## DETERMINATION OF THE DIRECTOR OF ADMINISTRATION

Under the authority delegated to me by the Secretary of Defense, 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:

> Any and all data regarding Information Technology (IT) systems that store, process or transmit Department of Defense Special Access Programs (SAP) data.

Date: 6.19.2018

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 information regarding Department of Defense (DoD) Special Access Programs (SAP) Information Technology (IT) systems. I have determined that this information qualifies as DoD critical infrastructure security information as defined by 10 U.S.C. § 130e(f) because it concerns the protection, storage, processing, and transmittal of the most sensitive data in the Department. Because of the extremely sensitive nature of SAP data, the details of these systems and the organizations that develop, operate, and maintain them must be protected to ensure adequate operational security.

This information includes but is not limited to: system requirements, system configurations, specific hardware technologies and configurations used, specific software technologies and configurations used, source code, supplier information, supply chain management information, configuration control processes and procedures, contracts and contractors that support or develop SAP IT (this information could be included in documents such as: Requests for Information, Requests for Proposals, Statements of Work, Statements of Objectives), system security and other system assessments, system vulnerabilities, system authorization documents, documentation describing vulnerabilities of any software or hardware used by SAP systems, documents or data with enough technical specification to reveal potential system vulnerabilities, locations of systems, services, infrastructure, including locations of personnel supporting SAP systems, specific details on performers who could be targeted to derive the above information, and contact information for performers (contractors) and DoD personnel.

Gaining this information about these systems and assets, individually or in the aggregate, would enable an adversary to identify vulnerabilities in these systems that, if exploited, would likely result in the significant disruption, destruction, or damage of or to DoD operations. While some items of information associated with SAP systems may be unclassified, the composite of the information could be used by adversaries to cause grave damage to national security.

I considered the public interest in the disclosure of this SAP IT system data and weighed it against the risk of harm that might result if it were disclosed. Because the public interest in this information is minimal, and the risk of harm that might result from its disclosure is extremely significant, I have determined that the public interest does not outweigh the protection of this information. Therefore, it should be exempt from public disclosure.