, server racks access

[22] (U) Network Infrastructure Policy Security Technical Implementation Guide, Version 9, Release 6, July 27, 2018.

(U) should be limited to individuals who have a specific need. Leaving the server racks unlocked and failing to control access to the keys increases the risk that insiders could compromise or exfiltrate data even though they are authorized to be in the data center.

(U) At the [redacted], we found an unlocked server rack despite a posted sign on the rack stating that the server door must remain locked at all times. After notifying the [redacted] assistant security manager, he took immediate action to secure the server rack. The [redacted] Information System Security Officer stated that network operations staff were troubleshooting issues with the server in the rack we found unlocked and failed to notify the [redacted] assistant security manager once they completed maintenance on the server so he could lock it.

(U) Failing to keep server racks locked increases the risk that unauthorized individuals could access or tamper with servers that support network operations. Locking server racks provides an additional layer of security to protect sensitive information from inappropriate activities by individuals once inside the data center. The insider threat risk necessitates that organizations implement controls, such as locking server racks and controlling the keys to the server racks, to reduce the risk of malicious personnel manipulating a server's ability to function as intended and compromising sensitive and classified data as well as the integrity and availability of the networks and systems. The [redacted] CIO should develop and implement procedures to secure server racks, validate that the racks remain locked, and control keys to the server racks.

(U) Transferred Data Was Not Always Protected and Monitored

(U) [redacted] officials did not encrypt removable media or did not enforce the use of encryption when [redacted] BMDS technical information to the [redacted]. NIST SP 800-53 requires organizations to use cryptographic mechanisms such as hash totals and checksums to prevent unauthorized disclosure and modification of information. In addition, the DoD CIO issued a memorandum in July 2007 requiring DoD Components to encrypt sensitive data stored on removable media.[23] Furthermore, the Committee on National Security Systems Directive 504 requires Federal agencies to encrypt removable media (used for data at rest) to minimize the risk of unauthorized access to sensitive data.[24] According to the security manager at the

[23] (U) DoD CIO Memorandum, "Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media," July 3, 2007.
[24] (U) Committee on National Security Systems 504, "Directive on Protecting National Security Systems from Insider Threat," September 2016. The NIST Glossary of Key Information Security Terms describes removable media as portable electronic storage media, which users insert into or remove from a computing device, and that is used to store text, video, audit information, and imagery. Examples of removable media include compact discs, digital versatile discs, universal serial bus (USB) drives, and external hard drives.

(U) The [redacted] and [redacted] encrypted less than one percent of Controlled Unclassified Information stored on removable media.

(U) [redacted] and [redacted] encrypted less than one percent of Controlled Unclassified Information stored on removable media.

(U) In August 2006, the MDA issued Directive 8500.01 requiring the encryption of data on all removable media and devices, with the exception of removable internal hard drives that are secured in a safe when not in use.[25] However, the [redacted] policy did not address external encryption requirements to ensure BMDS technical information [redacted] was protected. The [redacted] allows [redacted] to transmit BMDS technical information to [redacted] using removable media without implementing safeguards, such as encryption, to protect the information on the devices. The security manager also stated that the [redacted] did not enforce the use of encryption on removable media because [redacted] used legacy systems that lacked the capability and bandwidth to encrypt data, did not have the resources to purchase encryption software, and used encryption software that did not always align with DoD encryption software.

(U) In addition, [redacted] officials did not encrypt data stored on removable media. The system owner for the [redacted] and the Information System Security Officer for [redacted] stated that their components did not encrypt data stored on removable media because the [redacted] did not require the use of encryption. Although the [redacted] did not require data stored on removable media to be encrypted, system owners and Information System Security Officers have a responsibility to implement and enforce Federal and DoD cybersecurity policies and procedures for encrypting data stored on removable media. In May 2018, the [redacted] directed [redacted] to begin encrypting data stored on removable media using Federal Information Processing Standard 140-2 certified methods by October 9, 2018, as a condition to operate on the [redacted].[26]

(U) System owners and Information System Security Officers have a responsibility to implement and enforce Federal and DoD cybersecurity policies and procedures for encrypting data stored on removable media.

[25] (U) MDA Directive 8500.01, "Use and Management of Removable Storage Media," August 8, 2006.
[26] (U) Federal Information Processing Standard 140-2, "Security Requirements for Cryptographic Modules," May 25, 2001, provides standards for Federal organizations for using cryptographic-based security systems to protect sensitive and valuable data to maintain the confidentiality and integrity of information.

