WEBCAM AND MICROPHONE USE ACKNOWLEDGMENT FORM

Authority:
Executive Order 10450, 9397; Public Law 99-474; the Computer Fraud and Abuse Act; 5 U.S.C Statute 301; 10 U.S.C. Part II; 14 U.S.C. Chapter 11; UCMJ; DOD 5500.7R, Joint Ethics Regulation; CJCSM 6510.05, SECNAVINST 5239.3A, DON Information Assurance (IA) policy, and E.O. 9397; NETWARCOM message;
311452ZMAR2005 and DON CIO message 161957ZOCT02 Remote Access To Enterprise Email From non-DoD Computers.

References:

(a) TASKORD 17-023, Actions for Microphone Mitigation;
(b) Network Services Policy STIG.
(c) NAVADMIN 148/20, Updated Policy for the Use of Embedded Computer Capabilities and Peripherals to Support Two-Way Collaboration.

Privacy Act of 1974 Statement: This Regulation is reissued under the authority of DoD Directive 5400.11, "DoD Privacy Program," May 8, 2007 (Reference (a)). It provides guidance on section 552a of title 5 United States Code (U.S.C.), the Privacy Act of 1974, as amended, (Reference (b)), and prescribes uniform procedures for implementation of the DoD Privacy Program.

Purpose: To ensure that the undersigned user fully understands the very intent of the policies and procedures of ONE-Net with respect to the use of Webcams and microphones on ONE-Net CLASSIFIED and UNCLASSIFIED workstations via network connection, OWA access, and/or VPN solution, either explicitly detailed or implicitly implied.

As a network user utilizing a web camera and/or microphone on a ONE-Net system, it is important to realize that these collaboration tools inherently present a risk, including unintentional information sharing and remote camera execution. By continuing use of this system, (which includes any device attached to the system), you acknowledge and consent to the following conditions to mitigate risk:

1. I understand that I WILL NOT utilize a laptop with an enabled embedded camera or microphone in a CLASSIFIED space;
2. I understand that I WILL NOT display SENSITIVE or CLASSIFIED information on walls that are within the view of the camera(s), nor will I place SENSITIVE or CLASSIFIED information on a table or desk within the view of the camera(s) without proper protection (e.g., a proper cover);
3. I understand that I WILL NOT read or view SENSITIVE or CLASSIFIED information at such an angle that the camera(s) could focus on it;
4. I understand that I WILL utilize a headset in lieu of long range microphone and speakers whenever possible;
5. I understand that I WILL maintain volume settings of speakers such that the session information is not heard by non-participants in a work area;
6. I understand that I WILL disconnect external web cameras and microphones when not in use;
7. I understand that I WILL disable (or cover) embedded cameras and/or microphones not in use whenever possible.
8. I understand that I WILL NOT utilize a device designated by Navy or the Defense Information Systems Agency (DISA) as prohibited. To include any company prohibited by law, such as Huawei, Hikvision, Hytera, Dahua, and ZTE (Zhong Xing Telecommunication Equipment).

By signing Requester Signature (Block 13, the requester acknowledges and consents to understanding items 1 through 8, as stated above, and therefore accepts responsibility for any violations.

NOTE: Wireless devices such as mice, keyboards, etc. are NOT AUTHORIZED to be connected to ONE-Net.

Any violation of the above constitutes a security incident and will be treated as such.

1.) TYPE OF REQUEST	2.) DESIGNATION OF REQUESTOR	3.) TYPE OF ACCESS	4.) DATE OF SAAR-N ON FILE (Format – dd-MON-yyyy)	5.) COMMAND	6.) DEPARTMENT/DIVISION
Initial	Military	NIPRNet			

7.) REQUESTOR'S NAME (Format–Last, First, Middle) ☐ Check box for multiple users (Use User Continuation Page)	8.) REQUESTER OFFICIAL (.MIL) EMAIL

9.) JUSTIFICATION FOR ACCESS	10.) DSN PHONE (Area Code + 7 Digits)	11.) COMMERCIAL PHONE (Format – enter number after + (add dashes))
To perform official Government work.		

12.) ONE-NET WORKSTATION INFORMATION Requester understands: Only Government-owned LAPTOPS are approved for VPN access and are subject to re-inspection every 30-days.

