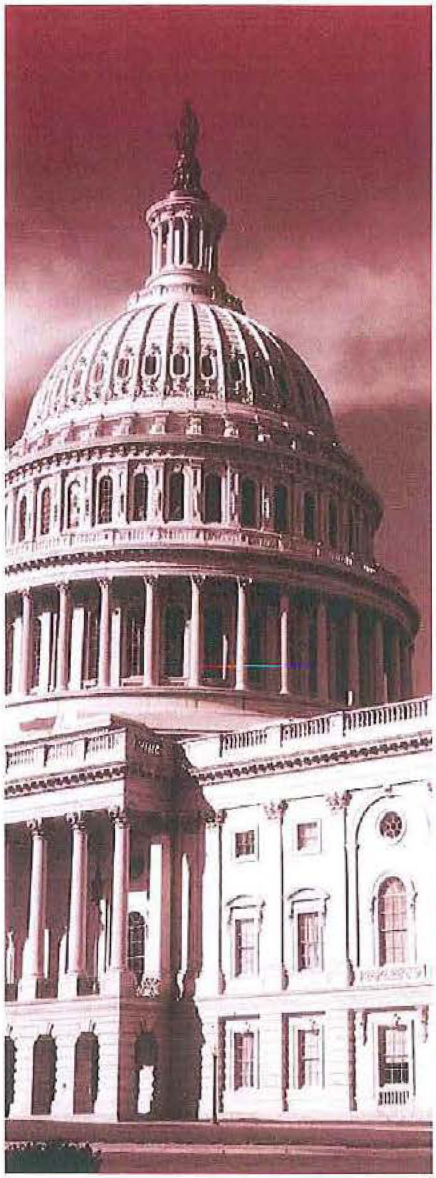
Report No. DODIG-2017-093

~~SECRET~~

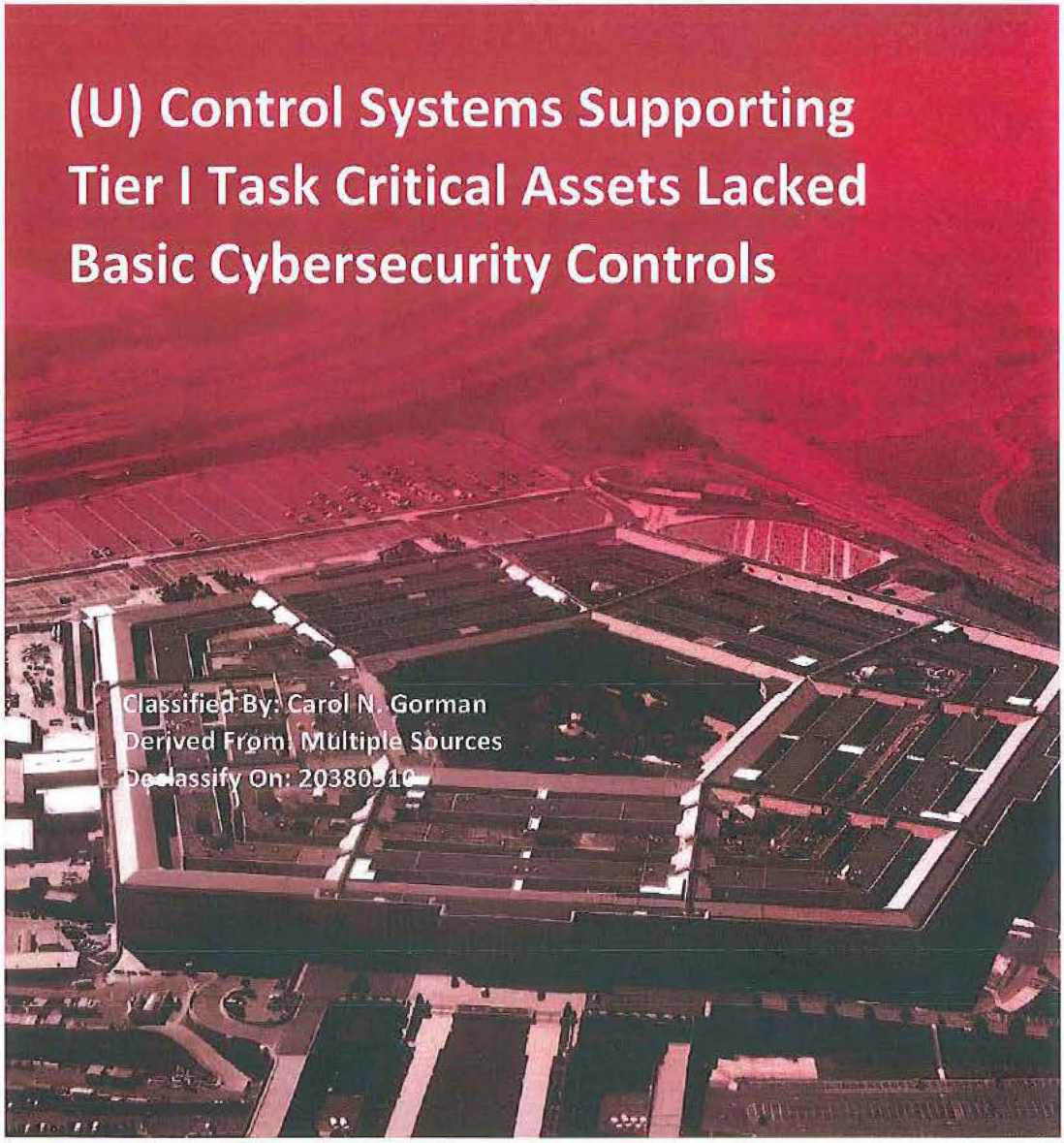
INSPECTOR GENERAL

U.S. Department of Defense

JUNE 15, 2017



(U) Control Systems Supporting Tier I Task Critical Assets Lacked Basic Cybersecurity Controls



Classified By: Carol N. Gorman
Derived From: Multiple Sources
Declassify On: 20380510

INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

~~SECRET~~

~~SECRET~~

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.

~~SECRET~~

~~SECRET~~

(U) Results in Brief

(U) Control Systems Supporting Tier I Task Critical Assets Lacked Basic Cybersecurity Controls

June 15, 2017

(U) Objective

(U) We determined whether the DoD has implemented cybersecurity controls to protect, detect, counter, and mitigate potential cyber attacks on control systems[1] that support DoD critical missions or assets.

(U) Background

(U) DoD Instruction 8510.01, "Risk Management Framework for DoD Information Technology," March 12, 2014, incorporating change 1, May 24, 2016, mandates all DoD information technology, including control systems, be appropriately secured against cyber attacks by implementing the National Institute of Standards and Technology Risk Management Framework. In the past, control systems were generally not connected to information technology networks and did not contain complex computing capabilities; therefore, they could be adequately protected using physical security measures. However, those legacy control systems and their components are being updated or replaced with commercially available hardware and software creating a greater need to secure the systems. Due to their unique performance, reliability, and safety requirements, control systems require modification to the standards that are commonly used to secure traditional information technology systems. The National Institute of Standards and Technology describes how to develop those specialized sets of security controls, known as "overlays" to reduce the need for case-by-case modifications and ensure consistent implementation. Overlays can be

(U) Background (cont'd)

(U) Government-wide, such as those published by the Committee on National Security Systems, or organization-specific, which can be approved and issued by Departments and agencies. The DoD has adopted the use of overlays and developed overlays for other non-typical information systems including nuclear command and control systems. However, the DoD has not yet incorporated a control systems overlay into its procedures.

(U) Finding

~~(S)~~ Cheyenne Mountain Air Force Station 721st and Scott Air Force Base 375th Civil Engineer Squadron Information Assurance Managers did not fully implement cybersecurity controls to protect, detect, counter, and mitigate potential cyber attacks on control systems that provide essential infrastructure services to Tier I Task Critical Assets.[2] Specifically, 721st and 375th Civil Engineer Squadron Information Assurance Managers did not:

- ~~(S)~~ sufficiently configure control systems to protect against unauthorized system modifications and counter malicious software threats; and
- ~~(S)~~ consistently monitor control system activity to detect and mitigate incidents[3] or intrusions.

[1] (U) Control Systems are specialized systems and mechanisms that ensure installation infrastructure services, such as heating, cooling, ventilation and air conditioning, are delivered when and where required to accomplish the mission.

[2] (U) Tier I Task Critical Assets are of such extraordinary importance that their loss or destruction results in failure of strategic national- or theater-level missions or functional capabilities.

[3] (U) Actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein.

(U) Results in Brief

(U) Control Systems Supporting Tier I Task Critical Assets Lacked Basic Cybersecurity Controls

(U) Finding (cont'd)

(U) Cybersecurity controls were not fully implemented because the DoD did not develop and issue an overlay to address the unique security needs for control systems. In addition, the Air Force did not update its Engineering Technical Letter 11-1 "Civil Engineer Industrial Control System Information Assurance Compliance," March 30, 2011, or provide training for implementing adequate control system cybersecurity.

~~(S)~~ The lack of adequate cybersecurity on control systems supporting Tier I Task Critical Assets put DoD missions at an increased risk of failure. For example, Scott Air Force Base and Cheyenne Mountain Air Force Station have information technology systems categorized as Tier I Task Critical Assets that depend on reliable, uninterrupted cooling provided by heating, ventilation, and air conditioning systems. A successful cyber attack on those heating, ventilation, and air conditioning control systems could allow adversaries to compromise the Tier I Task Critical Assets leading to DoD critical mission failure.

(U) Recommendations

(U) We recommend that the:

- (U) DoD Chief Information Officer develop and issue a control system overlay or mandate the use of National Institute of Standards and Technology Special Publication 800-82 Revision 2, Appendix G, as the specific set of tailored cybersecurity controls for all control systems across the Department.
- (U) Headquarters Air Force Director of Civil Engineers update Engineering Technical Letter 11-1 or issue new guidance for control system cybersecurity. When updating or issuing new (U) guidance, Headquarters Air Force Director of Civil Engineers should consider the requirements outlined in National Institute of Standards and Technology Special Publication 800-82, Revision 2, Appendix G.
- (U) Headquarters Air Force Director of Civil Engineers develop and implement cybersecurity training for all civil engineer personnel responsible for control system cybersecurity management.

