OFFICE OF THE SECRETARY OF DEFENSE
5000 DEFENSE PENTAGON
WASHINGTON, DC 20301-5000

June 4, 2021

MEMORANDUM FOR SENIOR PENTAGON LEADERSHIP
COMMANDERS OF THE COMBATANT COMMANDS
DEFENSE AGENCY AND DOD FIELD ACTIVITY DIRECTORS

SUBJECT: Collaboration Peripherals in Secure Spaces

The significant number of unauthorized microphones found connected to unclassified Department of Defense (DoD) information systems in recent months highlights the need for all DoD personnel to redouble their security focus. Over the same period of time, DoD experienced an increased demand for unclassified collaboration capabilities as a replacement for in-person meetings to connect DoD personnel with others in DoD facilities, telework environments, and industry. In some cases, the DoD personnel utilizing unclassified collaboration capabilities are located in spaces designated or accredited for the storage, discussion, or processing of classified information ("secure spaces"). This joint memorandum provides direction on the use of headsets, webcams, and microphones ("collaboration peripherals") in DoD secure spaces, including on unclassified computers (e.g., desktops, laptops, tablets) in DoD secure spaces.

Collaboration capabilities often support, but do not require, the use of collaboration peripherals. Many unclassified collaboration capabilities are just as effective when not all parties have webcams, and many also support telephone-based dial-in for parties that do not have computer-based microphones. The use of authorized unclassified collaboration capabilities is encouraged from DoD secure spaces, but the use of collaboration peripherals with those capabilities from a DoD secure space poses a significant risk of unauthorized disclosure of classified information, and the use of such peripherals must be consistent with this memorandum.

The use of collaboration peripherals in collateral DoD secure spaces (those designated or accredited for the storage, discussion, or processing of CONFIDENTIAL, SECRET, or TOP SECRET information but not Sensitive Compartmented Information (SCI) or Special Access Program (SAP) information) is permitted only in accordance with Attachment 1. The use of collaboration peripherals in SCI Facilities (SCIFs) or SAP Facilities (SAPFs) is permitted only in accordance with Attachment 2. All other uses of collaboration peripherals in DoD secure spaces is prohibited. Each attachment outlines the process for requesting exceptions to the restrictions in that attachment, and attachment 3 summarizes these restrictions in table form. Only government-furnished collaboration peripherals may be used in DoD secure spaces.

This memorandum applies to all secure spaces designated or accredited by DoD for the storage, discussion, or processing of classified information in DoD-owned or -leased facilities and contractor-owned or -leased facilities (jointly referred to as "DoD secure spaces"). The May 22, 2018 Deputy Secretary of Defense memorandum, "Mobile Device Restrictions in the Pentagon," and exceptions to that memorandum signed jointly by the Under Secretary of Defense for Intelligence and Security and the DoD Chief Information Officer remain in effect. The use of authorized classified collaboration capabilities and peripherals (e.g., internal or wired external microphones or webcams attached to classified computers, SECRET or TOP SECRET video teleconference systems (VTCs), and SECRET or TOP SECRET Tandberg VTCs) or

authorized unclassified conference room-style VTCs specifically designed for use in secure spaces is not covered by this memorandum.

DoD Components are cautioned that successful application of the restrictions and procedures contained in this memorandum requires vigilance by users and security managers. Violations of these restrictions or procedures may result in administrative actions. Individuals unsure if their workspace is a secure space, or if their secure space is a collateral secure space or a SCIF or SAPF, should consult their local security personnel. Further information on Telephone Security Group (TSG)-approved devices, as described in the attachments, may be found at https://www.dni.gov/index.php/ncsc-what-we-do/ncsc-physical-security-mission. The point of contact for this matter is Mr. Josh Freedman at (703) 692-3724 or joshua.a.freedman.civ@mail.mil.