(U) [redacted] officials also stated that they were not aware of a requirement or a capability for encrypting removable media. However, the National Security Agency publishes capabilities packages that provide architecture and configuration requirements that allows organizations to implement secure solutions to protect data at rest using commercial off-the-shelf products. The capabilities packages use algorithms to implement layers of encryption to protect classified data and have been available since their release in September 2014. In addition, the Air Force developed a Trusted End Node Security solution in 2009 to encrypt removable media; this solution has been available to all DoD Components since 2013. [redacted] officials should have taken steps to identify available options for encrypting data stored on removable media to protect information critical to national security.

(U) Furthermore, [redacted] officials did not have controls in place to monitor the type and volume of classified data personnel downloaded to removable media. The Committee on National Security Systems Directive 504 also requires Federal agencies to log, audit, and monitor the use of removable media, and attribute data downloaded to removable media to specific users. According to [redacted] officials, administrators did not have the capability to record and monitor the volume of data personnel downloaded from their networks to removable media. [redacted] officials stated that [redacted] planned to begin using a log management and analysis tool and data loss prevention software to monitor the volume of data transferred to and downloaded from removable media, but did not provide a written plan or timeline for implementing that capability.[27] As of August 2018, [redacted] had not fielded additional capabilities to monitor the type and volume of data transferred to removable media nor has it developed a plan for fielding additional capabilities to monitor the use of removable media.

(U) Unless the [redacted] enforces the encryption of removable media and monitors the type and volume of data transferred to and from removable media by individual users, they will be at increased risk of not protecting sensitive and classified BMDS technical information from malicious users attempting to exfiltrate data that is critical to national security from [redacted]. Allowing the transfer of unencrypted technical information between the [redacted] also increases the risk of unauthorized access and use of critical BMDS data. The [redacted] CIOs should encrypt BMDS technical information stored on removable media. In addition, the [redacted] CIOs should develop and implement a process for identifying individuals who are authorized to use removable media on their networks and systems as well as procedures for monitoring the type and volume of data transferred to and from removable media.

[27] (U) Data loss prevention software provides the ability to identify, monitor, and protect data in use (end-point action), data in motion (network action), and data at rest (data storage) through deep packet content inspection (programs that analyze the content of information for security compliance within the entire operating system).

(U) [redacted] Did Not Implement Intrusion Detection and Prevention Controls

(U) [redacted] network administrators did not implement intrusion detection and prevention technology to restrict, block, and monitor suspicious network activities on their classified networks. Intrusion detection is the process of monitoring events or activities on a computer system or network and analyzing the events for signs of possible incidents, whereas intrusion prevention involves manual or automated processes designed to stop possible incidents from occurring.[28] Possible events are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices. Organizations use intrusion detection and prevention processes and technologies to identify possible security incidents, log information about the incidents, attempt to stop the incidents, and report the incidents to security administrators.

(U) Chairman of the Joint Chiefs of Staff Instruction 6510.01F requires agencies to monitor information systems to detect intrusions that could threaten the security of DoD operations.[29] In addition, NIST SP 800-94 requires Federal agencies to use multiple intrusion detection and prevention systems that are comprehensive and accurate in detecting and preventing malicious activities.[30] However, the [redacted] administrators stated that the [redacted] (network security device) used to protect the classified network lacked sufficient capacity (the amount of data that is able to be processed through a system) to support required intrusion detection and prevention configuration settings. Although [redacted] officials submitted a request in December 2017 to purchase technology that would support intrusion detection and prevention capabilities, the funding request had not been approved as of September 2018. Without intrusion detection and prevention capabilities, [redacted] cannot detect malicious attempts to access its networks and prevent cyberattacks designed to obtain unauthorized access and exfiltrate sensitive BMDS technical information from occurring. The [redacted] CIO should procure, install, and appropriately configure intrusion detection and prevention capabilities on [redacted] networks that maintain BMDS technical information.

[28] (U) The Committee on National Security Systems (CNSS) Glossary Number 4009, April 6, 2015.
[29] (U) Chairman of the Joint Chiefs of Staff Instruction 6510.01F, "Information Assurance and Support of Computer Network Defense (CND)," February 9, 2011, current as of June 9, 2015.
[30] (U) NIST SP 800-94, "Guide to Intrusion Detection and Prevention Systems (IDPS)," February 2007.

