Results in Brief

Audit of Access Controls in the Defense Logistics Agency's Commercial and Government Entity Code Program

September 30, 2019

Objective

~~(FOUO)~~ The objective of this audit was to determine whether the Defense Logistics Agency's (DLA) controls governing the Commercial and Government Entity (CAGE) code process are adequate and effective in:

- issuing CAGE codes to contractors;
- ~~(FOUO)~~ allowing contractors to update CAGE code information, [redacted] and
- managing contractor access to DLA systems.

An adequate control is a control that is designed to achieve a specific objective, such as requiring a password to access a system. An effective control is an adequate control that operates as designed. For example, an access control would be effective if it limited access to only approved users.

Background

The CAGE code is a unique five-character identifier assigned to contractors located in the United States and its territories to identify a commercial or government entity. Contractor representatives with CAGE codes can request access to the following DLA systems and programs:

- the DLA Internet Bid Board System (DIBBS), for submitting secure quotes or bids for DLA contracts;

Background (cont'd)

- the Collaboration Folders (C-Folders) application, for accessing and downloading technical data, including export-controlled data (unclassified military critical technical data that must be protected from public disclosure), to develop quotes or bids placed in DIBBS; and
- the Joint Certification Program (JCP), required for accessing the unclassified export-controlled data within the C-Folders.

Federal Information Processing Standards Publication 200 (FIPS Publication 200) identifies the minimum security requirements for information and information systems of the Government. DoD Directive 5230.25 states that if a contractor needs access to export-controlled data to bid or perform on a contract the contractor must describe why it needs the data in enough detail for the DoD to evaluate whether the request for data is related to a legitimate business purpose.

Findings

We determined that DLA Program Offices did not have adequate and effective controls to govern the CAGE code process, as required by DLA standard operating procedures and FIPS Publication 200.

~~(FOUO)~~ Specifically, the CAGE Code Program Office did not have adequate controls to identify and authenticate users when issuing CAGE codes to contractors or allowing the contractors to update CAGE code information, [redacted] The CAGE Code Program Office also issued and updated CAGE codes without determining whether the contractor [redacted] This occurred because DLA personnel relied on controls in the General Services Administration's System for Award Management (SAM) to identify and authenticate contractors.[1] However, the DLA standard operating procedure

[1] According to the Office of Defense Pricing and Contracting personnel, within the DoD the Office of Defense Pricing and Contracting can propose changes to SAM that are then reviewed and approved by a board comprised of representatives from other Federal agencies.

Results in Brief

Audit of Access Controls in the Defense Logistics Agency's Commercial and Government Entity Code Program

Findings (cont'd)

~~(FOUO)~~ requires the DLA, not the General Services Administration, to validate the contractor's [redacted] and prevent potential counterfeit [redacted] from obtaining CAGE codes. Also, according to a DLA official, the DLA does not [redacted] contractors requesting or updating a CAGE code. Furthermore, the DLA relied on notifications [redacted] Federal organizations, and not all Federal sources.

~~(FOUO-LES)~~ In addition, the DIBBS Program Office did not implement identification and authentication controls that limited access to DIBBS to authorized contractor representatives, allowing unauthorized representatives to submit quotes and bids on DLA solicitations. [redacted]

~~(FOUO-LES)~~ As a result, unauthorized contractors— [redacted] — received DLA contracts. According to the DLA, it granted access to DIBBS [redacted] As of September 2018, the DLA stated that it spent over $12.9 million to look for nonconforming parts. [redacted] When the

~~(FOUO-LES)~~ DLA tests an NSN and determines that the NSN is nonconforming, the DLA categorizes all of the parts associated with that NSN, and supplied by the same contractor, as nonconforming. The DLA disposed of the individual parts associated with these NSNs.

