Results in Brief

(U) Audit of Security Controls Over the Department of Defense's Global Command and Control System–Joint Information Technology System

March 18, 2020

(U) Objective

(U) The objective of this audit was to determine whether DoD combatant commands and Military Services implemented security controls over the Global Command and Control System–Joint (GCCS-J) to protect DoD data and information technology assets.

(U) Background

(U) The GCCS-J is an information technology system that provides critical information to the Commander in Chief, Secretary of Defense, National Military Command Center, combatant commanders, Joint Force commanders, and Service Component commanders to enable global and joint command and control operations. The GCCS-J provides users with a complete picture of operational environment across air, land, maritime, space, and cyberspace warfighting domains. The system allows users to plan, execute, and manage military operations into and across theaters, manage mission-specific information feeds, and gather battlefield data to provide commanders with an accurate status of air, space, land, and maritime units used for operations. GCCS-J capabilities include processing unmanned aerial vehicle video, targeting data, battlefield graphics, and air space control orders.

(U) GCCS-J critical sites are designated locations within the combatant commands and Military Services that provide information, data feeds, or other services critical to global and joint command and control operations in support of the National Military Command System. DoD Instruction 8510.01 requires all DoD information systems that receive, process, store, display, or transmit DoD information to be granted an authorization to operate after the system's security controls have been tested,

(U) Background (cont'd)

(U) evaluated, and approved. The Joint Staff appointed the Deputy Commander of the U.S. Strategic Command (USSTRATCOM) as the authorizing official for the GCCS-J "type" authorization to operate. A type authorization to operate allows a system to be installed and used at multiple sites if the site institutes the controls specified in the system security plan. At each site, the authorizing official is responsible for accepting the type authorization or updating the site authorization to operate based on specific control requirements at the site.

(U) There are three primary types of system security controls—common controls, system-specific controls, and hybrid controls. Common controls are security controls implemented at the organizational level that can be used by any information system that operates in the organizational environment, such as vulnerability management and physical access authorization controls. System-specific controls are security controls implemented at the system level that are not inherited by any other information system in the organizational environment, such as security categorization and least functionality controls. Hybrid controls are security controls that are in part a common control and a system-specific control, such as account management controls.

(U) Chairman of the Joint Chiefs of Staff Instruction (CJCSI), 6731.01C, "GCCS-J Security Policy," establishes roles and responsibilities for managing GCCS-J operations. The Instruction requires the Director for Operations, Joint Staff (J-3), and the Director for Command, Control, Communications, and Computers/Cyber, Joint Staff (J-6), to enforce the GCCS-J security requirements outlined in the Instruction. The Instruction also requires GCCS-J critical

Results in Brief

(U) Audit of Security Controls Over the Department of Defense's Global Command and Control System–Joint Information Technology System

(U) Background (cont'd)

(U) sites to have a GCCS-J authorizing official, program manager, information system security manager, or an information systems security officer as required.

(U) Finding

(U) We determined that cybersecurity officials at the seven GCCS-J critical sites we reviewed did not implement all required GCCS-J security controls. Specifically, of the 17 security controls we reviewed, cybersecurity officials did implement 9 controls. The nine security controls included six common controls, one system-specific control, and two hybrid controls. However, cybersecurity officials did not consistently implement the following eight controls:

- (U) common controls
  - (U) access control policy and procedures
  - (U) physical and environmental protection policy and procedures
  - (U) vulnerability management
  - (U) physical access authorization
  - (U) physical access control
- (U) system-specific controls
  - (U) least functionality
  - (U) security categorization
- (U) hybrid control
  - (U) account management

(U) Cybersecurity officials did not consistently implement these GCCS-J security controls because the critical site commanders did not appoint GCCS-J cybersecurity officials as required by CJCSI 6731.01C. The site cybersecurity officials at all seven critical sites stated that they thought

(U) the Defense Information Systems Agency was responsible for implementing security controls for the GCCS-J. In addition, the Joint Staff J-3 and J-6 did not ensure that the GCCS-J security policy was enforced at the GCCS-J sites.

~~(U//FOUO)~~ [redacted]

(U) Recommendations

(U) We recommend that the commanders at the GCCS-J critical sites:

- (U) appoint required personnel to implement the requirements in the GCCS-J type authorization to operate;
- (U) ensure the GCCS-J security controls are implemented; and
- (U) annually verify that the required GCCS-J security controls are implemented as required in the type authorization to operate and CJCSI 6731.01C.