REID.GARRY.PAUL.1072277860 Digitally signed by REID.GARRY.PAUL.1072277860 Date: 2021.06.04 15:08:37 -04'00'

Garry P. Reid
Director for Defense Intelligence
Counterintelligence, Law Enforcement, & Security

MCKEOWN.DAVID.W.1034948050 Digitally signed by MCKEOWN.DAVID.W.1034948050 Date: 2021.06.04 09:51:58 -04'00'

David W. McKeown
Deputy Chief Information Officer for Cybersecurity

Attachments:
As stated

Attachment 1 – Collaboration Peripherals in Collateral DoD Secure Spaces

Component Senior Information Security Officers (SISO), in coordination with Component Senior Agency Officials (SAO)[1], must establish standard operating procedures for the use of any collaboration peripherals approved in accordance with this attachment. In situations where the Component with cognizance over the computer differs from the Component with cognizance over the collateral DoD secure space, the SAOs from the two Components must coordinate on all matters in this attachment involving the SAO. Universal serial bus (USB) collaboration peripherals that have been connected to classified computers may not subsequently be connected to unclassified computers, or vice versa. Personally- or privately-owned headsets, microphones, desktop telephone units, and webcams are prohibited in DoD secure spaces.

Microphones and Headsets

Wireless headsets, with or without microphone capability, are prohibited in DoD secure spaces. Headsets with noise-cancelling capabilities contain embedded microphones and are considered headsets with microphones regardless of any other user-accessible microphone capability. Microphone capabilities built into unclassified computers are prohibited in DoD secure spaces unless physically disabled[2]. Wired externally-connected headsets with microphone capability that is not controlled by a push-to-talk (PTT) feature[3] or by a telephone security group (TSG)-approved positive disconnection device (PDD) that operates through physical (not software) means (referred to jointly as "PTT/PDD") are prohibited when attached to an unclassified computer in a DoD secure space. The use of wired externally-connected headsets with microphone capability on unclassified desktop telephone units and computer-based "softphone" telephones in DoD secure spaces must include a PTT/PDD capability (either in the headset itself, physically wired in-line with the headset, or integrated into the desktop telephone unit) in accordance with Committee on National Security Instructions 5000, 5001, 5002, and applicable annexes.

Component SISOs may authorize the use of wired, externally-connected government-issued headsets with PTT/PDD-controlled microphone capabilities on unclassified computers in collateral DoD secure spaces, subject to restrictions by the Component SAO. Component SISOs may authorize the use of built-in microphone capabilities and wired externally-connected government-issued headsets with microphone capabilities on classified computers in collateral DoD secure spaces, subject to restrictions by Component SAOs. Wired externally-connected government-issued headsets without microphone capability are authorized on classified and unclassified computers in collateral DoD secure spaces.

---

[1] "Senior agency official" is the person designated in writing by the Head of Executive Branch Departments and Agencies to direct and administer the Department's Classified National Security Information program, in accordance with paragraph 5.4(d) of Executive Order 13526.

[2] "Physically disabled" is a method of disablement that cannot be made or reversed, by privileged or non-privileged users or administrators, through logical settings configured by software (such as applications, operating systems, firmware, basic input/output system (BIOS), or unified extensible firmware interface (UEFI)), or otherwise configured in volatile or non-volatile memory or storage.

[3] "Push to talk" is a capability that requires the user of a device to depress a physical button somewhere on the device to physically enable the device's microphone, and that automatically physically disables the microphone when the button is released. The microphone remains physically disabled whenever the button is not depressed.

Webcams

Wireless webcams, with or without microphone capability, are prohibited in DoD secure spaces. Webcams built into unclassified computers are prohibited in DoD secure spaces unless physically disabled[2]. Component SISOs may authorize the use of built-in or wired externally-connected government-issued webcams, with or without microphone capability, on classified computers in collateral DoD secure spaces, subject to restrictions by Component SAOs.

Component SISOs may, subject to restriction by Component SAOs, authorize the use of wired, externally-connected government-issued webcams, with or without microphone capability, on unclassified computers in collateral DoD secure spaces only in private offices or conference rooms and only when connected through a TSG-approved automatic PDD. A private office is a room with solid walls on all sides, a ceiling, and one or more doors in which only one person is assigned to work. A conference room is a room with solid walls on all sides, a ceiling, and one or more doors in which no people are assigned to work. Solid walls and doors may have a reasonable number of windows provided sound attenuation is not significantly affected.