(U) Written Justification for System and Network Access Was Not Consistently Required or Maintained

(U) [redacted] administrators did not consistently require or maintain written justification as a condition for granting access to their networks and systems. The [redacted] administrators stated that they used access request forms to document the need for network and system access. However, the administrators did not consistently require or maintain written justification to describe the need for access. The [redacted] CIO stated that the [redacted] did not require written justification to specifically access BMDS technical information because all [redacted] users had a need to access all [redacted] data. However, NIST SP 800-53 requires system access to be granted based on the principle of least privilege, which is a security objective requiring users to have only the access needed to perform their official duties.

(U) We tested user access to the networks that contained BMDS technical information and identified instances where improvements to managing access are needed. Specifically, we selected a statistical sample of 188 of 9,059 users from the [redacted] to validate whether access was granted appropriately. At the [redacted], we selected a statistical sample of 33 of 115 users from the [redacted] to validate whether access was granted appropriately. However, [redacted] administrators from the [redacted] could not provide system access request forms for any of the 33 users; and could not determine whether the 33 users' access was granted appropriately. At the [redacted], we also selected a statistical sample of 44 of 8,117 users from the [redacted] to validate whether access was granted appropriately. [redacted] administrators for the [redacted] could not provide system access request forms for 23 of the 44 users and could not justify whether 1 of the remaining 21 users with an access request form on file was granted access appropriately. The [redacted] administrators for the [redacted] could not ensure that users' access was appropriate and the users had a need to know or access the information because they did not always retain user access forms and, for the forms that they did retain, they did not always require users and supervisors to justify why the user needed access to BMDS technical information.

(U) At the [redacted], we selected a statistical sample of 65 of 250 network users on [redacted] to validate whether access was granted appropriately. However, [redacted] administrators could not provide system access forms for 22 of the 65 users and could not explain why the forms were unavailable. Of the remaining 43 users, the system access requests included sufficient justification that described the need for accessing the [redacted].

(U) At the [redacted], we selected a statistical sample of 44 of 575 network users to validate whether access was granted appropriately. The [redacted] Information System Security Officer provided access request forms that were missing the users' justification for access; did not include actions to verify the user's need to know; and were not signed by the user's supervisor or the system owner. During the audit, the Information System Security Officer provided updated user access request forms for 43 of the 44 users, which substantiated their need for access. However, the [redacted] Information System Security Officer did not provide an updated access request form for one of the users, stating that the user was on extended leave and that [redacted] disabled the account until the user returns from leave.

(U) At the [redacted], we selected the only two network users to validate whether access was granted appropriately and found that neither of the user's access request forms included written justification supporting their need for access.

(U) At the [redacted], we could not determine whether 82 users were granted access based on assigned duties because written justification supporting their need for access was not maintained. Granting users access to the networks and systems that maintain BMDS technical information without requiring a justification for why the user needs a specific level of access could give users unnecessary access to sensitive and classified BMDS technical information that is not required to perform their assigned duties. An effective account management process that limits access to BMDS technical information based on roles that aligns with a user's assigned duties reduces the risk of intentional and unintentional disclosure of sensitive information to users who do not have a need to know the information. The [redacted] CIO should require written justification as a condition for obtaining access to all networks and systems that process, store, and transmit BMDS technical information. In addition, the [redacted] CIO should maintain access request forms for all users with access to networks and systems that contain BMDS technical information, and verify, at least annually, the continued need for access.

(U) Physical Security Controls Were Not Effective

(U) [redacted] officials did not implement effective physical security controls to limit unauthorized access to facilities that maintain BMDS technical information. NIST SP 800-53 requires organizations to authorize access to facilities. However, officials at the [redacted], did not repair a known security issue with one of the facility's doors. [redacted] security officials stated that the door's sensor erroneously showed that the door was closed and the security sensor engaged when it was not. The security site lead at [redacted] stated that the

(U) door sensors have been a problem for about 4 years. Although security officials were aware of the problem, they did not take appropriate actions to prevent unauthorized personnel from gaining unauthorized access to the facility.

(U) Although security officials were aware of the problem, they did not take appropriate actions to prevent unauthorized personnel from gaining unauthorized access to the facility.

(U) During our site visit, we observed security footage showing that a representative from the [redacted] gained unauthorized access to the [redacted] facility by simply pulling the door open. The security camera footage also showed that although the representative stopped to ask for directions, the individual she stopped did not request to see her [redacted] badge or question her facility access. Furthermore, the security footage showed that the security officer at the front desk also did not request to see her [redacted] badge. Annex F of the MDA security operations center standard operating procedures (access control) requires visitors to obtain a facility visitor badge from the access control center located in the lobby of the facility. Maintenance workers repaired the door while we were on site and we verified that the door functioned properly; however, the reoccurring security problem posed a serious threat to the safety of [redacted] personnel as well as potentially prevented the [redacted] efforts to protect BMDS technical information. Because management took action to correct the door sensors while we were on site, we do not make further recommendations for corrective action in this report. The [redacted] should provide security refresher training to security personnel and facility occupants to ensure physical security requirements, to include challenging individuals who do not display appropriate MDA badges, are met. In addition, the [redacted] should require facility security or maintenance personnel to physically verify, at least daily, that entry and exit doors operate as intended.

