MARK R. WARNER
VIRGINIA

COMMITTEES:
FINANCE
BANKING, HOUSING, AND URBAN AFFAIRS
BUDGET
INTELLIGENCE
RULES AND ADMINISTRATION

United States Senate

WASHINGTON, DC 20510–4606

February 26, 2020

Dana Deasy
Chief Information Officer
U.S. Department of Defense
1300 Defense Pentagon
Washington, DC 20301-1300

Dear Mr. Deasy:

I write about some recently reported cybersecurity issues at DoD. In particular, I read about malware actively exploiting a security misconfiguration that was recently discovered on a Department of Defense (DoD) web server. From the current analysis and reporting of the incident, the malware was part of a botnet that apparently mined cryptocurrency using DoD resources and IT systems[1] and raises broader cybersecurity concerns.

According to news reports, a security researcher first found the vulnerability on a DoD-managed cloud computing system exposed to the internet. The researcher then discovered that malware associated with mining Monero cryptocurrency was installed and operating on the same server. In January, once the security certificate identified the web server as an official DoD resource, the researcher reported the vulnerability and subsequent malware discovery under DoD's official vulnerability disclosure program.[2]

This incident demonstrates the inherent value of vulnerability disclosure programs for information technology products operated by federal agencies. These programs are a crucial force multiplier for federal cybersecurity efforts. Clear guidelines and a process for security researchers to find and share vulnerabilities enabled this malware discovery, and ultimately prompt remedial action by DoD. Continuing to encourage the responsible discovery and disclosure of bugs or vulnerabilities on federal information technology systems with both internal and outside security researchers can only strengthen the cybersecurity posture of federal and DoD systems.

There is pending bipartisan, bicameral legislation that I have introduced which would ensure that vendors of key information technology products, such as Internet of Things devices, maintain

[1] Catalin Cimpanu, "Zero Day," ZDNet (February 5, 2020) available at https://www.zdnet.com/article/bug-hunter-finds-cryptocurrency-mining-botnet-on-dod-network
[2] Nitesh Surana, "Public Instance of Jenkins," HackerOne (January 31, 2020) available at https://hackerone.com/reports/768266

coordinated vulnerability programs.[3] This bill would serve as a complement to the procedures DoD already employs.

While the use of commercial cloud computing can be a cost effective method to deploy and manage information technology and services, the use of a cloud itself does not ensure cybersecurity. Rigorous cybersecurity defensive measures and monitoring remain crucial for systems, even when DoD resources are deployed on commercial cloud computing platforms. While open source software, such as the automation server employed in this incident, may be beneficial, it is also essential to monitor all software for vulnerabilities and ensure they are promptly mitigated. Likewise, continuous use of software requires an effective continuous monitoring process for addressing newly discovered vulnerabilities in the software. And perhaps most importantly in the shared security model of commercial cloud computing, ensuring safe and secure configurations related to access is a key concern.

I am hopeful that DoD will take the lessons from this incident seriously and reassess current processes as necessary. It is crucial to ensure that future incidents involving open vulnerabilities and improper access configurations that permit malware installation on federal information technology systems cannot reoccur, including on systems hosted by commercial cloud service providers. I also hope to continue to work with you on passing my legislation and continuing to push for strong, thoughtful, cybersecurity policies.

As always, I appreciate your service in this important role.

Sincerely,

Mark R Warner

MARK R. WARNER
United States Senator

[3] Internet of Things Cybersecurity Improvement Act of 2019, S. 734, 116th Cong. (2019).