12a.) MAKE	12b.) MODEL	12c.) SERIAL NUMBER/NAME

13.) ONE-NET WEBCAM/MICROPHONE INFORMATION Lists device that will be associated to workstation.

13a.) MAKE	13b.) MODEL/NAME	13c.) SERIAL NUMBER

14.) REQUESTOR (DIGITAL ONLY) SIGNATURE	15.) DATE (Format – dd-MON-yyyy)

16.) REQUESTOR'S SUPERVISOR NAME (Format – Last, First, Middle)	17: DSN PHONE (Area Code + 7 Digits)	18.) DATE (Format – dd-MON-yyyy)

19.) REQUESTOR'S SUPERVISOR OFFICIAL (.MIL) EMAIL	20.) REQUESTOR'S SUPERVISOR (DIGITAL ONLY) SIGNATURE

WEBCAM AND MICROPHONE USE ACKNOWLEDGMENT FORM (USER CONTINUATION PAGE)

Purpose: This page is ONLY to be utilized in situations where there are multiple users using a single Web-cam/Workstation. Disregard this page for single user requests.

Each user listed below is stating that they are a network user utilizing a web camera and/or microphone on a ONE-Net system, and realizes that these collaboration tools inherently present a risk, including unintentional information sharing and remote camera execution. By continuing use of this system, (which includes any device attached to the system), you acknowledge and consent to the following conditions to mitigate risk:

1. I understand that I WILL NOT utilize a laptop with an enabled embedded camera or microphone in a CLASSIFIED space;
2. I understand that I WILL NOT display SENSITIVE or CLASSIFIED information on walls that are within the view of the camera(s), nor will I place SENSITIVE or CLASSIFIED information on a table or desk within the view of the camera(s) without proper protection (e.g., a proper cover);
3. I understand that I WILL NOT read or view SENSITIVE or CLASSIFIED information at such an angle that the camera(s) could focus on it;
4. I understand that I WILL utilize a headset in lieu of long range microphone and speakers whenever possible;
5. I understand that I WILL maintain volume settings of speakers such that the session information is not heard by non-participants in a work area;
6. I understand that I WILL disconnect external web cameras and microphones when not in use;
7. I understand that I WILL disable (or cover) embedded cameras and/or microphones not in use whenever possible.
8. I understand that I WILL NOT utilize a device designated by Navy or the Defense Information Systems Agency (DISA) as prohibited. To include any company prohibited by law, such as Huawei, Hikvision, Hytera, Dahua, and ZTE (Zhong Xing Telecommunication Equipment).

By signing below, each requester acknowledges and consents to understanding items 1 through 8, as stated above, and therefore accepts responsibility for any violations.

NOTE: Wireless devices such as mice, keyboards, etc. are NOT AUTHORIZED to be connected to ONE-Net.

Any violation of the above constitutes a security incident and will be treated as such.

ADD'L USER	REQUESTOR'S NAME (Format – Last, First, Middle)	DESIGNATION OF REQUESTOR	REQUESTOR'S OFFICIAL (.MIL) EMAIL	DATE OF SAAR-N ON FILE (Format – dd-MON-yyyy)	REQUESTOR (DIGITAL ONLY) SIGNATURE
1.		Military			
2.		Military			
3.		Military			
4.		Military			
5.		Military			
6.		Military			
7.		Military			
8.		Military			
9.		Military			
10.		Military			
11.		Military			
12.		Military			
13.		Military			
14.		Military			
15.		Military			

ISSO/SECURITY OFFICIAL'S NAME (Format – Last, First, Middle)	Requesting ISSO/Security Official is verifying that a SAAR-N is on file for each user listed above.	ISSO/SECURITY OFFICER'S DSN PHONE	ISSO/SECURITY OFFICIAL'S (DIGITAL ONLY) SIGNATURE

REQUESTING OFFICIAL'S NAME (Format – Last, First, Middle)	REQUESTING OFFICIAL'S DSN PHONE	REQUESTING OFFICIAL'S COMMERCIAL PHONE

REQUESTING OFFICIAL'S (.MIL) EMAIL	REQUESTING OFFICIAL'S (DIGITAL ONLY) SIGNATURE