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

August 14, 2019
Ref: DODOIG-2019-000614

SENT VIA EMAIL TO: john@greenewald.com
Mr. John R. Greenewald
The Black Vault
27305 W. Live Oak Road, Suite 1203
Castaic, CA 91384

Dear Mr. Greenewald:

This responds to your Freedom of Information Act (FOIA) request for a copy of Report DODIG-2019-054, "Evaluation of Special Access Programs Industrial Security Program." We received your request on April 22, 2019, and assigned it case number DODOIG-2019-000614.

The Office of the Deputy Inspector General for Evaluations conducted a search and located the report that is responsive to your request. Upon coordination with the Evaluations component, the Office of the Secretary of Defense, and the original classification authority, we determined that the report is appropriate for release in part pursuant to 5 U.S.C. § 552 (b)(1), which applies to information that is currently and properly classified in accordance with Sections 1.1, 1.2, 1.4, and 1.7(e) of Executive Order 13526. This information, if released, could be expected to cause serious damage to the national security of the United States.

If you consider this an adverse determination, you may submit an appeal. Your appeal, if any, must be postmarked within 90 days of the date of this letter, clearly identify the determination that you would like to appeal, and reference to the FOIA case number above. Send your appeal to the Department of Defense, Office of Inspector General, ATTN: FOIA Appellate Authority, Suite 10B24, 4800 Mark Center Drive, Alexandria, VA 22350-1500, or via facsimile to 571-372-7498. For more information on appellate matters and administrative appeal procedures, please refer to 32 C.F.R. Sec. 286.9(e) and 286.11(a).

You may contact our FOIA Public Liaison at 703-604-9785, or FOIAPublicLiaison@dodig.mil, for any further assistance with your request. Additionally, you may contact the Office of Government Information Services (OGIS) at the National Archives and Records Administration to inquire about the FOIA mediation services they offer. The contact information for OGIS is as follows: Office of Government Information Services, National Archives and Records Administration, 8601 Adelphi Road-OGIS, College Park, Maryland 20740-6001, e-mail at ogis@nara.gov; telephone at 202-741-5770; toll free at 1-877-684-6448; or facsimile at 202-741-5769. However, OGIS does not have the authority to mediate requests made under the Privacy Act of 1974 (request to access one's own records).

August 14, 2019
Ref: DODOIG-2019-000614

If you have any questions regarding this matter, please contact Frederick Nuss at 703-604-9604 or via email at foiarequests@dodig.mil.

Sincerely,

Searle Slutzkin
Division Chief
FOIA, Privacy and Civil Liberties Office

Enclosure(s):
As stated

(U) Introduction

(U) Objective

(U) Our objective was to determine if special access program (SAP) industrial security inspections conducted by DoD Components are effectively ensuring the protection and security of defense contractor facilities, information, and technology.

(U) Background

[redacted]

(U) The Defense Security Service (DSS) provides the Military Services, Defense agencies, federal agencies, and cleared contractor facilities with security support services. The Under Secretary of Defense for Intelligence provides authority, direction, and control over DSS. However, the DSS Director is relieved of this oversight function when a carve-out provision is approved by the Secretary of Defense or the Deputy Secretary of Defense. According to DoD Directive 5205.07 a carve-out is defined as, "A provision approved by the Secretary or Deputy Secretary of Defense that relieves DSS of its National Security Program obligation to perform industrial security oversight functions for a DoD SAP."[1] Therefore, we focused our evaluation efforts on reviewing DoD Components' SAPs that are carved out from DSS oversight.

