



CHIEF INFORMATION OFFICER

DEPARTMENT OF DEFENSE

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

DEC 13 2021

The Honorable Ronald Wyden
221 Dirksen Senate Office Building
Washington, DC 20510

Dear Senator Wyden:

Thank you for your interest in the protection of the Department of Defense (DoD) computers and personnel from hacking and surveillance threats by foreign spies and criminals misusing online advertising. This response is to your July 20, 2021 letter addressed to the then-Acting Department of Defense (DoD) Chief Information Officer (CIO), Mr. Sherman. My sincerest apologies for the delayed response due to administration transitions and associated personnel changes. The Department appreciates your support and understands the concerns you raised.

The following are answers to the specific questions from your letter on July 20, 2021:

1. Has DoD deployed ad blocking technology on DoD-issued computers and mobile devices that DoD personnel use to browse the internet, as recommended by the National Security Agency (NSA) and Cybersecurity and Infrastructure Security Agency (CISA)? If not, please provide a timeline for when DoD intends to deploy technology to protect against online-advertising related malware and data collection threats.

Yes, the Defense Information Systems Agency (DISA) has deployed various technologies to protect against online-advertising related malware and data collection threats. Web content filter and Sharkseer tools block bad traffic that traverses our internet access points and Cloud Based Internet Isolation (CBII) also isolates all traffic, including ads.

2. Section 1645 of the 2017 National Defense Authorization Act gave DoD the authority to protect the personal devices of DoD personnel from cyber threats. What actions has DoD taken to protect personal smartphones carried by DoD personnel in sensitive locations from online-advertising related malware and data collection threats? If DoD has taken no actions, please explain why and provide a timeline for when DoD intends to address these threats.

DISA recently released the "Telework Dos and Don'ts," updated for Mobile Devices. This interactive training explains security issues associated with unclassified government-provided and government-authorized mobile devices, as well as personal mobile devices used in a government setting. It outlines various types of mobile devices and wireless radio technologies and their vulnerabilities, reviews which personal mobile devices may be used in a government

setting and under what conditions, and discusses methods of protecting unclassified government-provided and government-authorized mobile devices. Specifically, for government-issued mobile devices, DISA deployed a Mobile Threat Detection capability on each device that monitors the device, network, and applications for malware and other threats that could use online advertising as an attack vector.

3. What actions has DoD taken to require contractors and sub-contractors to implement the NSA and CISA guidance to protect against online-advertising related malware and data collection threats? If DoD has taken no actions, please explain why and provide a timeline for when DoD intends to address these threats.

The Department routinely shares “best cybersecurity practices” with contractors/sub-contractors via the Defense Industrial Base Network (DIBNet) Portal. This includes the National Security Agency (NSA) and Cybersecurity and Infrastructure Security Agency (CISA) guidance released to protect all employees against online-advertising related malware and data collection threats. Additionally, the Department requires DoD Contractors to comply with the cybersecurity requirements of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, as specified in the Defense Federal Acquisition Regulation Supplement (DFARS) Clause 252.204-7012.

Sincerely,

A handwritten signature in black ink, appearing to read 'Kelly E. Fletcher', followed by a long horizontal line extending to the right.

Dr. Kelly E. Fletcher
Performing the Duties of the CIO
of the Department of Defense