JEANNE SHAHEEN
NEW HAMPSHIRE

SUITE SH-506
HART BUILDING
WASHINGTON, DC 20510
(202) 224-2841

United States Senate

WASHINGTON, DC 20510

October 17, 2017

The Honorable James Mattis
Secretary of Defense
1000 Defense Pentagon
Washington, DC 20301

Dear Secretary Mattis:

I am writing with deep concerns about news reports that Hewlett Packard Enterprise (HPE) allowed a Russian defense agency, the Federal Service for Technical and Export Control (FSTEC), to review the source code of cyber defense software used by the Department of Defense (DoD) to defend its computer networks from cyber attacks.

HPE's ArcSight system constitutes a significant element of the U.S. military's cyber defenses. Therefore, the disclosure of ArcSight's source code presents FSTEC and other Russian military and intelligence entities with the opportunity to exploit a system used on DoD platforms. Such disclosure could also lead to the illicit transfer of valuable intellectual property to domestic Russian competitors.

Cybersecurity experts generally agree that source code inspection or disclosure regimes are unlikely to enhance a nation's cybersecurity because of the complexity involved in identifying coding flaws through inspection of codebases. Yet, unfortunately, Russia has used national security as a justification for adopting far-reaching legal requirements mandating disclosure of source code or intrusive inspections of intellectual property as prerequisites for foreign businesses to access their domestic markets. Indeed, the disclosure of ArcSight's source code was reportedly required in order to achieve Russian certifications necessary to sell the product to Russian public sector entities. I understand that individual businesses must make decisions weighing the risk of intellectual property disclosure against the opportunity of accessing significant overseas markets; however, when such products undergird DoD cyber defenses, our national security may be at stake in these decisions.

With these concerns in mind, I am writing with several specific questions about DoD's efforts to monitor and mitigate such risks:

- What specific risks do you foresee with the disclosure of ArcSight's source code to FSTEC, and what steps is DoD taking to mitigate these risks?
- In general, what measures does DoD take to monitor whether its information technology vendors disclose source code or other sensitive technical data to other governments, and to mitigate risks when such disclosures occur?
- How frequent are instances in which vendors disclose to foreign governments the source code or sensitive technical data of systems or products used within the Department?

- Does DoD require vendors providing information technology to DoD to disclose whether they have provided other governments access to source code or other sensitive technical data prior to purchasing such products?
- What is the strategy of the Department, and the broader Administration, to oppose and challenge source code disclosure and similar regimes in Russia, China, and other nations?

I would appreciate a detailed response to these questions at your earliest convenience. The cybersecurity of the Department of Defense is critical to the United States Military's global technological and battlefield supremacy, and I stand ready to work with you to take whatever measures may be necessary to bolster its security in this regard.

Thank you for your attention to this matter.

Sincerely,

Jeanne Shaheen
United States Senator