[redacted]

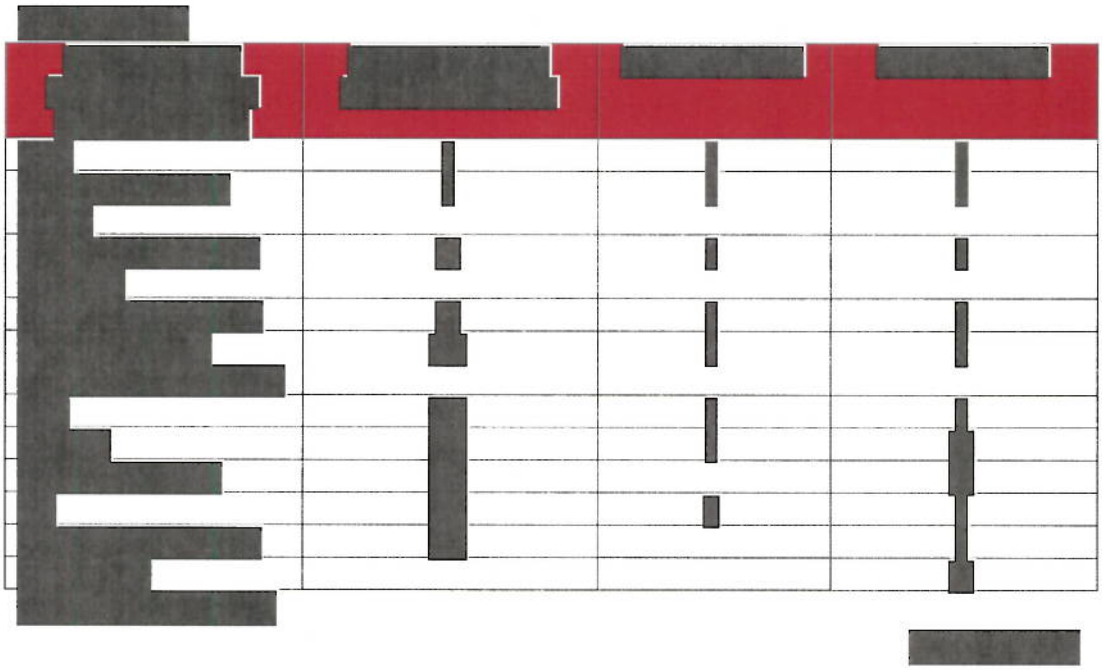
(U) To assess the contractor SAP security controls, we used the Security Compliance Inspection Template, dated November 14, 2017, required by DoD Manual 5205.07, Volume 1. See Appendix A for more information on how we selected our non-statistical sample of site visits. Table 1 below includes information organized by the specific DoD Component responsible for SAP security oversight, including the total number of

[1] (U) DoD Directive 5205.07, "Special Access Program (SAP) Policy, " July 1, 2010

[redacted]

cleared defense contractors, the carve-out status of the cleared defense contractor, and the total number of facilities we visited during our fieldwork.

(U) NUMBER OF CLEARED DEFENSE CONTRACTORS BY COMPONENT RESPONSIBLE FOR SAP SECURITY OVERSIGHT



[redacted]

(U) See Appendix A for the scope and methodology of this report and prior evaluation coverage. See Appendix B for our response to the questions from the DoD SAPCO Director. See Appendix C for the identification of best practices we identified that can potentially be applied on a larger scale to industry and government.

(U) Criteria

(U) There are several DoD publications that establish policy for the oversight of SAPs and SAP security.

(U) DoD Directive 5205.07 contains policy and responsibilities for the oversight and management of all DoD SAPs. The SAP Oversight Committee is responsible for advising and assisting the Secretary of Defense and Deputy Secretary of Defense with governance, management, and oversight of DoD SAPs. DoD SAPCO is the primary liaison to executive branch agencies and the Congress on all SAP issues.[2]

(U) DoD Instruction 5205.11 establishes and implements policy, assigns responsibilities, as well as updates, and prescribes procedures for the management, administration, and oversight of all DoD SAPs. [3]

(U) DoD Manual 5205.07, Volume 1 assigns responsibilities and describes the general procedures for DoD SAP security.[4]

(U) DoD Manual 5205.07, Volume 2 assigns responsibilities and provides procedures for personnel security of SAPs.[5]

(U) DoD Manual 5205.07, Volume 3 assigns responsibilities and provides procedures for physical security of DoD SAPs.[6]

(U) DoD Joint SAP Implementation Guide (JSIG), April 2016, provides standardized cybersecurity and information assurance policy, procedures, and implementation guidance for use in the management of all networks, systems, and components at all classification levels under the purview of the cognizant SAP authorizing official.