(U) [redacted] officials did not always install security cameras that allowed security personnel to monitor physical access throughout facilities that maintained BMDS technical information.

(U) In addition, [redacted] officials did not always install security cameras that allowed security personnel to monitor physical access throughout facilities that maintained BMDS technical information. NIST SP 800-53 requires organizations to use automated mechanisms such as security cameras to monitor physical access to facilities, and to retain video recordings to detect and respond to physical security incidents. NIST also requires organizations to implement safeguards, such as cameras, for publicly accessible areas within facilities. To meet NIST requirements, active and timely surveillance as well as archived security footage is necessary to respond to suspicious activities and physical security incidents. For example, the [redacted] installed security cameras that monitored external entry points, but the security cameras [redacted]. Facility security personnel could not explain why the security cameras did not support that functionality.

(U) At [redacted] facilities that process, store, and transmit BMDS technical information, only [redacted] monitored personnel entering and exiting doors. [redacted] security personnel stated that [redacted] planned to install additional security cameras by FY 2020 to monitor personnel activity throughout the facility. Until [redacted] installs additional security cameras, security personnel will continue to be challenged with identifying the internal movements of personnel if a physical breach occurs. Furthermore, at the [redacted], only [redacted] monitored personnel entering and exiting the facility or specific areas within the facility. At both facilities, the number and placement of security cameras did not provide sufficient surveillance to monitor activity throughout [redacted]. [redacted] officials could not explain why cameras were installed at only the select locations and not throughout the facilities.

(U) Using security surveillance equipment enables security officials to continuously monitor personnel activity, all external facility entry and exit points, and publically accessible areas for signs of unusual or prohibited behaviors. By not installing security cameras throughout facilities [redacted] decrease their ability to promptly identify and respond to security incidents and suspicious activities in and around the facilities that maintain data critical to national security. The [redacted] CIOs should assess existing security camera placements to identify gaps in security coverage and install security cameras with [redacted] to monitor personnel movements throughout their facilities.

(U) Increased Risk of Compromise of BMDS Technical Information

(U) The Army, Navy, and MDA did not protect networks and systems that process, store, and transmit BMDS technical information from unauthorized access and use. The DoD requires components to secure networks and systems using applicable security requirements prescribed in NIST SP 800-53. Security controls, such as using multifactor authentication and encrypting data, decrease the risk of unauthorized access to classified and unclassified BMDS technical information. In addition, timely identification and mitigation of vulnerabilities decreases the risk that cyberattacks could exploit known network and system weaknesses, and controlling access to servers within a data center decreases the risk of unauthorized individuals manipulating network devices. Furthermore, limiting access to BMDS technical information to users with a mission-related need to know reduces the risk of intentional or unintentional disclosures of data critical to national security. Active and passive security and

(U) surveillance measures, such as controlling keys within data centers and installing and maintaining operating security cameras that provide the ability to monitor movement throughout a facility, reduce the capability of insiders to intentionally compromise networks and systems that contain BMDS technical information.

(U) DoD systems that process, store, and transmit technical details about BMDS are exposed to greater risks unless actions are taken to improve security and reduce the threat of compromise. When security requirements are not applied or are ineffective, networks, systems, and facilities that store, process, and transmit classified and unclassified BMDS technical information are vulnerable to cyberattacks, data breaches, data loss and manipulation, and unauthorized disclosure of technical information. Inadequate security controls that result in unauthorized access to or disclosure of BMDS technical information may allow U.S. adversaries to circumvent BMDS capabilities, leaving the United States vulnerable to missile attacks that threaten the safety of U.S. citizens and critical infrastructure.

(U) The [redacted] share the responsibility for ensuring that security controls are implemented to protect BMDS technical information. The [redacted] and the CIOs for the [redacted] should assess whether the security control issues identified in this report related to not using multifactor authentication to access networks and systems that contain BMDS data; mitigating vulnerabilities in a timely manner; protecting data stored on removable media; and implementing adequate physical security controls exist at the other DoD facilities that manage BMDS technical information. The [redacted] should develop and implement a plan to ensure network, system, and physical security weaknesses are corrected.