(U) Management Actions Taken

(U) We provided a discussion draft with the finding and recommendations of this report to the DoD CIO and the Air Force on May 4, 2017. The DoD CIO and the Air Force agreed and had no substantive comments on the discussion draft. Therefore, we did not require a written response, and are publishing this report in final form.

(U) During the audit, we advised the Director, Cybersecurity/Acquisition Implementation and Integration, from the Office of the DoD Chief Information Officer and Air Force Deputy Director of Civil Engineers, from the Office of the Deputy Chief of Staff for Logistics, Engineering, and Force Protection, of the policy deficiencies related to control system cybersecurity. We also advised the Air Force, Deputy, Director Civil Engineers of the deficiencies related to cybersecurity training for civil engineer personnel. Furthermore, we issued a classified notice of concern to the Commander, 375th Civil Engineering Squadron, to address significant cybersecurity deficiencies requiring immediate attention.

(U) The Director, Cybersecurity/Acquisition Implementation and Integration, acknowledged the lack of control systems overlay as a deficiency and agreed to take corrective actions to update existing guidance or issue a

(U) Results in Brief

(U) Control Systems Supporting Tier I Task Critical Assets Lacked Basic Cybersecurity Controls

(U) Management Actions (cont'd)

(U) memorandum directing DoD Components to use the National Institute of Standards and Technology Special Publication 800-82, Revision 2, Appendix G, as the applicable control system overlay. The Director's response addressed all specifics of the recommendation; therefore, the recommendation is resolved but remains open. We will close the recommendation once we receive and analyze the updated or new guidance to ensure it provides a specific set of security controls for control systems.

(U) In an unsolicited response to our classified notice of concern, the Deputy Director of Civil Engineers acknowledged the lack of guidance for control systems cybersecurity and stated that Headquarters Air Force, Directorate of Civil Engineers was finalizing a replacement guidance for Engineering Technical Letter 11-1. On February 2, 2017, the Headquarters Air Force Deputy Chief of Staff for Logistics, Engineering and Force Protection issued Air Force Guidance Memorandum 2017-32-01[4] directing implementation of the National Institute of Standards and Technology Special Publication 800-82 Revision 2, Appendix G, to the greatest extent possible. The Air Force actions taken addressed all specifics of the recommendation to issue new policy for control system cybersecurity; therefore, the recommendation is closed.

(U) In addition, the Deputy Director of Civil Engineers agreed to take corrective actions to address the lack of trained civil engineer personnel responsible for control system cybersecurity. Specifically, the Deputy Director stated that the Air Force secured funding for FYs 2018 through 2022 to provide full-time cybersecurity professionals at each base dedicated to managing the control system cybersecurity efforts, including conducting and maintaining accurate inventories, performing mission support analysis, managing and configuring control system networks, conducting self-assessments of security controls, and performing cybersecurity maintenance and lifecycle management. Furthermore, in January 2017, the Deputy Director of Civil Engineers issued the "Air Force Civil Engineer Control Systems Cybersecurity Implementation Plan," which outlines a strategic approach for control system cybersecurity training across the Air Force. The Air Force response addressed all specifics of the recommendation to ensure control systems personnel are properly trained; therefore, the recommendation is resolved but remains open. We will close the recommendation once we verify that cybersecurity professionals are actively managing cybersecurity efforts at each base, and the control system cybersecurity training program is being implemented.

[4] (U) Air Force Guidance Memorandum, "Civil Engineer Control Systems Cybersecurity," February 2, 2017.

(U) Recommendations Table

Unclassified			
Management	**Recommendations Unresolved**	**Recommendations Resolved**	**Recommendations Closed**
DoD Chief Information Officer	None	1	None
Headquarters Air Force Director of Civil Engineers	None	3	2
			Unclassified

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

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

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

June 15, 2017

(U) MEMORANDUM FOR DOD CHIEF INFORMATION OFFICER
ASSISTANT SECRETARY OF THE AIR FORCE
(FINANCIAL MANAGEMENT AND COMPTROLLER)

(U) SUBJECT: Control Systems Supporting Tier I Task Critical Assets Lacked Basic Cybersecurity Controls (Report No. DODIG-2017-093)

~~(S)~~ We are providing this report for information and use. Cheyenne Mountain Air Force Station 721st and Scott Air Force Base 375th Civil Engineer Squadron Information Assurance Managers did not fully implement cybersecurity controls to protect, detect, counter, and mitigate potential cyber attacks on control systems providing essential infrastructure services to Tier I Task Critical Assets. Specifically, the Information Assurance Managers did not sufficiently configure control systems to protect against unauthorized system modifications and counter malicious software threats and did not consistently monitor control system activity to detect and mitigate incidents or intrusions. The lack of adequate cybersecurity on control systems supporting Tier I Task Critical Assets put DoD missions at an increased risk of failure. We conducted this audit in accordance with generally accepted government auditing standards.

(U) During the audit, we notified the Director, Cybersecurity/Acquisition Implementation and Integration, Office of the DoD Chief Information Officer; and the Air Force Deputy Director of Civil Engineers, Office of the Deputy Chief of Staff for Logistics, Engineering and Force Protection about the identified deficiencies. To address the lack of guidance for Air Force control systems cybersecurity, Headquarters Air Force, Deputy Chief of Staff for Logistics, Engineering and Force Protection issued Air Force Guidance Memorandum 2017-32-01, "Civil Engineer Control Systems Cybersecurity," February 2, 2017, directing the implementation of the National Institute of Standards and Technology Special Publication 800-82 Revision 2, Appendix G. The Deputy Chief of Staff's actions taken addressed all specifics of Recommendation 2; therefore, the recommendation is closed.

(U) The Headquarters Air Force Deputy Director of Civil Engineers agreed to take corrective actions to address the lack of trained civil engineer personnel responsible for control system cybersecurity. The Deputy Director stated that the Air Force secured funding for FYs 2018 through 2022 to provide full-time cybersecurity professionals at each base dedicated to managing the cybersecurity efforts. Additionally, in January 2017, the Deputy Director of Civil Engineers issued the "Air Force Civil Engineer Control Systems Cybersecurity Implementation Plan," which outlines a strategic approach for control system cybersecurity training across the Air Force. According to the

(U) implementation plan, the Air Force is evaluating training already available from both commercial and government communities to serve as the foundation for a comprehensive training program on control system cybersecurity. The Deputy Director's actions addressed all specifics of Recommendation 3; therefore, the recommendation is resolved but remains open. We will close Recommendation 3 once we verify that cybersecurity professionals are actively managing control systems cybersecurity efforts at each base, and the control system cybersecurity training program is being implemented.

(U) In addition, the Director, Cybersecurity/Acquisition Implementation and Integration, Office of the DoD Chief Information Officer, acknowledged the lack of a control systems overlay as a deficiency and agreed to take corrective actions by updating existing guidance or issuing a new instruction requiring the use of applicable control systems overlay. The Director's actions addressed all specifics of Recommendation 1; therefore, the recommendation is resolved but remains open. We will close Recommendation 1 once we obtain and analyze the guidance and determine it provides a specific set of cybersecurity controls for control systems.

(U) We appreciate the courtesies extended to the staff. Please direct questions to me at (b) (6) (DSN (b) (6)).

Carol N. Gorman
Assistant Inspector General
Readiness and Cyber Operations

(U) Table of Contents

(U) Introduction

(U) Objective

(U) Our audit objective was to determine whether the DoD implemented cybersecurity controls to protect, detect, counter, and mitigate potential cyber attacks on control systems[5] supporting DoD critical missions or assets. See Appendix A for the scope and methodology and prior audit coverage related to our objective. See the Glossary for specialized terms used throughout the report.

(U) Background

(U) The United States relies on the Internet, cyberspace systems, and data for a wide range of critical services. This reliance leaves its individuals, military, businesses, schools, and Government vulnerable to the real and dangerous cyber threats[6] posed by well-resourced foreign intelligence and military services, and non-state actors, such as terrorist groups. Since 2011, the number of reported cyber incidents on critical infrastructure[7] has more than doubled. For example, from FYs 2011 to 2015, the number of cyber incidents reported to the Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)[8] increased from 140 incidents to 295 incidents, an increase of 111 percent. Furthermore, in 2016, ICS-CERT expressed concern about the rise in targeted and successful malware campaigns allowing sophisticated threat actors to manipulate control system settings, control processes, and destroy data and equipment. According to the DoD's April 2015 Cyber Strategy, a cyber attack on the critical infrastructure that the DoD relies on for its operations could impact the U.S. military's ability to operate in a contingency.

(U) Defense Critical Infrastructure Program

(U) The DoD relies on a global network of Defense Critical Infrastructure so essential that the incapacitation, exploitation, or destruction of an asset within the network could severely affect the DoD's ability to deploy, support, and sustain its forces and operations worldwide and to implement its core missions. To identify and help assure the availability of this mission-critical infrastructure, in August 2005, the DoD established the Defense Critical Infrastructure Program[9] and formalized

[5] (U) Control systems are specialized systems and mechanisms that ensure installation infrastructure services (for example, electricity, fluids, gases, air, traffic, and people) are delivered when and where required to accomplish the mission.

[6] (U) Cyber threats include any circumstance or event with the potential to adversely affect organizational operations, assets, individuals, or the Nation through an information system through unauthorized access, destruction, disclosure, modification of information, or denial of access.

[7] (U) Critical infrastructure is defined as the systems or assets so vital to the United States that their incapacitation or destruction would have a debilitating effect on national and economic security, public health and safety.

[8] (U) The ICS-CERT mission is to guide a cohesive effort between Government and industry to improve the cybersecurity posture of control systems within the Nation's critical infrastructure. ICS-CERT coordinates control systems-related security incidents and provides focused operational capabilities for defense of control system environments against emerging threats.

