DETERMINATION OF THE CHIEF MANAGEMENT OFFICER

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:

> Department of the Navy Strategic Weapons System Program safety and security information.

HERSHMAN.LISA.W.1544505641 Digitally signed by HERSHMAN.LISA.W.1544505641 Date: 2019.07.05 15:50:38 -04'00'

Date: _____ _____

Lisa W. Hershman
Acting Chief Management Officer

STATEMENT OF THE BASIS FOR THE DETERMINATION BY THE CHIEF MANAGEMENT OFFICER

In accordance with 10 U.S.C. § 130e, I reviewed the information provided to me by the Department of the Navy (DON) concerning the safety and security of the Strategic Weapons System (SWS) Program of the Strategic Systems Programs (SSP), and determined that it qualifies as Department of Defense (DoD) critical infrastructure security information (DCRIT). As defined by 10 U.S.C. § 130e(f), DCRIT 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."

SSP is the DON Echelon II Command whose core missions include cradle-to-grave responsibility for approximately 70% of the United States strategic deterrent; DON nuclear weapons security; submarine large diameter launch tube payload integration; strategic nuclear weapons treaty implementation; and the design, acquisition, and sustainment of strategic conventional prompt strike capabilities. The SWS Program refers to the operations, systems, facilities used or employed in support of those missions. SWS Program assets include nuclear capable and conventional weapon and weapon control systems, supporting information systems, research and development assets, key personnel and installations, and test and evaluation equipment.

The SWS Program maintains safety and security information on its various assets, which are essential to supporting SSP's core missions. This safety and security information, some of which is unclassified, includes: ammunition and explosives storage locations, nuclear weapons accident and incident response plans, cybersecurity risk assessments, and nuclear and conventional weapons security capabilities. Gaining access to this SWS Program safety and security information in the categories of unclassified information listed below, individually or in the aggregate, would enable an adversary to determine how and where to most effectively disrupt SWS Program operations. Amongst other impacts, a disruption of such operations could impact SSP's ability to meet United States Strategic Command's strategic deterrent and conventional strike requirements, which poses a significant threat to national security. Therefore, it is imperative that adversaries or potential adversaries are denied access to information that would enable them the ability to replicate, reverse engineer, compromise, defeat, or otherwise challenge the credibility of the sea-based strategic deterrent, the safeguarding of nuclear-capable weapons, or the DON's conventional strike capabilities.

The categories of unclassified information containing such SWS Program safety and security information, thereby qualifying as DCRIT, include:

- SWS Program Installation and Facility Information (e.g., physical vulnerabilities, capabilities, ordnance handling routes, industrial safety, and NWS);

- Explosives Safety Information (e.g., explosives safety quantity distance arcs and explosives safety standards);

- SWS Program Incident Response Information (e.g., incident response force personnel and incident response force capabilities);

- Nuclear Weapons Security and Transit Protection Program Operational and Technical Information (e.g., security force and Transit Protection Program (TPP) personnel, security force and TPP capabilities, Electronic Security System, and Entry and Circulation Control System);

- SWS Program Security Information (e.g., physical security and cybersecurity);

- SWS Program Operations Information (e.g., movement of nuclear capable and conventional weapons, operational support equipment capabilities, and weapons production and storage);

- SWS Program Specifications (e.g., systems engineering, systems testing data, and sensitive financial and budgeting information);

- SWS Program Logistical Data (e.g., supply chain management, logistics information systems, and transportation of SWS Program assets);

- SWS Program Information Technology (e.g., SWS Network Enterprise (SWSNET), stand-alone SWS Program networks and systems, and physical infrastructure and connectivity)

I considered the public interest in the disclosure of DON SWS Program information and weighed this against the risk of harm that might result if this information were to be disclosed. Because the public interest in the disclosure is minimal, and the risk of harm that might result from this information is extremely significant, I have determined that the protection of this information is critical to the security of the DoD infrastructure and should be exempt from disclosure.