United States Senate
WASHINGTON, DC 20510

Ms. Leslie Beavers
Office of the Department of Defense
Acting Chief Information Officer
6000 Defense Pentagon
Washington, D.C. 20301-6000

July 19, 2024

Dear Ms. Beavers:

On July 19, 2024, businesses and governments around the world experienced crippling IT outages that caused widespread system disruptions. It is reported that entities and individuals using CrowdStrike cybersecurity products to protect Microsoft Windows encountered a “Blue Screen of Death”, rendering entire IT systems inoperable. Although CrowdStrike and Microsoft have publicly stated systems are being restored to a fully operational status, entities affected by the outage will take days and weeks to recover. This outage is a warning that consolidation and dependence on one provider can be catastrophic, which is why business and government IT systems should have the requisite redundancies in place that promote resiliency, as well as competition and innovation.

In today's interconnected world, IT systems form the backbone of nearly every aspect of personal, business, and government operations. They ensure the secure processing of vast amounts of data, support critical infrastructure, and drive innovations that fuel economic growth and societal progress. Our deep reliance on this technology underscores the importance of reliable IT systems, without which global implications such as the ones experienced by the CrowdStrike incident can render critical infrastructure and other vital systems useless, disrupting major aspects of daily life.

The Department of Defense (DoD) is no exception, relying heavily on a complex stack of interoperable cybersecurity products that facilitate communication and connectivity across the DoD enterprise. Testing software updates before release is crucial to ensure the reliability, security, and performance of the Department of Defense Information Network (DoDIN). Unvetted updates can introduce bugs, vulnerabilities, and compatibility issues, leading to significant operational disruptions and potential data breaches. This testing process protects users from unexpected issues, maintains trust in the software, and ultimately saves time and resources by preventing the need for urgent fixes post-release. In environments where security and precision are paramount, such as within the DoD, rigorous testing of software updates is essential to uphold operational integrity and safeguard sensitive information.

Therefore, I am requesting a briefing to answer the following questions. I am requesting this briefing no later than July 26th, 2024:

1. Was DoD affected by a widespread outage affecting Microsoft Windows hosts due to an issue with a recent CrowdStrike update or any other disruptions?
2. If so, what were the impacts, and how did the outage affect mission readiness?
3. What procedures does DoD employ to evaluate and vet software updates before deploying them on the DoDIN?
4. How is regression testing conducted to ensure that new updates do not negatively impact existing functionalities and system performance?

I appreciate your prompt attention to these concerns and your timely response to these questions.

Sincerely,

Eric S. Schmitt

Eric. S. Schmitt
United States Senator