[9] (U) DoD Directive 3020.40, "Defense Critical Infrastructure Program," August 19, 2005, cancelled and reissued as DoD Directive 3020.40, "Mission Assurance," November 29, 2016.

(U) the process for identifying and prioritizing its critical infrastructure in 2008.[10] The DoD annually compiles a list of Defense Critical Infrastructure consisting of all DoD-owned and non-DoD-owned infrastructure essential to accomplish the DoD's missions. To support this effort, the combatant commands and Military Services are to identify and place their critical assets into prioritized tiers, including Tier I Task Critical Assets, which are assets of such extraordinary importance that their loss or destruction results in failure of strategic national-level or theater-level missions or functional capabilities.

(U) Control Systems

(U) On DoD installations, control systems are primarily associated with ensuring installation infrastructure services—such as environmental services—are delivered when and where required to accomplish the mission. Examples include electrical infrastructure, for which control systems regulate actions, such as opening and closing switches; for water pipes, opening and closing valves; and for buildings, operating the heating, ventilation, and air conditioning (HVAC) systems.

(U) Initially, many control systems had little resemblance to traditional information technology systems because they were isolated systems running proprietary hardware and software. Additionally, control systems had long life cycles typically exceeding 20 years, while traditional information technology life cycles generally do not exceed 3 years. However, control systems and their components are being updated or replaced with Internet-capable devices and implemented using industry-standard computers, operating systems, and network protocols. While the integration of information technology solutions to control system operations supports new capabilities, it also provides significantly less isolation for control systems and increases the risk of cybersecurity vulnerabilities and attacks. In a February 2016 memorandum to the Secretary of Defense, the Commanders of U.S. Northern Command and U.S. Pacific Command identified cyber attacks to control systems as an emerging threat having serious consequences on their ability to execute critical missions if not addressed.

(U) Control System Cybersecurity Policy

(U) In March 2014, the DoD Chief Information Officer issued policy[11] establishing the requirement that all DoD information technology, including control systems,[12] be appropriately secured against cyber attacks by implementing the National Institute of Standards and Technology (NIST) Risk Management Framework. DoD Instruction 8510.01 requires systems to be categorized according to the potential impact (low, moderate, or high) resulting from the loss of confidentiality, integrity,

[10] (U) DoD Manual 3020.45-M, "Defense Critical Infrastructure Program: DoD Mission-Based Critical Asset Identification Process, Volume 1," October 24, 2008.

[11] (U) DoD Instruction 8500.01, "Cybersecurity," March 12, 2014; and DoD Instruction 8510.01, "Risk Management Framework for DoD Information Technology," March 14, 2014, Incorporating Change 1, May 24, 2016.

[12] (U) DoD Instruction 8510.01 uses the term platform information technology systems to categorize the types of systems that include control systems. The DoD defines platform information technology systems as a collection of information technology hardware and software that is physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems, and that is structured by physical proximity or by function. Because control systems are the focus of this report, we are using the term "control system" rather than "platform information technology systems."

(U) and availability if a security breach occurs. This categorization process determines the corresponding set of security controls from NIST SP 800-53, Revision 4, that should be implemented for the system. According to the NIST, although some characteristics are similar, control systems have different requirements than traditional information technology systems, which created difficulties when implementing standard security controls. Due to their unique performance, reliability, and safety requirements, control systems often require modification to the standards that are commonly used to secure traditional information technology systems. NIST guidance describes how to develop those specialized sets of security controls, known as overlays, to reduce the need for case-by-case modifications and ensure consistent implementation. Overlays can be Government-wide, such as those published by the Committee on National Security Systems, or organization-specific, which can be approved and issued by Departments and agencies. The DoD has directed the use of overlays and developed overlays for other non-typical information systems, including nuclear command and control systems. In May 2015, the NIST issued Special Publication 800-82, "Guide to Industrial Control Systems Security," Revision 2, which provides guidance on control system environments.

(U) Air Force Initiatives to Improve Security on Control Systems

(U) On March 30, 2011, the Air Force issued Engineering Technical Letter 11-1 "Civil Engineer Industrial Control System Information Assurance Compliance" to provide technical guidance and criteria for information assurance of civil engineer control systems and assign personnel responsible for implementing such requirements. Specifically, Engineering Technical Letter 11-1 requires Base Civil Engineers to appoint control systems information assurance managers (IAMs) to be responsible for implementing control systems cybersecurity. Furthermore, in June 2014, the Air Force Civil Engineer Center (AFCEC) and Air Forces Cyber signed a collaboration agreement to enhance the security of control systems that support Air Force critical infrastructure around the world. Subsequently, in 2015, the Air Force established Task Force Cyber Secure to identify and better understand cybersecurity vulnerabilities that could impact critical missions for the Air Force, including those vulnerabilities related to control systems.

(U) Review of Internal Controls

~~(S)~~ DoD Instruction 5010.40 requires DoD organizations to implement a comprehensive system of internal controls that provides reasonable assurance that programs are operating as intended and to evaluate the effectiveness of the controls.[13] We identified control weaknesses related to control systems cybersecurity. Specifically, DoD and Air Force civil engineer units did not have adequate policy and guidance to ensure consistent implementation of cybersecurity controls on control systems supporting Tier 1 task critical assets. Additionally, the Air Force did not ensure that Civil Engineer Squadron (CES) personnel received cybersecurity training. We will provide a copy of this report to the senior officials responsible for internal controls at the Office of the DoD Chief Information Officer and Headquarters Air Force, Directorate of Civil Engineers.

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

(U) Finding

(U) Control Systems Supporting Tier I Task Critical Assets Lacked Basic Cybersecurity Controls

~~(S)~~ Cheyenne Mountain Air Force Station (CMAFS) 721st and Scott Air Force Base (AFB) 375th Civil Engineering Squadron (CES) IAMs did not fully implement cybersecurity controls to protect, detect, counter, and mitigate potential cyber attacks on control systems providing essential infrastructure services to Tier I Task Critical Assets. Specifically, the IAMs did not:

- ~~(S)~~ sufficiently configure control systems to protect against unauthorized system modifications and counter malicious software[14] threats; and
- ~~(S)~~ consistently monitor control system activity to detect and mitigate incidents or intrusions.

~~(S)~~ Cybersecurity controls were not fully implemented at CMAFS and Scott AFB because the:

- (U) DoD did not develop and issue an overlay of cybersecurity controls for control systems;
- (U) Air Force did not update existing policy for control systems; and
- (U) Air Force did not provide training or guidance to base personnel for implementing cybersecurity controls on control systems.

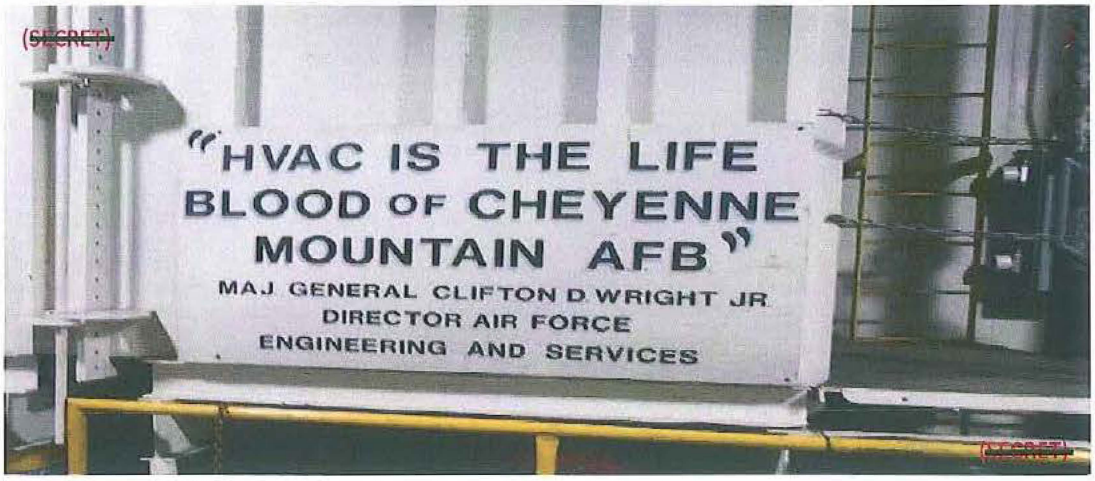
~~(S)~~ Lack of basic cybersecurity on control systems that provide essential infrastructure services to Tier I Task Critical Assets increases the risk of strategic national-level or theater-level mission failure. For example, Scott AFB and CMAFS have information technology systems categorized as Tier I Task Critical Assets that depend on reliable HVAC systems to provide uninterrupted cooling. A successful cyber attack on those HVAC control systems could allow adversaries to compromise the Tier I Task Critical Assets, leading to DoD critical mission failure.

[14] (U) Malicious software, also known as malware, is intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system.

~~(S)~~ Environmental Control Systems at Cheyenne Mountain Air Force Station and Scott Air Force Base

~~(S)~~ CMAFS and Scott AFB have mission-critical systems that require the use of building automation systems.[15] CMAFS uses the Operational Management Control System (OMCS), and Scott AFB uses the Energy Management Control System (EMCS). The OMCS and EMCS are standalone networks[16] with interconnected components throughout each base. Each installation use its systems mainly for monitoring and controlling the HVAC needs for the installation including selected Tier 1 Task Critical Assets. For example, CMAFS is a self-contained underground facility that depends on the OMCS to provide essential services, such as HVAC, throughout the complex. The following figure illustrates a quote from Major General Clifton D. Wright Jr, Director Air Force, Engineering and Services, identifying HVAC as one of the most essential services supporting CMAFS.

~~(S)~~ *Figure. Cheyenne Mountain Air Force Station*



(U) Source: DoD OIG.

[15] (U) Building automation systems, such as Energy Management Control Systems, provide centralized control—through software and hardware (for example, computer modems, sensors, controllers, and printers)—to monitor and adjust building systems (for example, temperature settings and schedules for running equipment)—such as a heating and cooling systems.

[16] (U) Standalone networks (also known as closed networks) are not connected to any other network and do not transmit, receive, route, or exchange information outside of the system's authorization boundary.