(U) Recommendations, Management Comments, and Our Response

(U) Recommendation 1

(U) We recommend that the [redacted] develop and implement a plan to correct the systemic weaknesses at the facilities, data centers, and laboratories that manage ballistic missile defense system technical information related to:

a. (U) using multifactor authentication;

b. (U) mitigating vulnerabilities in a timely manner;

c. (U) securing server racks;

d. (U) protecting and monitoring data on removable media;

e. **(U) implementing intrusion detection controls;**

f. **(U) requiring and maintaining justifications for accessing networks; and**

g. **(U) implementing physical security controls.**

(U) Management Comments Required

(U) The [redacted] did not respond to the recommendation in the draft report. Therefore, the recommendation is unresolved. We request that the Director, Commanding General, and Commander provide comments on the final report.

(U) Recommendation 2

(U) We recommend that the [redacted]:

a. **(U) Enforce the use of multifactor authentication to access systems that process, store, and transmit ballistic missile defense system technical information or obtain a waiver that exempts the networks from using multifactor authentication.**

b. **(U) Encrypt ballistic missile defense system technical information stored on removable media.**

c. **(U) Develop and implement a process for identifying individuals who are authorized to use removable media on their networks and systems as well as procedures for monitoring the type and volume of data transferred to and from removable media.**

d. **(U) Assess existing security camera placements to identify gaps in security coverage and install security cameras with [redacted] to monitor personnel movements throughout their facilities.**

e. **(U) Develop plans of action and milestones, and take appropriate and timely steps to mitigate known vulnerabilities.**

f. **(U) Provide security refresher training to security personnel and facility occupants to ensure physical security requirements, to include challenging individuals that do not display appropriate [redacted] badges, are met.**

g. **(U) Require facility security or maintenance personnel to physically verify, at least daily, that entry and exit doors operate as intended.**

h. **(U) Require data center managers to develop and implement procedures to secure server racks, validate that the racks remain locked, and control keys to the server racks.**

i. **(U) Require written justification as a condition for obtaining access to all networks and systems that process, store, and transmit ballistic missile defense system technical information.**

j. **(U) Maintain access request forms for all users with access to networks and systems that contain ballistic missile defense system technical information, and verify, at least annually, the continued need for access.**

(U) Management Comments Required

(U) The [redacted] did not respond to the recommendation in the draft report. Therefore, the recommendation is unresolved. We request that the Director provide comments on the final report.

(U) Recommendation 3

(U) We recommend that the Chief Information Officer for the [redacted]:

a. **(U) Enforce the use of multifactor authentication to access systems that process, store, and transmit ballistic missile defense system technical information or obtain a waiver that exempts the networks from using multifactor authentication.**

b. **(U) Implement intrusion detection capabilities on networks that maintain ballistic missile defense system technical information.**

(U) Management Comments Required

(U) The [redacted] CIO did not respond to the recommendation in the draft report. Therefore, the recommendation is unresolved. We request that the CIO provide comments on the final report.

(U) Recommendation 4

(U) We recommend that the Chief Information Officers for the [redacted]:

a. **(U) Encrypt ballistic missile defense system technical information stored on removable media.**

b. **(U) Develop and implement a process for identifying individuals who are authorized to use removable media on their networks and systems as well as procedures for monitoring the type and volume of data transferred to and from removable media.**

c. (U) Assess existing security camera placements to identify gaps in security coverage and install security cameras with [redacted] to monitor personnel movements throughout their facilities.

(U) Management Comments Required

(U) The [redacted] CIOs did not respond to the recommendation in the draft report. Therefore, the recommendation is unresolved. We request that the CIOs provide comments on the final report.

(U) Recommendation 5

(U) We recommend that the Chief Information Officer for the [redacted]:

a. (U) Require data center managers to develop and implement procedures to secure server racks, validate that the racks remain locked, and control keys to the server racks.

b. (U) Require written justification as a condition for obtaining access to all networks and systems that process, store, and transmit ballistic missile defense system technical information.

c. (U) Maintain access request forms for all users with access to networks and systems that contain ballistic missile defense system technical information, and verify, at least annually, the continued need for access.

(U) Management Comments Required

(U) The [redacted] CIO did not respond to the recommendation in the draft report. Therefore, the recommendation is unresolved. We request that the CIO provide comments on the final report.

(U) Appendix

(U) Scope and Methodology

(U) We conducted this performance audit from February through October 2018 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.

