DETERMINATION OF THE DIRECTOR OF ADMINISTRATION

I have determined that the following information is exempt from disclosure under Exemption 3 of the Freedom of Information Act (5 U.S.C. § 552(b)(3)) because it meets the requirements for exemption under 10 U.S.C. § 130e:

The Department of Defense Activity Address Directory Database.

Date: 12·18·14

Michael L. Rhodes
Director of Administration

STATEMENT OF THE BASIS FOR THE DETERMINATION BY THE DIRECTOR OF ADMINISTRATION

In accordance with 10 U.S.C. § 130e, I reviewed the information provided to me by the Defense Logistics Agency concerning the Department of Defense Activity Address Directory (DoDAAD) database as a single authoritative source for the Department of Defense (DoD) business enterprise architecture and determined that it qualifies as DoD critical infrastructure security information (CISI). As defined by 10 U.S.C. § 130e, CISI includes:

> "…sensitive but unclassified information that, if disclosed, would reveal vulnerabilities in Department of Defense critical infrastructure that, if exploited, would likely result in the significant disruption, destruction, or damage of or to Department of Defense operations, property, or facilities, including information regarding the securing and safeguarding of explosives, hazardous chemicals, or pipelines, related to critical infrastructure or protected systems owned or operated by or on behalf of the Department of Defense, including vulnerability assessments prepared by or on behalf of the Department of Defense, explosives safety information (including storage and handling), and other site-specific information on or relating to installation security."

The DoDAAD meets this definition of CISI because it is comprised of both Department of Defense Activity Address Code (DoDAAC) and Routing Identifier Code (RIC) identifiers in an interactive relational database serving as a single authoritative source of identification, routing, and address information for authorized users, including Military Components and Agencies, participating Federal Agencies, authorized contractors, and authorized special program activities such as state and local governments (DLM 4000.25 Volume 6, December 19, 2013). DoDAAD supports business application systems data and interoperability requirements, including (but not limited to) supply chain, materiel procurement, and acquisition systems. Each activity that requisitions, contracts for, receives, has custody of, issues, or ships DoD assets, or funds/pays bills for materials and/or services is identified by a DoDAAC (six-position alphanumeric code).

DoDAACs are used in a myriad of business systems spanning the entirety of the DoD's business enterprise architecture, including acquisition, procurement, contracting, requisitioning, shipping, billing, pay, maintenance, installations management, human resources, energy resources, and the accountability and requisition of ordnance, ammunition, and perishables in logistics systems across the DoD. DoDAACs are also used for business operations involving the accountability of property and facilities, as well as for hazardous material management. Access to the DoDAAD allows access to these DoDAACs. When coupled with access to other unclassified logistic systems, users are provided with multiple data points which, when combined, disclose location of materials and operational status and plans. If the DoDAAD is released it would reveal vulnerabilities in Department of Defense critical infrastructure that, if exploited, would likely result in the significant disruption, destruction, or damage of or to DoD operations, property, or facilities related to critical infrastructure or protected systems owned or operated by or on behalf of the DoD.

The contents of the DoDAAD are sensitive for a number of reasons:

- DoDAACs are created to support sensitive operations and to facilitate the business process associated with them.

- DoDAACs for the following locations include names of employees and Service members as well as duty station addresses for:
    a. Department of Defense installations and ports that are outside the contiguous United States (OCONUS)
    b. Deployed units and activities performing real world contingency operations or exercises from both contiguous United States (CONUS) and OCONUS bases
    c. Ships afloat
    d. Ships still in CONUS ports but scheduled to go afloat
    e. Ships still in OCONUS ports but scheduled to go afloat
    f. Embassies
    g. War Reserve Equipment sets pre-positioned OCONUS

If an adversary had the DoDAAD they could determine the issuance of orders; the movement of specially qualified personnel to units and the installation of special capabilities, as well as the conduct of activities in a way that will reveal intensification of preparations before initiating operations. From this information, the adversary could identify very sensitive DoD activities including clandestine locations of DoD activities, force structure, and even troop movement.

In addition, a DoDAAC could be used in an unauthorized way whereby the internal controls of the Agency can be circumvented and appropriations obligated without the proper authority being involved in the process. A DoDAAC is very much like a credit card number which, in the wrong hands, can be used to spend money without the rightful "owner" of the code (i.e., the entity with authority to use the code) being aware that the Agency's appropriations are being spent. Individuals have been prosecuted who have used a DoDAAC to purchase items (i.e., televisions) for personal gain. Therefore, effective management, control, and use of DoDAACs by all DoD Components is critical to ensure DoD fiscal responsibility.

Moreover, the public interest in disclosure of the DoDAAD is minimal. FOIA requests for the DoDAAD are made by commercial entities with commercial interests. Therefore, the public interest consideration in the disclosure of this information does not outweigh preventing the disclosure of the information.