(U) Control Systems Were Not Securely Configured

~~(S)~~ CMAFS 721st and Scott AFB 375th CES IAMs did not sufficiently configure control systems to protect against unauthorized system modifications and counter malicious software (malware) threats to the OMCS and EMCS. Specifically, the IAMs did not:

- ~~(S)~~ identify and disable unnecessary control system communication ports and services; and
- ~~(S)~~ install virus protection and Windows security updates and patches as they became available.

~~(S)~~ In addition, Scott AFB 375th CES personnel did not remove computers that used unsupported operating systems from the EMCS network.

(U) Unnecessary Communications Ports and Services Were Not Disabled

~~(S)~~ CMAFS 721st and Scott AFB 375th CES IAMs did not identify and disable unnecessary control system communication ports and services. NIST SP 800-53, Revision 4, requires organizations to configure information systems to provide only essential capabilities, including prohibiting or restricting the use of unused or unnecessary ports and services. CES personnel at CMAFS 721st and Scott AFB 375th did not assess which ports and services were necessary to support the control systems or disable physical ports,[17] including USB and Ethernet ports, on their workstations. As of November and July 2016, IAMs at CMAFS and Scott AFB had been waiting 3 months and 10 months, respectively, for AFCEC guidance on how to properly configure their control systems.

~~(S)~~ The NIST states that open ports and available services are an inviting target for attackers, especially if there are known vulnerabilities associated with a given port or service.[18] For example, while not specific to CMAFS or Scott AFB, in July 2016, the National Security Agency Information Assurance Directorate issued a cybersecurity advisory to alert the DoD control system community of a commodity malware affecting building automation systems such as those used to operate HVAC, fire, and security systems.[19] The source of the malware was traced to removable media connected to control systems through physical ports.

[17] (U) The entry or exit point from a computer for connecting communications or peripheral devices.

[18] (U) NIST SP 800-128, "Guide for Security-Focused Configuration Management of Information System," August 2011.

[19] (U) National Security Agency, Information Assurance Directorate, Advisory No. IAA U/OO/801939-16, "Commodity Malware on Industrial Control Systems/Supervisory Control and Data Acquisition Devices," July 18, 2016.

(U) Anti-Virus Software Updates Not Installed Timely

~~(S)~~ The Scott AFB 375th CES IAM did not install anti-virus software updates on EMCS computers as they became available as required by NIST SP 800-53, Revision 4. Scott AFB 375th CES used McAfee anti-virus software to identify malware affecting the EMCS. The EMCS system administrator's computer had McAfee Rogue System Detection anti-virus software version 4 that was last updated on January 11, 2013. McAfee Rogue System Detection version 4 reached its end of life on December 31, 2015, and has been replaced by McAfee Rogue System Detection Version 5. According to the NIST, anti-virus software should be kept current to detect newly discovered malware affecting computer networks and prevent software from performing unintended functions that could compromise control systems' missions.[20]

(U) Anti-Virus Scans Not Performed Timely

~~(S)~~ The CMAFS 721st CES IAM did not perform timely virus scans on OMCS computers. Specifically, during our site visit in November 2016, we identified that the last virus scan was performed in July 2016. CMAFS 721st OMCS computers used the McAfee anti-virus software, which recommends monthly virus scans, while quarterly virus scans are considered to be the absolute minimum. According to the National Security Agency, malware can pose a significant threat to critical control system networks.[21] Ensuring that periodic virus scans are conducted is critical to protecting control systems from cyber attacks. Destructive malware has the capability to target a large scope of systems, removing all information and rendering the system inoperable.

(U) Operating System Security Updates Were Not Implemented

~~(S)~~ CMAFS 721st and Scott AFB 375th CES IAMs did not install operating system security updates as the updates became available. NIST SP 800-53, Revision 4, requires organizations to install security-relevant software and firmware updates as they become available. Furthermore, a National Security Agency Information Assurance Directorate publication recommends that system administrators apply security patches and upgrades to remove known vulnerabilities before the vulnerabilities are exploited in a cyber attack.[22] During our site visit in November 2016, we observed CMAFS OMCS computers with Windows 7 operating systems that had not been updated since November 20, 2015. The 721st CES control system IAM stated that the OMCS contractor provided computers with pre-loaded operating system security configurations, but the IAM had not installed any security updates thereafter. The IAM stated that he did not have the training to

[20] (U) NIST SP 800-83, "Guide to Malware Incident Prevention and Handling," November 2005.

[21] (U) National Security Agency Information Assurance Directorate "Securely Managing Industrial Control System Networks," October 1, 2015.

[22] (U) National Security Agency, Information Assurance Directorate, "Securing Assets within a Closed Industrial Control Systems Network Perimeter," October 1, 2015.

~~(S)~~ identify or implement applicable security updates for the OMCS. At Scott AFB, the 375th CES control system IAM stated that she could not remember the last time she installed an operating system security update on the EMCS computers. Cyber attacks on out-of-date operating systems have a higher chance of success because adversaries can exploit known vulnerabilities to gain access to the control system network.

~~(S)~~ Computer Using Unsupported Operating System at Scott AFB Was Not Removed from Control System Network

~~(S)~~ The Scott AFB 375th CES IAM did not remove a computer that used an unsupported operating system from the EMCS network. NIST SP 800-53, Revision 4, requires the replacement of information system components when support for the component is no longer available from the developer, vendor, or manufacturer. During a September 2015 risk assessment at Scott AFB, AFCEC identified an EMCS computer that used an unsupported operating system. Although, Scott AFB 375th CES personnel corrected the vulnerability, we found another computer on the EMCS network that used an unsupported operating system. Specifically, an EMCS computer at building 1575 used the Windows XP operating system, which was no longer supported by Microsoft as of April 8, 2014. While we did not identify specific cyber attacks to the EMCS, industry best practices and reported incidents show that successful cyber attacks are more likely to occur if an unsupported operating system is used. The use of unsupported operating systems increases the risk of successful cyber attacks on the EMCS network because Windows XP has well-known severe security flaws that cannot be fully removed.

(U) Control Systems Were Not Consistently Monitored to Detect and Mitigate Incidents or Intrusions

~~(S)~~ CMAFS 721st and Scott AFB 375th CES IAMs did not consistently monitor control systems to detect and mitigate cybersecurity incidents or intrusions. Specifically, CMAFS 721st and Scott AFB 375th CES personnel did not:

- ~~(S)~~ perform vulnerability testing on control system computers; and
- ~~(S)~~ consistently review audit logs for inappropriate and unusual activity, or protect audit logs from manipulation.

~~(S)~~ In addition, Scott AFB 375th CES personnel did not test contractor maintenance computers for malware and vulnerabilities before contractors connected them to the EMCS network.

(U) Routine Vulnerability Testing Not Conducted

~~(S)~~ CMAFS 721st and Scott AFB 375th CES IAMs did not perform routine vulnerability testing on their control systems. NIST SP 800-53, Revision 4, requires organizations to perform vulnerability testing[23] on information systems and applications. According to the NIST, vulnerability testing can identify out-of-date software versions and application patches or system upgrades. In addition, vulnerability testing can identify open ports and associated vulnerabilities. The only vulnerability testing performed on the Scott AFB EMCS and CMAFS OMCS was performed by AFCEC on September 14, 2015, and August 9, 2016, respectively. Both control system IAMs stated that they did not have the time or experience to perform such testing.

(U) Audit Logs Not Consistently Reviewed or Protected

~~(S)~~ CMAFS 721st and Scott AFB 375th CES personnel did not consistently review the audit logs for the Windows operating system or the control system software to detect inappropriate or unusual activity. NIST SP 800-53, Revision 4, requires organizations to review and analyze audit logs to identify indications of unusual and malicious activity. The CMAFS 721st CES IAM stated that he did not review the Windows or control system software audit logs because he did not have the time or experience to properly conduct audit logs reviews. The Scott AFB 375th CES system administrator stated that he reviewed audit logs every 2 to 3 months or whenever necessary; however, when asked, he could not provide evidence to support that those reviews occurred. In addition, the system administrator stated that he was not trained to perform audit log reviews and that the method he used was based on his experience and knowledge performing job-related duties.

~~(S)~~ Furthermore, the CMAFS 721st CES IAM did not protect OMCS audit logs from manipulation or deletion because he was not trained on how to protect audit logs. NIST SP 800-53, Revision 4, requires information system owners to protect audit information and audit tools from unauthorized access, modification, and deletion. However, we observed that CMAFS CES personnel with OMCS access could delete single audit log events and entire logs from the audit log archives, which enables suspicious or malicious activities to go undetected.

~~(S)~~ Maintenance Computers at Scott AFB Not Tested for Malware and Vulnerabilities

~~(S)~~ Scott AFB 375th CES personnel did not test contractor maintenance computers for malware or vulnerabilities before contractor personnel connected their computers to the EMCS network. NIST SP 800-53, Revision 4, requires organizations to approve, control, and monitor maintenance tools to prevent malicious code from entering a control system network. During our site visit in July 2016, the 375th CES IAM stated that contractor personnel perform routine maintenance to update the EMCS software using company-provided laptops. The 375th CES IAM stated she did not perform any security testing of contractor laptops to mitigate the risk of malicious software infecting the EMCS network. In July 2011, the Idaho National Laboratory, Critical Infrastructure

[23] (U) Vulnerability testing involves scanning for improperly configured or incorrectly operating information flow control mechanisms.

~~(S)~~ Cyber Assessment Team, reported the same EMCS network vulnerability at Scott AFB, noting that contractors use contractor-provided laptops for personal use and to perform maintenance functions. ICS-CERT has reported that infected contractor laptops are a significant source for malware and one of the most common and exploitable control system weaknesses. For example, while not specific to Scott AFB, in 2016, ICS-CERT identified two successful cyber attacks that compromised control systems by targeting contractors' maintenance tools. Those attacks allowed sophisticated cyber threat groups to gain direct access to hundreds of control systems globally.

