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

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: Guidance for Use of Embedded Computer Capabilities and External Computer Peripherals in Telework Environments

References: (a) DoD Chief Information Officer Memorandum, "COVID-19 Response: Remote Work Capability," March 19, 2020
(b) DoD Chief Information Officer Memorandum, "Authorized Telework Capabilities and Guidance," April 10, 2020
(c) Deputy Secretary of Defense Memorandum, "Mobile Device Restrictions in the Pentagon," May 22, 2018
(d) DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014

The DoD Chief Information Officer (DoD CIO) issued references (a) and (b) to support mission initiatives in a telework environment. This memorandum addresses the use of embedded computer capabilities (e.g., cameras, microphones, WiFi) and external computer peripherals on DoD-issued unclassified computers (e.g., desktop/laptop, tablets, smartphones, etc.) used in telework environments. For the purpose of this memorandum, computer peripherals are external devices (e.g., common access card (CAC) readers, cameras, microphones, keyboards, mice, monitors, printers, etc.) physically or wirelessly connected to DoD-issued computers.

Personnel may connect personally-owned computer peripherals to DoD-issued computers used in telework environments in accordance with reference (b). Storage devices (e.g., USB memory sticks, hard drives, etc.) remain prohibited. Personally-owned external monitors may be connected to DoD-issued computers in telework environments via VGA or DVI, but not via USB. HDMI or DisplayPort may be used if VGA and DVI are unavailable. Personnel may not connect personally-owned peripherals manufactured by any source designated by their Component or the Defense Information Systems Agency (DISA) as being prohibited. This includes any company prohibited by law, to include Huawei, ZTE, Hikvision, Hytera, and Dahua. DISA has published an Approved Products List to https://cyber.mil/covid19, which can be used to help inform Component risk acceptance decisions. Personnel may connect any DoD-issued peripherals to their DoD-issued computers in telework environments.

Component Senior Information Security Officers (SISOs) are authorized to enable embedded cameras, microphones and WIFI on DoD-issued computers used in telework environments, but must also document procedures for both enabling and then re-disabling these embedded capabilities. Cameras, microphones and WIFI must be disabled prior to reintroduction into any classified spaces. In addition, prior to reintroduction into classified spaces in the Pentagon, these capabilities must be physically disabled in accordance with reference (c). Users of DoD-issued computers with these capabilities enabled must be notified that they may

not reintroduce their computers into classified spaces until these capabilities have been properly disabled in accordance with the approved procedures.

Components must develop a methodology for reintroducing DoD-issued computers once the current telework requirements are ended. DoD-provided peripherals, including CAC readers used on non-DoD-issued computers, may be returned and reused. Personally-owned devices must be approved in accordance with Component guidance and local procedures prior to introduction into DoD spaces, and personally-owned external peripherals other than wired headsets are not permitted into DoD classified spaces.

Components and personnel must ensure that their telework activities and use of peripherals does not introduce more risk to the Department than necessary. Components must:

- Make personnel aware of the telework guidance posted to https://cyber.mil/covid19;
- Mitigate risks with documented tactics, techniques and procedures to the greatest extent possible;
- Consider product risks in the context of the specific operational use environment;
- Provide training specific to the peripheral being issued and used; and
- Ensure peripherals used on DoD computers shall be acquired, approved, and authorized by the agency managing the DoD computer in accordance with Reference (d).

Adherence to all standing cybersecurity policies and guidance is as important while teleworking as it is while working on-site. Questions for any aspects of this memo should be directed to OSD.COVID19.RemoteWorkTeam@mail.mil.

Digitally signed by WILMER.JOHN.W.III.1267975430
Date: 2020.05.01 08:54:21 -04'00'

John W. Wilmer, III
Senior Information Security Officer

DISTRIBUTION:
CHIEF MANAGEMENT OFFICER OF THE DEPARTMENT OF DEFENSE
SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
CHIEF OF THE NATIONAL GUARD BUREAU
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR OF COST ASSESSMENT AND PROGRAM EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR OF OPERATIONAL TEST AND EVALUATION
CHIEF INFORMATION OFFICER OF THE DEPARTMENT OF DEFENSE
ASSISTANT SECRETARIES OF DEFENSE FOR LEGISLATIVE AFFAIRS
ASSISTANT TO THE SECRETARY OF DEFENSE FOR PUBLIC AFFAIRS
DIRECTOR OF NET ASSESSMENT
DIRECTORS OF DEFENSE AGENCIES
DIRECTORS OF DOD FIELD ACTIVITIES