(U) We also recommend that the Vice Director of the Joint Staff ensure that the Joint Staff J-6 and J-3 develop and implement a plan for enforcing the GCCS-J security requirements in CJCSI 6731.01C at each site that operates the GCCS-J.

Results in Brief

(U) Audit of Security Controls Over the Department of Defense's Global Command and Control System–Joint Information Technology System

(U) Management Comments and Our Response

~~(U//FOUO)~~ [redacted], Chief Information Officer, responding for the [redacted], agreed to implement GCCS-J security controls for vulnerability management, access management, and security categorization, and to establish an annual verification process for ensuring that the controls are implemented in accordance with the type authorization. The Director also provided verification that the required personnel were appointed to implement the GCCS-J security controls. However, the Director did not agree to implement physical access controls for the server room cabinets and did not detail how the [redacted] would ensure that unused or unnecessary ports are disabled. Therefore, the Director should provide additional comments describing how [redacted] will implement those controls.

~~(S)~~ [redacted]

Although the Chief of Staff agreed with the recommendation to conduct a GCCS-J security classification assessment, he did not state whether the assessment was actually conducted. Therefore, the Chief of Staff should provide additional comments on the final report to demonstrate that [redacted] officials completed a GCCS-J security classification assessment to ensure that all required GCCS-J security controls are implemented.

~~(U//FOUO)~~ [redacted], responding for the [redacted], stated that on approximately January 29, 2019, [redacted] was removed from the GCCS-J critical sites list by USSTRATCOM. Further, the Joint Staff Support Center provided documents to support that the GCCS-J was no longer operational at [redacted]. Therefore, all recommendations directed to the [redacted] in this report are closed.

~~(S)~~ [redacted]

~~(U//FOUO)~~ [redacted] agreed to appoint the required personnel to implement the GCCS-J security controls. He also agreed to implement GCCS-J security controls for vulnerability management, physical access, least functionality, and security categorization, and to establish an annual verification process for ensuring that the controls are implemented in accordance with the type authorization. However, the [redacted] did not agree to notify the [redacted] higher headquarters, as required, when its GCCS-J users no longer require system access, or maintain a list of authorized GCCS-J users. Therefore, we request that the Squadron Commander provide additional comments on the final report identifying how [redacted] will implement those controls.

Results in Brief

(U) Audit of Security Controls Over the Department of Defense's Global Command and Control System–Joint Information Technology System

(U) Management Comments (cont'd)

~~(U//FOUO)~~ The [redacted] to develop and implement a plan for enforcing the GCCS-J security requirements and stated that the enforcement requirements are included in a draft interim policy memorandum, "GCCS-J Cybersecurity Instructions and Best Practices."

~~(U//FOUO)~~ The [redacted] and the [redacted] did not respond to the recommendations in the report; therefore, we request that the Commanders provide comments on the final report.

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

(U) Recommendations Table

~~U//FOUO~~ Management	Recommendations Unresolved	Recommendations Resolved	Recommendations Closed
[redacted]	1.a, 1.b, 1.c, 1.d, 1.e, 1.f, 1.g, 1.h, and 1.i.	None	None
[redacted]	2.f, 2.g, and 2.h	2.b, 2.c, 2.d, 2.e, 2.i, and 2.j	2.a
[redacted]	3.i	3.a, 3.b, 3.c, 3.d, 3.e, 3.f, 3.g, 3.h, and 3.j	None
[redacted]	4.a, 4.b, 4.c, 4.d, 4.e, 4.f, 4.g, and 4.h	None	None
[redacted]	None	None	5.a, 5.b, 5.c, 5.d, 5.e, 5.f, 5.g, 5.h, 5.i, and 5.j
[redacted]	None	6.a, 6.b, 6.c, 6.d, 6.e, 6.f, 6.g, 6.h, and 6.i	None
[redacted]	7.e	7.a, 7.b, 7.c, 7.d, 7.f, 7.g, 7.h, 7.i, and 7.j	None
[redacted]	None	8	None ~~U//FOUO~~

Please provide Management Comments by April 18, 2020.

NOTE: The following categories are used to describe agency management's comments to individual recommendations:

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