(U) DoD and Air Force Guidance and Training for Control System Cybersecurity Was Inadequate

~~(S)~~ Cybersecurity controls were not fully implemented at CMAFS and Scott AFB because the:

- (U) DoD guidance did not clearly define control systems cybersecurity requirements;
- (U) Air Force did not update existing policy for control systems; and
- (U) Air Force did not provide training to CES personnel on how to implement cybersecurity controls on control systems.

(U) DoD Guidance Did Not Define Cybersecurity Requirements for Control Systems

(U) The DoD Chief Information Officer did not finalize the overlay or promulgate the requirement to use NIST SP 800-82, Revision 2, Appendix G.[24] According to officials from the DoD Chief Information Officer and Deputy Assistant Secretary of Defense for Energy, Installations, and Environment, the DoD developed a draft control system overlay in 2013 but agreed to stop the effort and instead refer to NIST SP 800-82, Revision 2, Appendix G, as the applicable control system overlay to avoid duplication of effort. However, the officials stated that DoD policy had not been updated to mandate the use of NIST SP 800-82, Revision 2, Appendix G. The DoD Chief Information Officer should develop and finalize the control system overlay or mandate the use of NIST SP 800-82 to address the unique control systems' security requirements.

(U) Air Force Control Systems Cybersecurity Policy Outdated

(U) In 2011, the Air Force issued Engineering Technical Letter 11-1, which provides guidance for civil engineer control system cybersecurity; however, the policy refers to superseded guidance. Specifically, the Air Force policy recommends using NIST SP 800-53, Revision 3, Appendix I, as best practices for securing control systems. Subsequently, Revision 3 was superseded by Revision 4 in April 2014. NIST SP 800-53 Revision 4 did not include Appendix I, which was transferred to NIST SP 800-82. In addition, NIST SP 800-82, Appendix G, outlines tailored security controls for control systems. As of January 2017, the Air Force had not updated Engineering Technical Letter 11-1 to require the use of NIST SP 800-82 or specified a tailored set of controls from

[24] (U) NIST SP 800-82, Revision 2 "Guide to Industrial Control Systems Security," May 2015.

(U) NIST SP 800-53, Revision 4. The Air Force should update Engineering Technical Letter 11-1 or issue new guidance for control system cybersecurity and consider the requirements of NIST SP 800-82, Revision 2, Appendix G to better secure Air Force control systems against cyber attacks.

(U) Civil Engineer Squadron Personnel Lacked Training

~~(S)~~ CMAFS 721st and Scott AFB 375th CES personnel were not fully trained to perform their control systems responsibilities. Both control system IAMs stated that they were appointed to the IAM position because they met the position qualifications, such as an Information Assurance Technical Level II certification, as required by Engineering Technical Letter 11-1. According to the CMAFS control system IAM, the only training offered was from the contractor who provides service for the control system and the training was unrelated to cybersecurity. The control system IAM at Scott AFB stated that besides her previous knowledge in cybersecurity, she had received no further training on control systems. CMAFS and Scott AFB CES personnel were unaware of known vulnerabilities directly affecting their control system components or how their control systems directly impact critical missions and assets at their facility. Therefore, the Air Force should develop and implement cybersecurity training for all civil engineer personnel responsible for control system cybersecurity management.

(U) Unsecured Control Systems Put DoD Missions at an Increased Risk of Failure

~~(S)~~ Lack of cybersecurity on control systems that provide essential infrastructure services to Tier I Task Critical Assets put DoD missions at increased risk of failure. Because of interdependencies of infrastructure services and defense critical assets, a successful cyber attack exploiting the EMCS and OMCS vulnerabilities identified in this report could lead to severe consequences to DoD missions that depend on those assets. For example, CMAFS is home to the 721st Communications Squadron Technical Control Facility, a Tier I Task Critical Asset that supports the air, space, and missile missions, as well as several other critical missions. The Technical Control Facility also houses the information technology servers for two additional Tier I Task Critical Assets, Missile Warning Center[25] and the Global Strategic Warning/Space Surveillance Systems Center.[26] The Technical Control Facility depends on reliable HVAC services to provide adequate cooling for these servers. Because HVAC services are monitored and controlled through the OMCS, a successful cyber attack could allow adversaries direct access to control the environmental operations for CMAFS. In 2015, the Defense Threat Reduction Agency reported that the loss of HVAC services to the Technical Control Facility would shut down critical equipment supporting the Missile Warning Center and degrade a combatant command's ability to execute their missions.

[25] ~~(S)~~ The Missile Warning Center uses a worldwide sensor and communication network to provide warning of missile attacks, either long or short range, launched against North America and forces overseas.

[26] ~~(S)~~ The Warning/Space Surveillance Systems Center is responsible for the operations and configurations of the communication processing node for the space surveillance and situational awareness mission.

~~(S)~~ In addition, at Scott AFB, building 1575 is a critical base communications facility and primary data center for the Tanker Airlift Control Center, Air Mobility Command, U.S. Transportation Command, and the Army Surface Deployment and Development Command. Building 1575 contains the Global Decision Support System, which is Army Material Command's primary command and control system used for mission planning and execution of airlift and air refueling assets. The EMCS provides heating and cooling for building 1575. A successful cyber attack exploiting the vulnerabilities on the OMCS could allow adversaries direct access to control the environmental operations in building 1575, causing critical information technology equipment to overheat and fail. In 2013, the Defense Threat Reduction Agency reported that a compromise to EMCS could cause extended outages of Global Decision Support System servers and disrupt or incapacitate the U.S. Transportation Command critical airlift and refueling missions.

(U) Suggested Actions, Management Comments, and Our Response

~~(S)~~ During the audit, we notified Scott AFB 375th CES personnel in a classified notice of concern that they had not implemented basic cybersecurity controls for the EMCS (See Appendix B). We suggested that management immediately:

- ~~(S)~~ disable unnecessary ports and services;
- ~~(S)~~ install updates and security patches on EMCS computers and software; and
- ~~(S)~~ test contractor laptops for malware and vulnerabilities before connecting them to the EMCS network.

~~(S)~~ Scott AFB 375th CES Comments

~~(S)~~ In response to the classified notice of concern, the 375th CES Operations Flight Commander agreed and provided a copy of the finalized EMCS System Security Plan, which specifically addresses all suggested actions.

(U) Our Response

~~(S)~~ We reviewed the EMCS System Security Plan and verified that it included procedures to address our suggested actions, such as disabling unnecessary ports, installing software and security updates, and using approved Government-owned computers to perform maintenance functions in the EMCS network.

(U) Recommendations, Management Comments, and Our Response

(U) Recommendation 1

(U) We recommend that the DoD Chief Information Officer develop and issue a control system overlay or mandate the use of National Institute of Standards and Technology Special Publication 800-82 Revision 2, Appendix G, as the tailored set of cybersecurity controls for all control systems across the DoD.

(U) DoD CIO Comments

(U) During the audit, we met with the Director, Cybersecurity/Acquisition Implementation and Integration, from the Office of the DoD Chief Information Officer to discuss our preliminary findings and obtain clarification on the control systems overlay referenced in DoD Instruction 8510.01. We notified the Director that DoD Instruction 8510.01 directs DoD Components to implement cybersecurity controls from the applicable control systems overlay, but the overlay has not yet been developed or specified. The Director acknowledged that the DoD had not developed an overlay and agreed to revise DoD Instruction 8510.01 or issue a Cybersecurity Clarification Memorandum requiring the use of NIST SP 800-82, Revision 2, Appendix G, as the applicable overlay for control systems.

(U) Our Response

(U) The Director's response addressed all specifics of our recommendation; therefore, the recommendation is resolved but remains open. We will close Recommendation 1 once we obtain and analyze the guidance and ensures that it provides a specific set of security controls for control systems.

(U) Recommendation 2

(U) We recommend that the Headquarters Air Force Director of Civil Engineers update Engineering Technical Letter 11-1 or issue new guidance for control system cybersecurity. When updating or issuing guidance, Headquarters Air Force Director of Civil Engineers should consider adding the requirements outlined in National Institute of Standards and Technology Special Publication 800-82, Revision 2, Appendix G.

(U) Air Force Comments

~~(S)~~ In an unsolicited response to the notice of concern, the Air Force Deputy Director of Civil Engineers, from the Office of the Deputy Chief of Staff for Logistics, Engineering, and Force Protection, agreed that civil engineer units did not have adequate policy guidance and resources to mitigate the vulnerabilities. On February 2, 2017, the Deputy Chief of Staff for Logistics, Engineering, and Force Protection issued Air Force Guidance Memorandum 2017-32-01, "Civil Engineer Control Systems," which requires Air Force personnel to implement NIST control systems

~~(S)~~ guidelines[27] to the greatest extent possible across all civil engineer-owned or operated control systems. The memorandum superseded Engineering Technical Letter 11-1. The memorandum establishes specific security controls and procedures for deficiencies identified in this report. For example, the memorandum includes procedures for managing computers that use unsupported operating systems and outdated anti-virus software, disabling unnecessary ports and services, and conducting maintenance procedures.

(U) Our Response

(U) The Air Force issued the Air Force Guidance Memorandum 2017-32-01, "Civil Engineer Control Systems Cybersecurity," February 2, 2017, directing the implementation of the National Institute of Standards and Technology Special Publication 800-82 Revision 2, Appendix G. The memorandum also establishes specific security controls and procedures for deficiencies identified in this report. The actions taken in response to the notice of concern addressed all specifics of the recommendation; therefore, Recommendation 2 is closed.

(U) Recommendation 3

(U) We recommend that Headquarters Air Force Director of Civil Engineers develop and implement cybersecurity training for all civil engineer personnel responsible for control system cybersecurity management.

(U) Air Force Comments

(U) In an unsolicited response to the notice of concern, the Air Force Deputy Director of Civil Engineers agreed, stating that the Air Force secured funding for FYs 2018 through 2022 to provide full-time cybersecurity professionals at each base. The cybersecurity professionals will be dedicated to managing the cybersecurity efforts including conducting and maintaining accurate inventories, performing mission support analysis, managing and configuring control system networks, conducting self-assessments of security controls, and performing cybersecurity maintenance and life cycle management. Furthermore, in January 2017, the Deputy Director of Civil Engineers issued the "Air Force Civil Engineer Control Systems Cybersecurity Implementation Plan," which outlines a strategic approach for control system cybersecurity training across the Air Force. According to the implementation plan, the Air Force is evaluating training already available from both commercial and government communities to serve as the foundation for a comprehensive training program on control system cybersecurity.

