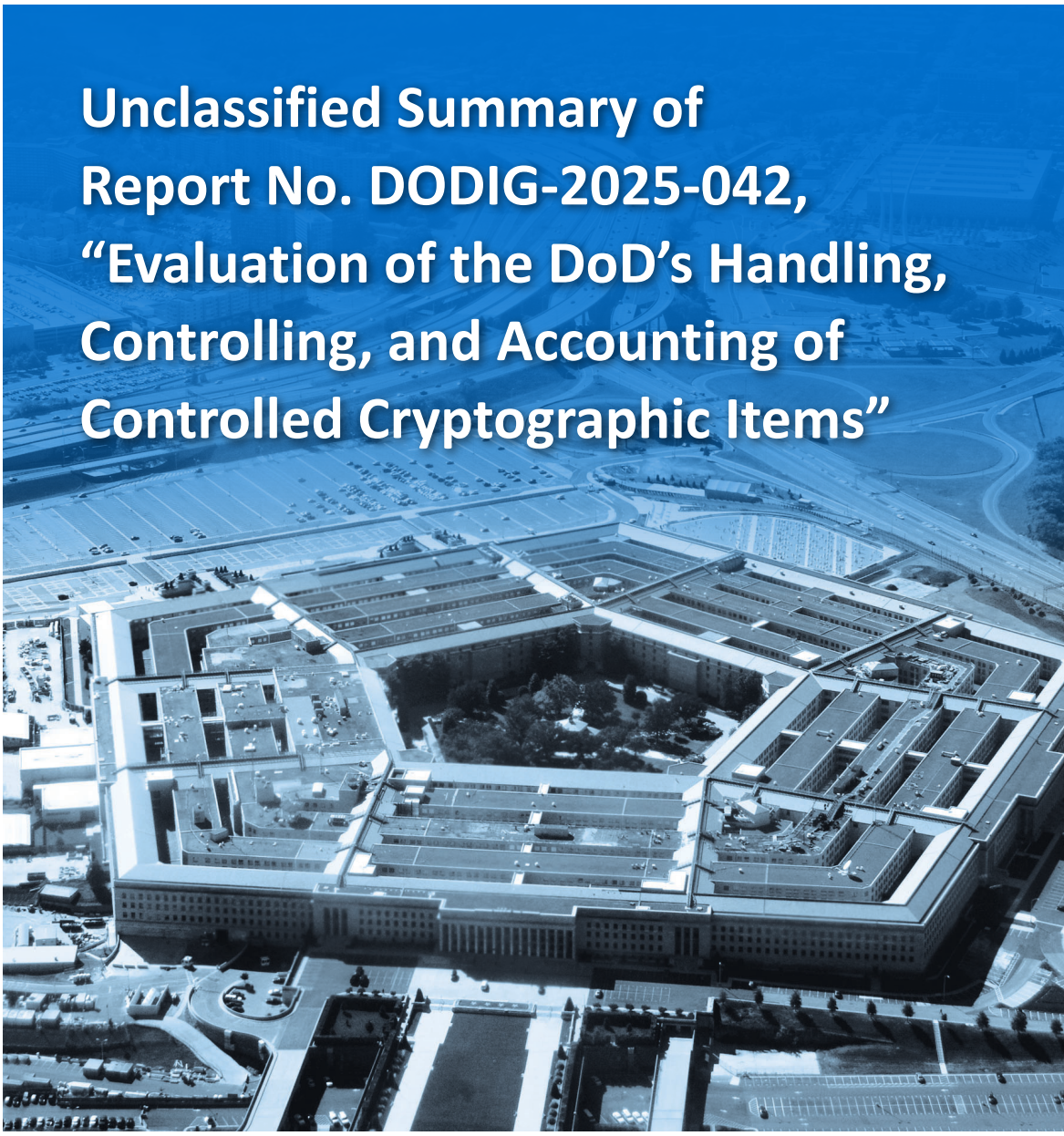
INSPECTOR GENERAL

U.S. Department of Defense

NOVEMBER 19, 2024

Unclassified Summary of Report No. DODIG-2025-042, "Evaluation of the DoD's Handling, Controlling, and Accounting of Controlled Cryptographic Items"



INDEPENDENCE ★ INTEGRITY ★ EXCELLENCE ★ TRANSPARENCY

On November 19, 2024, the DoD Office of Inspector General issued Evaluation report DODIG-2024-042, "Evaluation of the DoD's Handling, Controlling, and Accounting of Controlled Cryptographic Items." This original evaluation contains a substantial amount of what was determined by the stakeholders to be controlled unclassified information and, therefore, we are unable to release the full report or a redacted version of the report. In the interest of transparency, we prepared this summary report to release the unclassified finding identified during the evaluation.

Objective

The objective of this evaluation was to determine the efficiency and effectiveness of the DoD's handling, controlling, and accounting of controlled cryptographic items (CCI). We reviewed the policies for the seven DoD Central Offices of Record (CORs). We conducted additional interviews and observations at three of the seven CORs to determine implementation of the COR policies.