The PDD must physically and automatically disconnect the webcam from the unclassified computer upon the expiration of a timer, not to exceed 75 minutes but which may be renewed, or upon manual user action, and may not be manageable or configurable in any way from the unclassified computer. If the webcam includes microphone capability the PDD must sever both the audio and visual connection. Prior to activating the PDD to enable the webcam, the user must sanitize the space in the field of view of the webcam by physically removing any classified material and orienting the displays of any classified computers so that they are not in the field of view. The door or doors to the private office or conference room must be closed and signs must be posted at each entrance indicating that an unclassified webcam is in use.

Prior to authorizing such use of webcams in DoD secure spaces, Component SISOs must develop user agreements, to be signed by any individual authorized use of a webcam in collateral DoD secure spaces or in the telework environment, describing the increased restrictions on the use of webcams in collateral DoD secure spaces as compared to in the telework environment.

Exceptions

The Deputy DoD Chief Information Officer (CIO) for Cybersecurity and the Director for Defense Intelligence (Counterintelligence, Law Enforcement, & Security) may jointly approve exceptions to policy (E2P) for the restrictions contained in this attachment due to exceptional mission requirements that can only be met through the use of prohibited unclassified collaboration peripherals in a collateral DoD secure space. E2P requests, which must specify compensating security controls, will be submitted jointly by Component SISOs and Component SAOs through the E2P process established by the DoD CIO at https://rmfks.osd.mil/dode2p. In situations where an organization is a tenant in a DoD collateral secure space accredited by another DoD Component, both the SAO of the tenant Component and the SAO of the accrediting Component must coordinate on the E2P request. Requests for exceptions for collateral DoD secure spaces in the Pentagon are subject to the restrictions of the May 22, 2018 Deputy Secretary of Defense memorandum, "Mobile Device Restrictions in the Pentagon."

Attachment 2 – Collaboration Peripherals in SCIF or SAPF DoD Secure Spaces

Component Senior Information Security Officers (SISO), in coordination with the appropriate Sensitive Compartmented Information Facility (SCIF) Accrediting Official (SCIF AO) or the Special Access Program Facility (SAPF) Accrediting Official (SAPF AO), must establish standard operating procedures for the use of any collaboration peripherals approved in accordance with this attachment. In SCIF-based situations where the Component with cognizance over the computer, the Component that accredited the SCIF, or the Component that occupies the SCIF differ, the Component SISO, SCIF AO, and Cognizant Security Authority must coordinate with each other. In similar SAPF-based situations, the Component SISO, SAPF AO, and Program Security Officer must coordinate with each other. Universal serial bus (USB) collaboration peripherals that have been connected to classified computers may not subsequently be connected to unclassified computers, or vice versa. Personally- or privately-owned headsets, microphones, desktop telephone units, and webcams are prohibited in DoD secure spaces.

Microphones

Wireless headsets, with or without microphone capability, are prohibited in DoD secure spaces. Headsets with noise-cancelling capabilities contain embedded microphones and are considered headsets with microphones regardless of any other user-accessible microphone capability. Microphone capabilities built into unclassified computers are prohibited in DoD secure spaces unless physically disabled[4]. Wired external headsets with a microphone capability that is not controlled by a push-to-talk (PTT) feature[5] or a telephone security group (TSG)-approved positive disconnection device (PDD) that operates by physical (not software) means (referred to jointly as "PTT/PDD") are prohibited when attached to an unclassified computer in a DoD secure space. The use of wired externally-connected headsets with microphone capability on unclassified desktop telephone units and computer-based "softphone" telephones in DoD secure spaces must include a PTT/PDD capability (either in the headset itself, physically wired in-line with the headset, or integrated into the desktop telephone unit) in accordance with Committee on National Security Instructions 5000, 5001, 5002, and applicable annexes.

Component SISOs may authorize the use of wired, externally-connected headsets with PTT/PDD microphone capabilities on unclassified computers in SCIFs and SAPFs, subject to restriction by the SCIF AO and SAPF AO respectively. Component SISOs may authorize the use of built-in microphone capabilities or wired externally-connected headsets with microphone capabilities on <u>classified</u> computers in SCIFs and SAPFs, subject to restriction by the SCIF AO and SAPF AO respectively. Wired externally-connected headsets without microphone capability are authorized on classified and unclassified computers in SCIFs and SAPFs.