~~(FOUO-LES)~~ We also found that DLA Program Offices did not have adequate and effective controls governing the export-controlled data that are contained in the C-Folders. Specifically, the DLA JCP and C-Folders Program Office did not limit access to export-controlled data, as required by DoD Directive 5230.25 and DoD Form 2345 instructions. The DLA JCP Office approved contractor requests for access to export-controlled data without requiring that the contractor provide a detailed and specific rationale for requesting access. [redacted]

~~(FOUO-LES)~~ This occurred because before [redacted], the DLA did not train JCP personnel to ensure that the contractor's rationale for access to export-controlled data was detailed and specific. DoD Directive 5230.25 and DoD Form 2345 instructions require the contractor to provide a detailed and specific rationale. The new training, provided after [redacted], instructed the JCP personnel on the required level of detail. [redacted] DLA officials also stated that DoD Directive 5230.25 does not provide the DLA adequate authority to [redacted] in the C-Folders.

Results in Brief

Audit of Access Controls in the Defense Logistics Agency's Commercial and Government Entity Code Program

Findings (cont'd)

~~(FOUO-LES)~~ [redacted] export-controlled data allowed unauthorized contractors to view, download, and share unclassified military technical data with unauthorized parties. Unauthorized contractors could use these data to replicate military equipment or technology for their own improper purposes. For example, according to DoD Directive 5230.25, access to these data could make a significant contribution to the military potential of another country and prove detrimental to the security of the United States.

Recommendations

~~(FOUO)~~ We recommend that the Defense Logistics Agency Director of Information Operations (J6) conduct a comprehensive review of the internal controls for systems associated with the CAGE code process. Specifically, the Director should ensure that those responsible for issuing and updating CAGE codes comply with DLA procedures and meet the minimum identification and authentication requirements prescribed by FIPS Publication 200. The Director should also work with the Office of Defense Pricing and Contracting to propose changes to SAM regarding the information that feeds from SAM into the CAGE code process and information contained in SAM's list of counterfeit [redacted] Additionally, the Director should evaluate the new controls to validate that only authorized contractor representatives can access the DIBBS. Furthermore, the Director should determine whether the DLA can apply the recommendations for the CAGE code process to the North Atlantic Treaty Organization CAGE code program.

~~(FOUO-LES)~~ We also recommend that the Director retrain JCP approvers on the level of detail required by DoD Directive 5230.25, design and implement controls to limit contractor access to [redacted] in the C-Folders relevant to the reason contractors provided in the request form, and train Information Operations personnel on how to protect [redacted]. [redacted] The Director should also coordinate with the Offices of the Under Secretaries of Defense for Readiness and Engineering, Acquisition and Sustainment, and Policy to determine whether DoD regulations, guidance, or policy give the DLA the authority to limit access [redacted] and, if necessary, request these Offices make the appropriate revisions to the policy to grant the DLA authority to limit access [redacted].

Management Comments and Our Response

~~(FOUO)~~ The DLA Information Operations Acting Director and the DLA Logistics Operations Deputy Director agreed with our findings and recommendations. Specifically, the Directors agreed to:

- implement a business process change in which new and update CAGE code requests are manually reviewed to verify that only legitimate contractors and representatives receive or update a CAGE code;
- ~~(FOUO)~~ [redacted]
- ~~(FOUO)~~ work with [redacted] discuss processes associated with SAM and CAGE and propose changes to SAM, as applicable;

Results in Brief

Audit of Access Controls in the Defense Logistics Agency's Commercial and Government Entity Code Program

Comments (cont'd)

- implement a mechanism to control access to DIBBS and evaluate the results of the new control;
- determine whether the DLA can apply the recommendations for the CAGE code process to the North Atlantic Treaty Organization CAGE code process and share the recommendations with the North Atlantic Treaty Organization Allied Committee for consideration;
- retrain JCP approvers and implement a quality control program;
- ~~(FOUO)~~ coordinate with [redacted] request that the DLA be given authority to limit access to export-controlled data;
- ~~(FOUO)~~ [redacted]
- train personnel on how to protect export-controlled data; and
- ~~(FOUO)~~ [redacted]

Management comments addressed the specifics of the recommendations. Therefore, all recommendations are resolved and three recommendations have been closed. The six recommendations not closed will remain open until we review the specific actions taken and the associated documentation.

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

Recommendations Table

Management	Recommendations Unresolved	Recommendations Resolved	Recommendations Closed
Defense Logistics Agency Director of Information Operations (J6)	None	A.1.a, A.1.b, B.1.a, B.1.b, B.1.c, B.1.d	A.1.c, A.1.d, B.1.e

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.