[27] (U) NIST SP 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations," April 2013; and NIST SP 800-82, Revision 2, "Guide to Industrial Control Systems Security," May 2015.

(U) Our Response

(U) The Air Force addressed all specifics of our recommendation; therefore, the recommendation is resolved but remains open. We will close Recommendation 3 once we verify that cybersecurity professionals are actively managing cybersecurity efforts at each base, and the control system cybersecurity training program is being implemented.

(U) Appendix A

(U) Scope and Methodology

(U) We conducted this performance audit from May 2016 through April 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

(U) During the audit, we met with officials from the following offices:

- (U) Under Secretary of Defense for Acquisition, Technology, and Logistics;
- (U) Under Secretary of Defense for Policy;
- (U) DoD Chief Information Officer;
- (U) U.S. Cyber Command;
- (U) Air Force Office of Information Dominance and Chief Information Officer (SAF/CIO A6);
- (U) Air Force Operations (A3) and Civil Engineering (A4);
- ~~(S)~~ Cheyenne Mountain Air Force Station (CMAFS);
- ~~(S)~~ Scott Air Force Base (AFB); and
- (U) Joint Staff Operations (J3) and C4 and Cyber (J6).

(U) We reviewed the following criteria:

- (U) National Institute of Standards and Technology Special Publication 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations," April 2013;
- (U) National Institute of Standards and Technology Special Publication 800-82 Revision 2, "Guide to Industrial Control System Security," May 2015;
- (U) DoD Instruction 8500.01 "Cybersecurity," March 14, 2014;
- (U) DoD Instruction 8510.01 "Risk Management Framework for DoD Information Technology," March 12, 2016 Incorporated Changes May 24, 2016;
- (U) Air Force Instruction 33-210, "Air Force Certification and Accreditation Program," December 23, 2008; and
- (U) Air Force Engineering Technical Letter 11-1: "Civil Engineer Industrial Control System Information Assurance Compliance," March 30, 2011.

~~(S)~~ We obtained DoD and Air Force Tier I Task Critical Assets lists from the Assistant Secretary of Defense for Homeland Defense and Global Security, and Headquarters Air Force, Operations Policy Division. We analyzed the critical asset lists and selected CMAFS and Scott AFB based on the number of Tier I Task Critical Assets and impact to DoD missions if assets were compromised.

~~(S)~~ We conducted site visits at CMAFS and Scott AFB. While on site, we interviewed IAMs, Integrated Mechanical Control Technicians (system administrators), and control system users at CMAFS and Scott AFB. Those personnel were responsible for the daily operations of control systems. We also interviewed personnel from the CES, Mission Support Group, Security Forces Squadron, and Communication Squadron to understand their roles and responsibilities related to control systems. We reviewed and tested security controls over OMCS and EMCS at CMAFS and Scott AFB, respectively. Specifically, we reviewed 13 control families from NIST SP 800-53, Revision 4, and tested whether selected security controls were implemented for control systems supporting the Tier I Task Critical Assets.

(U) We reviewed the following control families from NIST SP 800-53, Revision 4.

- (U) AC-Access Controls
- (U) AU-Audit and Accountability
- (U) CA-Security Assessment and Authorization
- (U) CM-Configuration Management
- (U) CP-Contingency Planning
- (U) IA-Identification and Authentication
- (U) MA- Maintenance
- (U) PE-Physical and Environmental
- (U) PL-Planning
- (U) RA-Risk Assessment
- (U) SA-System and Services Acquisition
- (U) SI-System and Information Integrity Policy and Procedures
- (U) SC-System and Communications Protections

(U) Furthermore, we reviewed local guidance for the control systems cybersecurity, including System Security Plans. In addition, we obtained and reviewed documentation regarding the operation, configuration, and management of the control systems.

(U) Use of Computer-Processed Data

(U) We did not use computer-processed data to perform this audit.

(U) Prior Coverage

(U) During the last 5 years, the Government Accountability Office (GAO), the Department of Defense Office Inspector General (DoD OIG), and the Air Force Audit Agency issued four reports on control systems relating to our objective. Unrestricted GAO reports can be obtained at http://www.gao.gov. Unrestricted DoD OIG reports can be accessed at http://www.dodig.mil/audit/reports. Unrestricted Air Force reports can be accessed from https://www.efoia.af.mil/palMain.aspx by clicking on Freedom of Information Act Reading Room and then selecting audit reports.

(U) GAO

(U) Report No. GAO-15-749, "Defense Infrastructure – Improvements in DoD Reporting and Cybersecurity Implementation Needed to Enhance Utility Resilience Planning," July 2015.

(U) The audit objective was to determine whether threats and hazards caused utility disruptions on DoD installations and, if so, what impacts they have had, the extent to which the DoD's collection and reporting on utility disruptions are comprehensive and accurate, the extent to which the DoD has taken actions and developed and implemented guidance to mitigate risk to operations at its installations in the event of utility disruption. The GAO found that DoD installations experienced utility disruptions resulting in operation and fiscal impacts due to hazards such as mechanical failure, extreme weather, and cyber attacks. The GAO also found the collection and reporting of utility disruption data was not comprehensive and contained inaccuracies. However, the GAO reported that Military Services have taken actions to mitigate risks posed by utility disruptions and had generally taken steps in response to DoD guidance related to utility resilience.

(U) The GAO recommended that the DoD work with the Military Services to clarify utility disruption reporting guidance, improve data validation steps, and address challenges to addressing cybersecurity Industrial Control System guidance. Furthermore, the GAO recommended that the Secretary of Defense direct the Secretaries of the Army, Navy, and Air Force; and Commandant of the Marine Corps to address challenges related to inventorying existing industrial control systems, identifying personnel with the appropriate expertise, and programing and identify funding, as necessary.

(U) DoD OIG

(U) Report No. DODIG-2013-119, "Better Procedures and Oversight Needed to Accurately Identify and Prioritize Task Critical Assets," August 16, 2013.

(U) The audit objective was to determine whether Defense Critical Infrastructure Program lists of Task Critical Assets were accurate and prioritized based on established criteria. We found the Defense Critical Infrastructure Program Task Critical Asset lists were not accurate or prioritized based on established criteria. We recommended the Under Secretary of Defense for Policy amend the Defense Critical Infrastructure Program policy to require reviews of critical assets and implement an approach to facilitate asset information sharing among DoD Components. Furthermore, we recommended a comprehensive program review process to verify whether Defense Critical Infrastructure Program Task Critical Asset lists processes are effective.

(~~FOUO~~) Report No. DODIG-2013-036, "Improvements Are Needed to Strengthen the Security Posture of USACE, Civil Works, Critical Infrastructure and Industrial Control Systems in the Northwestern Division," January 14, 2013.

(~~FOUO~~) The audit objective was to determine whether U.S. Army Corps of Engineers, Civil Works, personnel implemented effective procedures and security controls over critical infrastructure to protect against unauthorized access from physical and cyber threats that affect information systems used to operate water control structures. We found that the U.S. Army Corps of Engineers personnel did not fully implement physical security controls to secure and protect critical infrastructure and Industrial Control Systems against unauthorized access from physical and cyber threats. We recommended that the Commanders and District Engineers implement required physical security measures in accordance with the U.S. Army Corps of Engineers, "Baseline Security Posture Guide for Civil Works Projects." In addition, we recommended that the Chief, Hydroelectric Design Center conduct required vulnerability assessments.

(U) Air Force Audit Agency

(U) Report No. F2014-0008-O10000, "Civil Engineer Platform Information Technology Security," September 4, 2014.

(U) The audit objective was to determine whether Air Force Civil Engineering personnel effectively identified and registered industrial control systems, coordinated identification and registration of non-industrial control systems, conducted industrial control systems information assurance risk assessments, and implemented industrial control systems information assurance controls. The Air Force Audit Agency found that Civil Engineer personnel did not identify or register Civil Engineer industrial control systems; coordinate identification and register non-industrial control systems information assurance; conduct industrial control systems information assurance risk assessments; and implement industrial

(U) control systems information assurance controls. The Air Force Audit Agency recommended the Air Force conduct an Air Force-wide data call to identify all civil engineer industrial control system, conduct risk assessments on all identified civil engineer industrial control systems, and implement Air Force Instruction 33-210 requirements for all applicable information assurance controls for industrial control systems.

(U) Appendix B

(U) Notice of Concern

~~SECRET~~

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

October 28, 2016

(U) MEMORANDUM FOR COMMANDER, 375TH CIVIL ENGINEERING SQUADRON

~~(FOUO)~~ SUBJECT: Cybersecurity Vulnerabilities Identified During the Audit of Control Systems Cybersecurity at Scott Air Force Base (Project No. D2016-D000RB-0149.000)

~~(FOUO)~~ We are issuing this notice of concern to address concerns identified during our ongoing Audit of Control Systems Cybersecurity at Scott Air Force Base (AFB). Our audit objective is to determine whether the DoD has implemented cybersecurity controls to protect, detect, counter, and mitigate potential cyber attacks on control systems supporting DoD critical missions and assets. This notice of concern pertains to cybersecurity controls assessed for the Energy Management Control System (EMCS) at Scott AFB. We are concerned that the Air Mobility Command, through its subordinate unit, the 375th Civil Engineering Squadron (CES), has not ensured the implementation of cybersecurity controls on the EMCS. We identified three areas of concern that we believe require immediate attention. The work conducted on this audit is preliminary, and there is additional work ongoing to satisfy the audit objective. We will continue to analyze and summarize additional information obtained during our visit to Scott AFB that will be presented in our final report.