(U) To understand the process used to protect classified and unclassified BMDS technical information, we interviewed officials from the [redacted]. We also interviewed system owners, chief information officers, network and system engineers, Information System Security Officers, and users to identify security controls implemented to protect classified and unclassified BMDS technical information.

(U) Additionally, we reviewed Federal laws and DoD policies, including Army, Navy, and MDA guidance to identify specific security requirements for protecting information systems, networks, and data. We selected a nonstatistical sample of 5 of the 104 DoD facilities across the [redacted] that manage BMDS elements and technical information to visit within the scope of this audit. We visited the following five locations.

- (U) [redacted]
- (U) [redacted]
- (U) [redacted]
- (U) [redacted]
- (U) [redacted]

(U) At the [redacted], we assessed the security controls and processes at the office of the [redacted] Chief Information Officer, who has a responsibility for protecting the [redacted] networks, the data centers at each location, and the following internal organizations.

- (U) [redacted]
- (U) [redacted]
- (U) [redacted]
- (U) [redacted]
- (U) [redacted]

(U) In addition, we visited [redacted] because the Military Departments maintain BMDS technical information and are responsible for operating different BMDS elements. Specifically, we assessed security risks and implemented controls over [redacted] containing BMDS technical information.

(U) At the five components, we reviewed whether the [redacted] assessed security risks and tested the suitability of implemented system security controls to protect classified and unclassified BMDS technical information from unauthorized access and disclosure. We tested the effectiveness of the following security controls for classified networks and systems related to:

- (U) boundary defense;
- (U) using encryption for data stored on systems (at rest) and data transmitted across the network (in transit);
- (U) administering and managing system access and authentication;
- (U) protecting BMDS technical information from unauthorized modification and deletion;
- (U) audit logging;
- (U) security incident handling and response; and
- (U) risk assessment.

(U) Use of Computer-Processed Data

(U) We used computer-processed data from classified [redacted] networks and databases to develop a universe of users at each site visited. System and database administrators provided us with extracts of active users from the networks and databases as Notepad and Adobe Acrobat files, and Excel spreadsheets. We used the universe of users to select a sample of users to verify the appropriateness of users' access to networks and databases that maintain BMDS technical information.

(U) We reviewed system access requests for the selected users, when available, to determine whether the justification for access described the need for access to networks and databases that maintained BMDS technical information. When system access requests were not available, we interviewed system and database administrators at each site to determine their reasons and the appropriateness of the justification for granting users access. We determined that the universe data were sufficiently reliable to test whether a users' justification for access to networks and databases was appropriate.

(U) We also used computer-processed data from the classified networks to validate the security configuration settings used to protect the networks' boundary. Network administrators from the [redacted] provided screenshots of security configuration settings as Microsoft Word files and Excel spreadsheets for firewall; intrusion detection and prevention; switch configurations; and anti-virus security configuration settings. To assess the reliability of the security configuration settings, we observed the process network administrators followed to provide evidence of the security configuration settings. We compared security configuration settings to select Security Technical Implementation Guide controls for firewall; intrusion detection and prevention; and anti-virus protection to verify compliance with DoD requirements. We determined that the data were sufficiently reliable to define the security configuration settings for each network device tested.

(U) Use of Technical Assistance

(U) The DoD Quantitative Methods Division provided assistance in developing the nonstatistical sampling methodology that we used to select system users. We also used statistical testing to test compliance for 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).[31] If the error rate exceeded the pass rate of five percent, the test was considered a failure. Table 3 shows the results of our compliance testing.

(U) Table 3. User Access Controls Test Results

Unclassified Network Location	Number of Users	Users Tested	Result
[redacted] [redacted]	115 8,117	33 44	Fail Fail
[redacted]	250	65	Fail
[redacted]	575	44	Fail
[redacted]	2	2	Fail
			Unclassified

(U) Source: The DoD OIG.

(U) Prior Coverage

(U) During the last 5 years, the DoD OIG issued one report discussing BMDS technical information. Unrestricted DoD OIG reports can be accessed at http://www.dodig.mil/reports.html/.

[31] (U) Council of the Inspector General on Integrity and Efficiency, "Journal of Public Inquiry," Fall/Winter 2012-2013.

(U) DoD OIG

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

(U) The DoD OIG identified that the MDA did not oversee its contractors' actions to protect BMDS technical information on classified and unclassified systems and networks before contract award or during the contract period of performance. The DoD OIG identified systemic weaknesses in the MDA's contractor efforts to:

- (U) configure systems to use multifactor authentication or meet password complexity requirements;
- (U) mitigate known vulnerabilities in a timely manner;
- (U) protect data at rest and in transit;
- (U) implement procedures to grant system access based on roles that align with assigned user responsibilities;
- (U) configure systems to lock automatically; and
- (U) maintain and review system audit logs.