Background

CCI are a subset of communications security (COMSEC) material that provide critical secure communications for the DoD and the Federal government. The Committee of National Security Systems (CNSS), a committee under the President's Critical Infrastructure Protection Board, governs requirements for COMSEC material. CNSS instructions define CCI as secure telecommunications, information systems, or associated cryptographic components that are unclassified and handled through either the communications security material control system, an equivalent material control system, or a combination of the two for accounting and visibility.

CNSS Instructions 4001, 4003, and 4005 provide minimum communication security guidance for all national security systems used by DoD Components. The DoD published implementing Instruction 8523.01, which is specific to managing communication networks in the DoD. CNSS Instruction 4005 provides guidance for managing CCI, stating that a National Manager for the National Security Telecommunications and Information Systems Security should maintain a National Office of Record to provide oversight and guidance to Department and agency CORs. This National Office of Record provides guidance to a total of 22 CORs across the U.S. Government—7 of which are within the DoD.

Scope and Methodology

We focused our evaluation on the 7 of 22 CORs that are DoD Components. We reviewed CCI hardware accounting data and evaluated CCI processes and procedures, as well as laws and policies. In addition, we reviewed CCI program implementation by each of the seven DoD Components. We also reviewed organization communication and coordination regarding incident reporting.

We issued a request for information to gather data on COMSEC accounts, CCI inventories, and CCI incident reporting from the evaluated DoD departments and agencies. We also requested information from the Joint Staff Command, Control, Communications, and Computers/Cyber and DoD Chief Information Officer regarding CCI policy implementation. We compared the data provided by stakeholders with Federal and DoD policies and guidance on CCI. We interviewed personnel from all seven DoD Components to understand how each organization conducted oversight of CCI.

We selected three of the seven DoD CORs for in-depth site visits. We did not conduct site visits at the four remaining DoD CORs. In February and March 2024, we conducted site visits at the U.S. Army Garrison Humphreys, South Korea; Marine Corps Base Hawaii; Schofield Barracks, Hawaii; Joint Base Pearl Harbor–Hickam Wahiawa Annex, Hawaii; and Joint Base Pearl Harbor–Hickam, Hawaii. We physically observed implementation of Federal and Department requirements, including CNSS Instruction 4001, "Controlled Cryptographic Items"; CNSS Instruction 4003, "Reporting and Evaluating Communications Security (COMSEC) Incidents"; CNSS Instruction 4005, "Safeguarding Communications Security Facilities and Materials"; and DoD Instruction 8523.01, "Communications Security." Furthermore, we held interviews to understand CCI oversight roles and responsibilities, particularly in executing DoD-wide policy and guidance for handling, controlling, and accounting for CCI. We performed in-briefs with leadership and functional area representatives, held meetings with personnel from appropriate functional areas, and toured relevant facilities to observe CCI oversight processes.

Findings, Recommendations, Management Comments, and Our Response

The seven DoD CORs complied with Federal and Department instructions for the handling, controlling, and accounting of CCI. Specifically, the CORs at the Defense Intelligence Agency, National Geospatial-Intelligence Agency, National Reconnaissance Office, National Security Agency/Central Security Service, and the Departments of the Army, Navy, and Air Force implemented CCI oversight and operations protocols that aligned with the COMSEC mission of their respective organizations, in accordance with CNSS Instructions 4001, 4003, 4005, and DoD Instruction 8523.01.

We conducted a policy review of all seven CORs to determine implementation of the CNSS and DoD instructions' requirements into their respective policies. Additionally, we interviewed personnel from all seven CORs to understand implementation of CNSS and DoD instruction requirements into the CORs' CCI oversight and operations policies. To further determine implementation and adherence to CCI oversight and operations below the COR level, we interviewed personnel at and observed CCI storage and shipping locations in the U.S. Indo-Pacific Command area of operations with organizations that fell under three separate CORs: the Departments of the Army and Navy and the DIA.

We coordinated a discussion draft of this report with officials from the Defense Intelligence Agency, National Geospatial-Intelligence Agency, National Reconnaissance Office, National Security Agency/Central Security Service, and the Departments of the Army, Navy, and Air Force. The officials concurred with our report and provided technical comments, which we incorporated as appropriate.

Based on the findings of our evaluation, we did not make any recommendations.

This original evaluation contains a substantial amount of what was determined by the CORs to be controlled unclassified information and, therefore, we are unable to release the full report or a redacted version of the report. To file a Freedom of Information Act request, please submit a request to FOIA.gov.


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

Whistleblower Protection
U.S. Department of Defense

Whistleblower Protection safeguards DoD employees against retaliation for protected disclosures that expose possible fraud, waste, and abuse in Government programs. For more information, please visit the Whistleblower webpage at www.dodig.mil/Components/Administrative-Investigations/Whistleblower-Reprisal-Investigations/Whistleblower-Reprisal/ or contact the Whistleblower Protection Coordinator at Whistleblowerprotectioncoordinator@dodig.mil

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

Congressional Liaison
703.604.8324

Media Contact
public.affairs@dodig.mil; 703.604.8324

www.twitter.com/DoD_IG

LinkedIn
www.linkedin.com/company/dod-inspector-general/

DoD Hotline
www.dodig.mil/hotline

DEPARTMENT OF DEFENSE | OFFICE OF INSPECTOR GENERAL

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