(U) Background

~~(U)~~ Scott AFB 375th CES personnel use the EMCS to monitor and control the operation of building utility and environmental systems through the Metasys software application developed and maintained by Johnson Controls Incorporated (JCI). The EMCS is a standalone Supervisory Control and Data Acquisition network hardwired to assets in various Scott AFB buildings. EMCS provides heating, ventilation, and air conditioning control, monitoring, and alarm notification in the buildings, to include building 1575. Building 1575 is identified as a Tier I Task Critical Asset[1] serving as the telecommunications hub for the majority of Scott AFB tenants and the primary data center for the 618th Tanker Airlift Control Center, Air Mobility Command, U.S. Transportation Command, and the Army Surface Deployment and Development Command. Building 1575 houses multiple information technology servers, such as

[1] (U) Tier I Task Critical Assets are defined as an asset the loss, incapacitation, or disruption of which could result in mission (or function) failure at the DoD, Military Department, Combatant Commands, sub-unified command, Defense agency, or Defense Infrastructure Sector Lead Agent levels.

Derived From: Multiple Sources
Declassify by: 20370518

1

~~SECRET~~

(U) Notice of Concern (cont'd)

~~SECRET~~

~~(S)~~ Global Decision Support System servers that U.S. Transportation Command and the Air Mobility Command use as the primary command and control system for planning and executing airlift and refueling operations.

~~(FOUO)~~ EMCS Lacked Basic Cybersecurity Controls

~~(FOUO)~~ During our site visit conducted from July 18 to July 22, 2016, we identified three concerns that require immediate attention. Specifically, Scott AFB 375th CES personnel did not:

- ~~(FOUO)~~ test JCI maintenance computers for malware and vulnerabilities before contractors connected them to the EMCS network,
- ~~(FOUO)~~ install updates and security patches on EMCS computers and software as they became available, and
- ~~(FOUO)~~ disable unnecessary EMCS communication ports and services.

~~(S)~~ According to the Scott AFB Industrial Control Systems (ICS) Information Assurance Manager, 375th CES personnel did not test JCI maintenance computers for malware or vulnerabilities before JCI personnel connected the computers to the EMCS network. In July 2011, the Idaho National Laboratory (INL), Critical Infrastructure Cyber Assessment Team, reported the same EMCS network vulnerability at Scott AFB, noting that contractors may use personal or contractor-provided laptops to perform maintenance functions. The Department of Homeland Security, Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) responsible for issuing alerts on control system vulnerabilities, reported that infected contractor laptops are a significant source for malware and one of the most prevalent and exploitable control system weaknesses. For example, while not specific to Scott AFB, ICS-CERT identified two successful cyber attacks that compromised control systems by targeting contractors' maintenance tools. Those attacks allowed sophisticated cyber threat groups to gain direct access to hundreds of control systems globally.

~~(S)~~ The 375th CES personnel also did not install updates and security patches on EMCS computers or software as they became available. On July 20, 2016, we conducted a walkthrough of the main computing facility, located in building 60. During the walkthrough, we observed the alternate ICS Information Assurance Manager using one EMCS computer with McAfee antivirus software that was last updated on January 11, 2013. In addition, although most EMCS computers had Windows 7 installed, we found the use of unsupported operating systems was a prevailing weakness on the EMCS network. Specifically, during our walkthrough, we observed that an EMCS workstation at building 1575 used the Windows XP operating system, which was no longer supported by Microsoft as of April 8, 2014. During a September 2015 risk assessment at Scott AFB, the Air Force Civil Engineering Center identified the use of unsupported operating

(U) Notice of Concern (cont'd)

~~SECRET~~

~~(S)~~ systems on EMCS assets as a Category I vulnerability.[2] Although the vulnerability was corrected for the computer in building 60, it was not addressed across all EMCS assets. Out-of-date antivirus software and the use of unsupported operating systems increase the risk of successful cyber attacks on the EMCS network. The National Security Agency publication, "Securing Assets within a Closed Industrial Control Systems Network Perimeter," October 1, 2015, recommends system administrators apply security patches and upgrades to remove known vulnerabilities before the vulnerabilities are exploited in a cyber attack. For example, the National Security Agency reported that unsupported Windows operating systems have well-known severe security flaws that cannot be fully removed. Therefore, the National Security Agency recommends that all computers in use on control system networks be upgraded to operating system versions that are supported and patched by the vendor.

~~(FOUO)~~ Further, 375th CES personnel did not disable EMCS communications ports and services not needed to support EMCS operations. The ICS Information Assurance Manager and EMCS administrators acknowledged that unnecessary EMCS network ports and services were not identified and disabled. The aforementioned National Security Agency publication describes the importance of port and services management. Specifically, the publication states that electronic cyber attacks often exploit flaws in vulnerable communication services and recommends disabling unused services or communication ports to eliminate associated attack vectors.

~~(S)~~ The three cybersecurity deficiencies identified in this notice of concern increased the risk of successful cyber attacks on EMCS. A successful cyber attack on the EMCS could allow adversaries direct access to control the environmental operations in building 1575 causing critical information technology equipment to overheat and fail. Without basic cybersecurity controls on the EMCS, critical DoD and Combatant Command missions depending on building 1575 could be compromised. For example, the failure of Global Decision Support System servers increases the risk of disruption or incapacitation of U.S. Transportation Command critical airlift and refueling missions.

(U) Suggested Actions

(U) We suggest the 375th CES:

- ~~(FOUO)~~ test all JCI computers for malware and vulnerabilities before connecting them to the EMCS network,
- ~~(FOUO)~~ update all EMCS computers with the most current antivirus software,
- ~~(FOUO)~~ upgrade all EMCS computers with supported operating systems, and

[2] (U) Any vulnerability, the exploitation of which will directly and immediately result in loss of Confidentiality, Availability, or Integrity.

(U) Notice of Concern (cont'd)

~~SECRET~~

- ~~(FOUO)~~ identify and disable all ports and services not needed to support EMCS operations.

(U) Please respond to these suggested actions or provide alternative actions taken within 10 calendar days of the issuance of this notice of concern. My points of contact for your responses are [redacted] and [redacted] This memorandum and management comments to the suggested actions will be included in the final audit report. Please contact me at (b) (6) (DSN (b) (6)) or (b) (6) with any questions.

Carol N. Gorman
Assistant Inspector General
Readiness and Cyber Operations

(U) CC:

(U) DIRECTOR OF CIVIL ENGINEERS, DEPUTY CHIEF OF STAFF FOR LOGISTICS ENGINEERING AND FORCE PROTECTION, HEADQUARTERS U.S. AIR FORCE

(U) DIRECTOR, AIR FORCE CIVIL ENGINEER CENTER

(U) Appendix C

(U) Scott Air Force Base 375th Civil Engineer Squadron Response to Notice of Concern

CLASSIFICATION: **UNCLASSIFIED/~~FOUO~~**

MEMORANDUM FOR DoD IG

FROM: 375 Civil Engineer Squadron

SUBJECT: Response to Notice of Concern

1. In response to your notice of concern memorandum dated 29 Oct 16, the 375 Civil Engineer Squadron (CES) will take the following action to address all of the specific observations you identified during the recent site visit:

a. Recommendation: Test all JCI Computers for malware and vulnerabilities before connecting them to the EMCS network.

ACTION: 375 CES instituted a local policy in coordination with Johnson Controls Inc. (JCI) that JCI will use only AF Standard Desktop configuration laptop computers for EMCS updates. Additionally, all software programs, upgrades, patches and modifications will be permitted onto the laptop and/or be introduced to the EMCS system after it is scanned by 375 CES IT Systems Administrator. The laptop(s) will remain in positive control of a federal employee of the Heating Ventilation and Air Conditioning shop (military or civilian member) or authorized designated representative at all times while in service or secured under lock and key. ECD - 1 Dec 16

b. Recommendation: Update all EMCS computers with the most current antivirus software.

ACTION: 375 CES IT Systems Administrator follows a regular schedule of antivirus software upgrades and installation. At the present time, all upgrades and patches occur at each individual terminal resulting in a natural gap in protection since the CE IT office is a 1 person shop. When the CE VLAN goes live, all antivirus upgrades and patches will be done electronically via the server drastically reducing the man hours required to keep the entire system protected. The IG observation was made in the midst of an effort to upgrade and patch all EMCS computers. ECD – Continual

c. Recommendation: Upgrade all EMCS computers with supported operating systems.

ACTION: 375 CES IT Systems Administrator follows a regular schedule of operating system conversion. At the present time, all conversion and upgrades occur at each individual terminal resulting in a natural gap since the CE IT office is a 1 person shop. When the CE VLAN goes live, all antivirus upgrades and patches will be done electronically via the server drastically reducing the man hours required to the entire system up to date with the required operating systems. The IG observation was made in the midst of an effort to convert all computers to the supported operating systems. ECD – 1 Jan 17

d. Recommendation: Identify and disable ports and services not needed to support EMCS operation.

ACTION: 375 CES IT Systems Administrator has scheduled to disable all ports and services not needed to support the EMCS operations in the coming weeks. ECD – 1 Jan 17

2. Thank you for taking the time to conduct this inspection of our Industrial Control Systems. We look forward to addressing your concerns. If you have any questions, my POC is [redacted]

//SIGNED--arm, 7Nov16//
ANDREW R. MYERS, Major, USAF, P.E.
Commander

CLASSIFICATION: **UNCLASSIFIED/~~FOUO~~**

(U) Appendix D

(U) Headquarters Air Force, Directorate of Civil Engineers Comments to Notice of Concern

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

MEMORANDUM FOR DOD OIG [redacted]

FROM: AF/A4C
1200 Air Force Pentagon
Washington, DC 20330-1030

SUBJECT: Response to Notice of Concern (NOC)

1. A4C acknowledges the findings in the subject NOC entitled Cybersecurity Vulnerabilities Identified During Audit of Control Systems Cybersecurity at Scott Air Force Base (Project No. D2016-D000RB-0149.000).

2. At the time of the inspection Air Force civil engineer units did not have adequate policy guidance and Industrial Control System (ICS) cybersecurity resources to adequately mitigate the vulnerabilities found in the specific ICS mentioned in the NOC. As part of an effort to update policy, A4C has in final draft an Air Force Guidance Memorandum (AFGM2016-32-06) intended to replace Engineering Technical Letter 11-1, *Civil Engineer Industrial Control System Information Assurance Compliance*, as well as implement the Risk Management Framework for civil engineer ICS.

