DETERMINATION OF THE DIRECTOR OF ADMINISTRATION AND MANAGEMENT

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:

> The programmable source code for the ForcePro software used by the Department of the Air Force.

Date: 2-12-2014

Michael L. Rhodes
Director of Administration and Management

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

In accordance with 10 U.S.C. § 130e, I reviewed the information provided to me by the Department of the Air Force concerning the programmable source code for the ForcePro software used by the Department of the Air Force, and determined that it qualifies as Department of Defense (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 programmable source code for the ForcePro software meets this definition of CISI because the ForcePro program is used by Air Force installation commanders and security personnel to determine security vulnerabilities at Air Force bases worldwide and conduct risk management assessments of identified critical security weaknesses.

If an adversary had this source code, they would have access to the methodologies and algorithms used within the program which would provide insight into the priorities the Air Force places on high value, strategic, nuclear, and political targets, and other valuable infrastructure resources directly related to the defense of DoD assets. The code methodology is based upon an in-depth review of copious vulnerability assessment reports obtained from agencies that conducted visits to numerous DoD installations and sites. With knowledge of these targeted objectives through examination of the source code, an adversary has the tools necessary to cultivate the intelligence and counterintelligence relationships necessary in determining potential vulnerabilities. They can then exploit those weak points to bypass force protection measures, thereby causing grave or serious damage to Air Force priority resources, disruption of operations, or harm to Air Force personnel.

Additionally, an adversary having the source code would gain insight as to the lower priority prospective targets which the Air Force cannot provide as much protection for because of limited manpower resources or protective measures. The adversary would then be able to circumvent implemented security tactics, techniques, and procedures, thereby increasing the risk to resources and personnel.

The public interest in the disclosure is minimal in this instance. Therefore, the public interest consideration in the disclosure of this information does not outweigh preventing the

disclosure of the information. This determination excludes editable electronic files or other information associated with the ForcePro software.