Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems DODIG-2019-105

Audit / Published July 23, 2019

Publicly released: July 25, 2019

Objective

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

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

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

Background

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

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

Findings

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

- using multifactor authentication;
- enforcing the use of strong passwords;
- identifying network and system vulnerabilities;
- mitigating network and system vulnerabilities;
- protecting CUI stored on removable media;
- overseeing network and boundary protection services provided by a third-party company;
- documenting and tracking cybersecurity incidents;
- configuring user accounts to lock automatically after extended periods and unsuccessful logon attempts;
- implementing physical security controls;
- creating and reviewing system activity reports; and
- granting system access based on the user's assigned duties.

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

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

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

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

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

Recommendations

We recommend that the Director for Contract Policy and Oversight for the Defense Threat Reduction Agency revise the agency's process for monitoring security incidents verify that contractors took appropriate steps to identify, respond to, and report security incidents that involve DoD data. We also recommend that the Director review the performance of the contracting officer responsible for monitoring the security incident identified in this report and consider administrative action, as appropriate, for not ensuring that a contractor took actions to remove the classified information from its corporate network and the contractor's commercial cloud environment. Furthermore, we recommend that the Director for the Defense Counterintelligence and Security Agency (formerly known as the Defense Security

Service) assess and document the risk of leaving classified information unprotected in unclassified environments and, based on the assessment, develop and implement controls to protect the information.

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

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

- Revise its current policy related to assessing a contractor's ability to protect DoD information to require DoD Component contracting offices, as part of the Request for Proposal and source selection processes, and requiring activities, during the contract performance, to validate, at least annually, that contractors comply with security requirements for protecting CUI before contract award and throughout the contract's period of performance.
- Develop and implement policy requiring DoD Component contracting offices and requiring activities to maintain an accurate accounting of contractors that access, maintain, or develop controlled unclassified information as part of their contractual obligations.
- Revise its current policy to include language that would require DoD Component contracting offices to validate contractor compliance with minimum security requirements.

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

Management Comments and Our Response

The Principal Deputy Chief Information Officer, responding for the DoD Chief Information Officer, disagreed with the recommendations to require stronger passwords and lock accounts after 15 minutes of inactivity stating that those requirements were prohibited by 32 Code of Federal Regulation section 2002, "Controlled Unclassified Information" and contrary to Executive Order 13556, "Controlled Unclassified Information." However, we do not consider the 32 CFR section 2002 and Executive Order 13556 prohibitive in allowing the DoD to require contractors to implement more stringent requirements, when warranted. Therefore, the DoD Chief Information Officer should provide additional comments to clarify how the recommendations conflict with or are contrary to 32 Code of Federal Regulation

section 2002 and the Executive Order 13556, or how the DoD Chief Information Officer will implement the recommendations as stated.

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

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

The Defense Counterintelligence and Security Agency Executive Director agreed to include aspects of the recommendation in future incident responses and decisions, he did not state how the agency planned to.]. Therefore, the Executive Director should provide additional comments describing how the Defense Counterintelligence and Security Agency plans to assess that risk.

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

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

describing how the Corps of Engineers will verify that the contractor corrected the weaknesses.

The Deputy Assistant Secretary for the Navy (Research, Development, Test, and Evaluation), responding for the U.S. Navy Contracting Officer, acknowledged that the Navy was working with the Office of the Secretary of Defense to develop policy for ensuring contractor compliance with DFARS clause 252.204-7012. However, he did not address actions that the Naval Information Warfare Systems Command (formerly known as the Space and Naval Warfare Center) will take to ensure the contractor corrected identified weaknesses. Therefore, the Deputy Assistant Secretary should provide additional comments describing how the Naval Information Warfare Systems Command will verify that the contractor corrected those weaknesses.

The Principal Deputy Assistant Secretary of the Air Force (Acquisition, Technology, and Logistics), responding for the U.S. Air Force Contracting Officer, neither agreed nor disagreed with the recommendations and did not address actions that the Air Force will take to ensure the contractor corrected identified weaknesses. Therefore, the Principal Deputy Assistant Secretary should provide additional comments describing how the Air Force will verify that the contractor corrected those weaknesses.

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

This report is a result of Project No. D2018-D000CR-0171.000

Related Documents

DODIG-2019-105.PDF