3. To address the resourcing shortfall, A4C has already successfully secured a new funding line in the FY18-FY22 POM to provide full-time cybersecurity professionals at each base dedicated to managing the cybersecurity efforts for the civil engineer functional community, including conducting and maintaining accurate inventories, performing mission support analysis, managing and configuring ICS network enclaves, conducting self-assessments of security controls and performing cybersecurity maintenance and lifecycle management of civil-engineer-owned ICS.

4. The draft guidance memorandum outlines policy for civil engineer units to mitigate all of the vulnerabilities identified in the NOC. It is important to note, however, that the Operational Technology (OT) that makes up many of our ICS is based on hardware and software refresh rates on the order of decades. While policy may dictate the update of unsupported operating systems (OS), the cost to ICS could include not only the software itself, but also the wholesale replacement of hardware. This could prove to be an unsupportable cost burden that might force a risk management decision to maintain older OS in certain cases.

5. Please direct any questions or concerns to the A4C point of contact for industrial control system cybersecurity, [redacted]

OSHIBA.EDWIN.H.1180200211

EDWIN H. OSHIBA, SES
Deputy Director of Civil Engineers
DCS/Logistics, Engineering & Force Protection

(U) Glossary

(U) Anti-virus Software. Software products and technology used to detect and remove malicious code that that has infected the system.

(U) Audit Logs. Chronological record of information system activities, including records of system accesses and operations performed in a given period.

(U) Authorization to Operate. The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations, organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.

(U) Control System. Specialized systems and mechanisms that ensure installation infrastructure services (that is, electricity, fluids, gases, air, traffic, and people) are delivered when and where required to accomplish the mission.

(U) Cybersecurity Controls. Safeguards or countermeasures use in the prevention of damage to, protection of, and restoration of computers and electronic communication services, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

(U) Information Assurance Manager. Official responsible for the information assurance of a program, organization, system, or enclave.

(U) Malware. Software intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system.

(U) Overlay. A specification of security controls, control enhancements, supplemental guidance, and other supporting information intended to complement (and further refine) security control baselines.

(U) Patch. Additional pieces of code that have been developed to address specific problems or flaws in existing software.

(U) Platform Information Technology System. A collection of information technology hardware and software that is physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems, and that is structured by physical proximity or by function.

(U) Port. The entry or exit point from a computer for connecting communications or peripheral devices.

(U) Standalone Networks. Networks that are not connected to any other network and do not transmit, receive, route, or exchange information outside of the system's authorization boundary.

(U) Tier 1 Task Critical Assets. An asset of such extraordinary importance that the loss, incapacitation, or disruption could result in mission (or function) failure at the DoD, Military Department, combatant command, sub-unified command, Defense agency, or Defense infrastructure Sector Lead Agent levels.

(U) Vulnerability. Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

(U) Source of Classified Information

Source 1: (U) Air Force Tier 1 & 2 Critical Assets List 6-8-2016: SECRET
Declassification Date: February 15, 2021
Generated Date: June 6, 2016

Source 2: (U) Joint Mission Assurance Assessment: SECRET//NOFORN
Declassification Date: October 19, 2025
Generated Date: August 14, 2015

Source 3: ~~(FOUO)~~ 618th Air and Space Operation Center/Tanker Airlift Command Center Balanced Survivability Assessment Report: SECRET
Declassification Date: May 10, 2038
Generated Date: May 17, 2013

(U) Acronyms and Abbreviations

AFB	Air Force Base
AFCEC	Air Force Civil Engineer Center
CES	Civil Engineer Squadron
CMAFS	Cheyenne Mountain Air Force Station
EMCS	Energy Management Control System
HVAC	Heating, Ventilation, and Air Conditioning
IAM	Information Assurance Manager
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
NIST	National Institute of Standards and Technology
OMCS	Operational Management Control System
SP	Special Publication

~~SECRET~~

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/programs/whistleblower.

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

Congressional Liaison
congressional@dodig.mil; 703.604.8324

Media Contact
public.affairs@dodig.mil; 703.604.8324

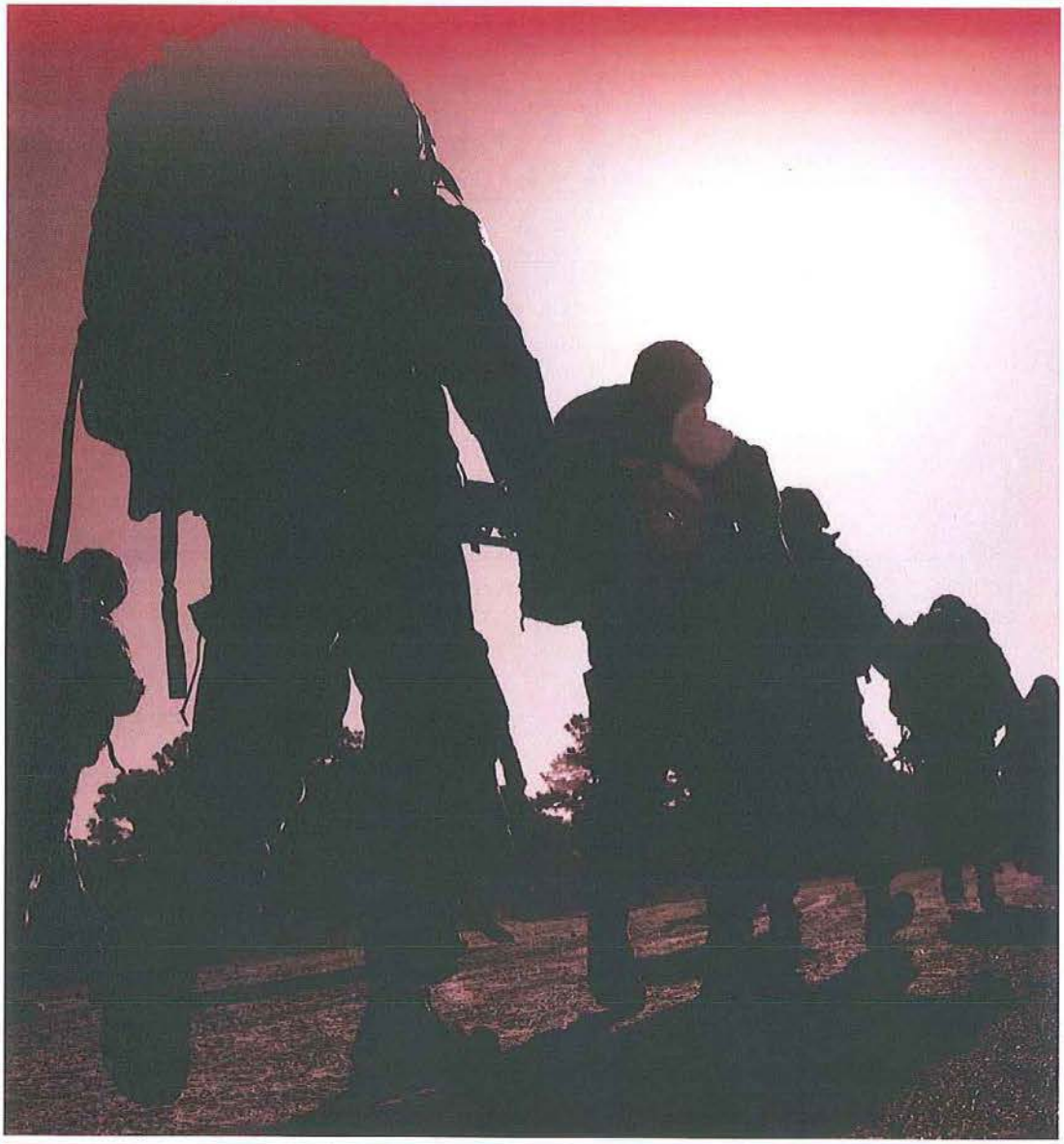
For Report Notifications
http://www.dodig.mil/pubs/email_update.cfm

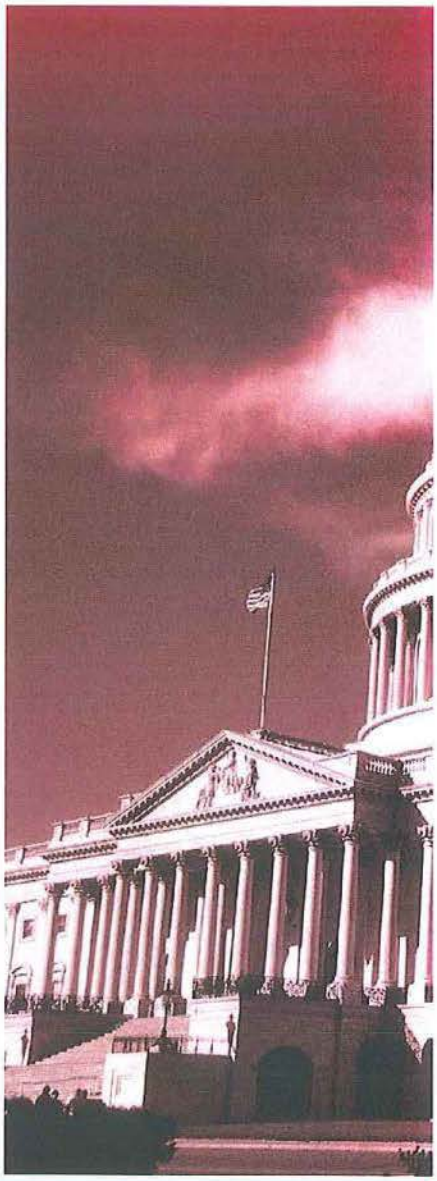
Twitter
twitter.com/DoD_IG

DoD Hotline
dodig.mil/hotline

~~SECRET~~

~~SECRET~~





DEPARTMENT OF DEFENSE | OFFICE OF INSPECTOR GENERAL

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

~~SECRET~~