DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

CHIEF INFORMATION OFFICER

DEC - 7 2017

The Honorable Jeanne Shaheen
United States Senate
Washington, D.C. 20510

Dear Senator Shaheen:

I am responding on behalf of the Secretary of Defense to your letter of October 17, 2017. The Department shares your concerns pertaining to Russia's Federal Service for Technical and Export Control (FSTEC) review of Hewlett Packard Enterprise (HPE) product source code.

The Department of Defense (DoD) is aware of requirements imposed by certain countries, such as China and Russia, for companies to submit to source code reviews for certain types of security products under certain circumstances. Such disclosures may aid such countries in discovering vulnerabilities in those products under review.

DoD participates in Federal government-wide efforts to protect sensitive commercial technologies through export control risk management. In addition, DoD has processes in place to protect its sensitive information provided to the Defense Industrial Base. DoD does not currently monitor whether commercial information technology vendors share source code or other (non-controlled) commercial intellectual property.

To address the risks associated with the use of commercial products such as ArcSight, the Department has an established approach to supply chain risk management that uses clearly defined process and functions to acquire products. DoD Policy (DoDI 5200.44, Protecting Mission Critical Functions to Achieve Trusted Systems and Networks, November 5, 2012) requires DoD Components to perform supply chain risk management functions when acquiring products for use in national security systems.

These risk management processes may consider all source intelligence information, vulnerability information, results of hardware and software test and evaluation, and criticality of the product in the system. When a risk is revealed, the Department may employ any number of software analysis tools to determine whether a vulnerability exists. Some software analysis capabilities include static source code analysis, dynamic or static binary analysis, web application analysis, database analysis, and mobile application analysis. To advance hardware and software assurance in the Department, DoD established a Joint Federated Assurance Center. This organization identifies and promulgates expertise and capabilities, policies, guidance, requirements, best practices, contracting language, and more related to hardware and software assurance.

The Department does not currently require vendors of commercial information technology to disclose whether they have provided other governments' access to source code or other commercial intellectual property (IP). The Department is currently exploring the feasibility of such notification. The Department would be pleased to brief you on further classified details pertaining to its supply chain risk management efforts.

Sincerely,

John A. Zangardi
Acting