(U) Source of Classified Information

(U) The documents listed below are sources used to support classified information within this report.

Source 1: (U) [redacted] MetricsDVL January 2018 Scan (Document classified SECRET)
Declassification Date: January 13, 2043
Generated Date: January 13, 2018

Source 2: (U) [redacted] MetricsDVL March 2018 Scan (Document classified SECRET)
Declassification Date: March 7, 2043
Generated Date: March 7, 2018

Source 3: (U) [redacted] Windows January 2018 Scan (Document classified SECRET)
Declassification Date: January 20, 2043
Generated Date: January 20, 2018

Source 4: (U) [redacted] Printer January 2018 Scan (Document classified SECRET)
Declassification Date: January 20, 2043
Generated Date: January 20, 2018

Source 5: (U) [redacted] Linux Scan January 2018 (Document classified SECRET)
Declassification Date: January 20, 2043
Generated Date: January 20, 2018

Source 6: (U) [redacted] Printer April 2018 Scan (Document classified SECRET)
Declassification Date: April 23, 2043
Generated Date: April 23, 2018

Source 7: (U) [redacted] Network Switches April 2018 Scan (Document classified SECRET)
Declassification Date: April 23, 2043
Generated Date: April 23, 2018

Source 8: (U) [redacted] Linux April 2018 Scan (Document classified SECRET)
Declassification Date: April 23, 2043
Generated Date: April 23, 2018

Source 9: (U) [redacted] Windows April 2018 Scan (Document classified SECRET)
Declassification Date: April 23, 2043
Generated Date: April 23, 2018

Source 10: (U) POA&M Export Classified [redacted] (Document classified SECRET)
Declassification Date: April 20, 2043
Generated Date: April 20, 2018

Source 11: (U) [redacted] ICOFT-RTL-IC1-1st Quarter 2018 Scan (Document classified SECRET)
Declassification Date: January 11, 2043
Generated Date: January 11, 2018

Source 12: (U) [redacted] ICOFT-RTL-IC1 May 2018 Scan (Document classified SECRET)
Declassification Date: May 29, 2043
Generated Date: May 29, 2018

Source 13: (U) ICOFT-RTL-OT2-CDWI 1st Quarter 2018 Scan (Document classified SECRET)
Declassification Date: January 11, 2043
Generated Date: January 11, 2018

Source 14: (U) ICOFT-RTL-OT2-CDWI May 2018 Scan (Document classified SECRET)
Declassification Date: May 29, 2043
Generated Date: May 29, 2018

Source 15: (U) ICOFT-RTL-SID5 1st Quarter 2018 Scan (Document classified SECRET)
Declassification Date: January 11, 2043
Generated Date: January 11, 2018

Source 16: (U) ICOFT-RTL-SID5 May 2018 Scan (Document classified SECRET)
Declassification Date: May 29, 2043
Generated Date: May 29, 2018

Source 17: (U) [redacted] Linux Vulnerability Scans (Document classified SECRET//NOFORN)
Declassification Date: June 28, 2043
Generated Date: April 27, 2018

Source 18: (U) [redacted] Windows 10 Vulnerability Scans (Document classified SECRET//NOFORN)
Declassification Date: June 28, 2043
Generated Date: April 27, 2018

(U) Acronyms and Abbreviations

[redacted] [redacted]

BMDS Ballistic Missile Defense System

CAC Common Access Card

CIO Chief Information Officer

[redacted] [redacted]

MDA Missile Defense Agency

[redacted] [redacted]

[redacted] [redacted]

[redacted] [redacted]

NIST National Institute of Standards and Technology

[redacted] [redacted]

POA&M Plan of Action and Milestones

SP Special Publication

[redacted] [redacted]

(U) Glossary

(U) Ballistic Missile Defense System (BMDS). 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.

(U) Brute Force Attack. A trial and error method used to guess passwords.

(U) Checksum. A value computed on data to detect error or manipulation.

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

(U) Data in Transit. Information transferred from one system or network to another.

(U) Data Loss Prevention. The ability to identify, monitor, and protect data in use (end-point action), data in transit (network action), and data at rest (data storage) through deep packet content inspection and contextual security analysis within a centralized management framework.

(U) Domain Controller. A server that is running a version of the Microsoft Windows Server operating system and has the Active Directory service installed.