---

[2] (U) DoD Directive 5205.07, "Special Access Program (SAP) Policy, " July 1, 2010

[3] (U) DoD Instruction 5205.11, "Management, Administration, and Oversight of DoD Special Access Programs (SAPs)," February 6, 2013

[4] (U) DoD Manual 5205.07, Volume 1, "Special Access Program (SAP) Security Manual: General Procedures," June 18, 2015 (Incorporating Change 1, Effective February 12, 2018)

[5] (U) DoD Manual 5205.07, Volume 2, "Special Access Program (SAP) Security Manual: Personnel Security," November 24, 2015 (Incorporating Change 1, Effective February 12, 2018)

[6] (U) DoD Manual 5205.07, Volume 3, "Special Access Program (SAP) Security Manual: Physical Security," April 23, 2015 (Incorporating Change 2, Effective February 12, 2018)

[redacted]

(U) National Counterintelligence and Security Center, "Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities," Version 1.4, September 28, 2017, provides physical and technical specifications and best practices to comply with the intelligence community standards for sensitive compartmented information facilities.

(U) Review of Internal Controls

([redacted]) DoD Instruction 5010.40, "Managers' Internal Control Program Procedures," May 30, 2013, 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. [redacted] We will provide a copy of the final report to the senior official responsible for internal controls in the DoD SAPCO.

(U) Appendix A

(U) Scope and Methodology

(U) We conducted this evaluation from October 2017 through December 2018 in accordance with the Council of the Inspectors General on Integrity and Efficiency Quality Standards for Inspection and Evaluation, January 2012. Those standards require that we plan and perform the evaluation to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our evaluation objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our evaluation objectives.

(U) We performed site visits and interviewed DoD personnel at the following locations:

- (U) DoD SAPCO, Pentagon, Washington, D.C.
- (U) Air Force Office of Special Investigations, Joint Base Anacostia-Bolling, Washington, D.C.
- (U) DSS, Marine Corps Base, Quantico, Virginia

(U) We performed site visits and interviewed DoD contractors' personnel at the following locations:

[22] 

[23] (U) Our definition of a small to medium size contractor was subjective. One medium size contractor we selected is foreign-owned.

(U) To assess the DoD contractor compliance with SAP security controls, we used the Security Compliance Inspection Template, dated November 14, 2017, required by DoD Manual 5205.07, Volume 1. We reviewed the core compliance inspection items, including mandatory core functional areas. Specifically, we reviewed top secret and data and materials accountability, security education training and awareness, personnel security, security management and oversight, cyber security, and physical security checklist items. We also reviewed contracting items.[25] We did not review special emphasis items due to time constraints. We reviewed applicable policies and guidance, including DoD Directive 5205.07; DoD Instruction 5205.11; DoD Manual 5205.07, Volumes 1-3; the JSIG; and the National Counterintelligence and Security Center,

[25] (U) For example, we determined whether a subcontractor has the required facility clearance, if applicable.

"Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities," Version 1.4, September 28, 2017.

(U) We also reviewed SAP security documentation, including contractor SAP security SOPs, position appointment letters, authorization to operate letters, security authorization documentation, security self-inspections, operations security plans, co-utilization agreements, memorandums of agreement and understanding, intrusion detection system records, fixed facility checklists, facility accreditation letters, emergency action plans, annual SAP security awareness briefings, indoctrination briefings, program-specific indoctrination briefings, SAP refresher training records, and personnel security records.

(U) Use of Computer-Processed Data

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

(U) Prior Coverage

(U) No prior coverage has been conducted on the SAP industrial security programs in the last five years.