---

[4] "Physically disabled" is a method of disablement that cannot be made or reversed, by privileged or non-privileged or administrators, through logical settings configured by software (such as applications, operating systems, firmware, basic input/output system (BIOS), or unified extensible firmware interface (UEFI)), or otherwise configured in volatile or non-volatile memory or storage.

[5] "Push to talk" is a capability that requires the user of a device to depress a physical button somewhere on the device to physically enable the device's microphone, and that automatically physically disables the microphone when the button is released. The microphone remains physically disabled whenever the button is not depressed.

Webcams

Wireless webcams, with or without microphone capability, are prohibited in DoD secure spaces. Webcams built into unclassified computers are prohibited in DoD secure spaces unless physically disabled[4]. Wired external webcams connected to unclassified computers are prohibited in DoD SCIFs and SAPFs. Component SISOs may authorize the use of built-in or wired external webcams on classified computers in DoD SCIFs and SAPFs, subject to restriction by the SCIF AO and SAPF AO respectively.

Exceptions

The Deputy DoD Chief Information Officer (CIO) for Cybersecurity and the Director for Defense Intelligence (Counterintelligence, Law Enforcement, & Security) may jointly approve exceptions to policy (E2P) for the restrictions contained in this attachment due to exceptional mission requirements that can only be met through the use of prohibited unclassified collaboration peripherals in a SCIF or SAPF. E2P requests pertaining to SCIFs, which must specify compensating security controls, will be submitted jointly by the Component SISO and the SCIF AO that accredited the SCIF. E2P requests pertaining to SAPFs will be submitted jointly by the Component SISO and the SAPF AO that accredited the SAPF. E2P requests pertaining to DoD secure spaces that are co-accredited as a SCIF and a SAPF, or to a SCIF with a SAPF compartmented area within, will be submitted jointly by the Component SISO and both the SCIF AO and SAPF AO that accredited the secure space. All requests will be submitted through the E2P process established by the DoD CIO at https://rmfks.osd.mil/dode2p. Requests for exceptions for SCIFs or SAPFs in the Pentagon are subject to the restrictions of the May 22, 2018 Deputy Secretary of Defense memorandum, “Mobile Device Restrictions in the Pentagon.”

Attachment 3 – Summary Table

Collateral DoD Secure Spaces

Government-Issued	Open Work Areas (e.g., cubicles, bull-pen, etc.)	Private Offices & Conference Rooms
Wireless Headsets, Microphones, or Webcams	Prohibited.	
Built-In Microphones or Webcams	Prohibited in unclassified computers unless disabled by physical, not software, means. May be authorized in classified computers.*	
Wired External Microphones	May be authorized on unclassified devices only when equipped with push to talk (PTT) capability or a TSG-approved positive disconnect device (PDD) that operates by physical means.* May be authorized on classified computers.*	
Wired External Webcams	Prohibited on unclassified computers. May be authorized on classified computers.*	May be authorized on unclassified computers only when connected through a TSG-approved automatic PDD that operates by physical means and with restrictions described in this memorandum.* May be authorized on classified computers.*
Wired External Headsets without a Microphone	Authorized	Authorized

* Subject to approval by the SISO, and potential restriction by the SAO, of the Component with cognizance over the computer or device. In cases where this Component is different from the Component with cognizance over the secure space, the SAOs from the two Components must coordinate with each other.

SCIF or SAPF DoD Secure Spaces

Government-Issued	Open Work Areas (e.g., cubicles, bull-pen, etc.)	Private Offices & Conference Rooms
Wireless Headsets, Microphones, or Webcams	Prohibited.	
Built-In Microphones or Webcams	Prohibited in unclassified computers. May be authorized in classified computers.**	
Wired External Microphones	May be authorized on unclassified devices only when equipped with PTT capability or a TSG-approved PDD that operates by physical means.** May be authorized on classified computers.**	
Wired External Webcams	Prohibited on unclassified computers. May be authorized on classified computers.**	
Wired External Headset without a Microphone	Authorized	

** Subject to approval by the SISO of the Component with cognizance over the computer or device, and potential restriction from SCIF AO that accredited the SCIF or SAPF AO that accredited the SAPF.