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

(U) Hash Total. A value computed on data to detect error or manipulation.

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

(U) Intrusion Detection. The process of monitoring events that occur in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats that violate computer security policies, acceptable use policies, or standard security practices.

(U) Intrusion Prevention. The process of performing intrusion detection and attempting to stop detected possible incidents.

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

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

(U) Phishing. A method malicious actors use to masquerade as a reputable entity or person to obtain sensitive information, such as passwords and financial information.

(U) 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.

(U) Thin Client. A desktop appliance that does not contain any moving component such as a hard drive and executes applications from a central server.

(U) 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:

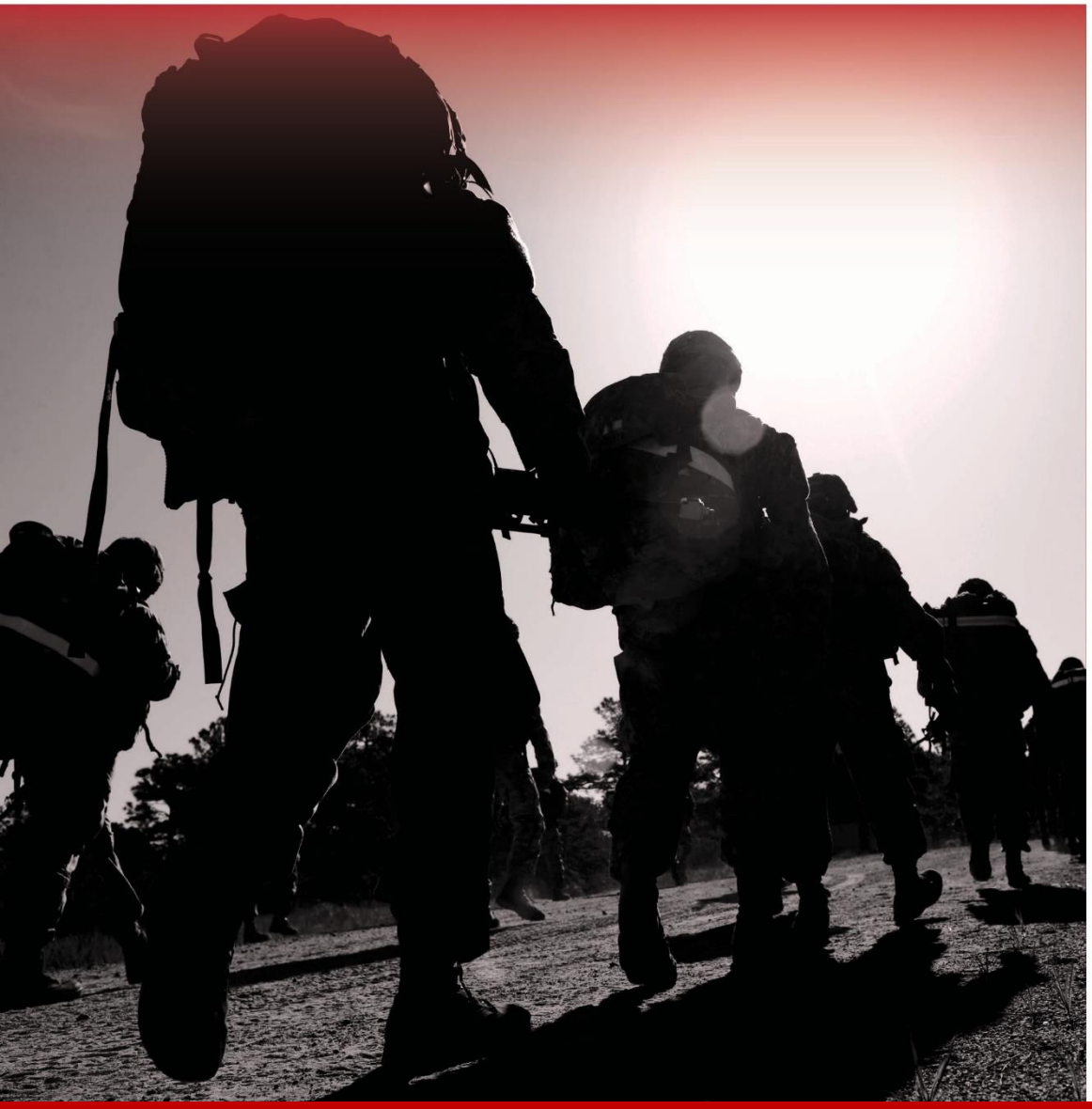
Congressional Liaison
703.604.8324

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