DEPARTMENT OF THE ARMY
HEADQUARTERS, UNITED STATES ARMY RESERVE COMMAND
4710 KNOX STREET
FORT BRAGG, NORTH CAROLINA 28310-5010

AFRC-CI 29 October 2020

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Use of Web Cameras on United States Army Reserve Managed Network Policy

1. References:

a. Voice Video Session Management Security Requirements Guide (SRG), Version 1, Release 6, 27 July 2018.

b. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4, April 2013 (updated 22 January 2015).

c. Windows 10 Security Technical Implementation Guide; Version 1, Release: 21 Benchmark Date: 24 Apr 2020 (V-63545 CAT II, V-100093 CAT II)

d. U.S. Army Forces Command (FORSCOM) Chief of Staff Directive 2016-01, Portable Electronic De4vices (PEDs).

e. USARC Device Exception to Policy (ETP) Request Procedures, 16 June 2020.

2. Purpose: This policy enforces secure use of web cameras on all United States Army Reserve (USAR) managed networks (Unclassified or Classified) with consideration for limiting network latency and preserving transport bandwidth.

3. Applicability: This policy applies to all users who access USAR managed networks (Unclassified or Classified).

4. Policy:

a. Webcams on USAR managed networks are disabled by GPO due to STIG rules V-63545 (CAT II) and V-100093 (CAT II), the propensity for privacy violations, and the difficulty in controlling what environments webcams may be employed in. The United States Army Reserve Command (USARC) Chief Information Officer (CIO)/G-6 further prohibits web camera devices with audio, video, recording, or transmission capabilities from areas where personnel discuss or electronically process classified information.

b. The Authorizing Official (AO) or Program Information System Security Manager (P- ISSM) may permit exceptions if the certification and accreditation package specifically documents the exception and the USARC CIO/G-6 Customer Support Branch enforces all classification, access, and encryption restrictions for the visual imagery (Reference 1a) as they would for a classified device. Webcam Type: USAR organizations may purchase products with built in web- camera functionality and are listed on the Approved Products List (APL) at https://aplits.disa.mil/processAPList.

c. The APL is the only listing of equipment authorized for use on DoD information systems. All purchases must be pre-approved by the USARC CIO/G-6 Strategy and Governance Branch and must be procured through the U.S. Army Computer Hardware and Enterprise Software and Solutions (CHESS) program at https://chess.army.mil/. Only CHESS approved webcams can be placed on ARNET. Wireless webcams are not authorized under any circumstances.

d. Webcams are only authorized for use with government provided video-capable applications (Microsoft Teams (CVR), GVS, Skype for Business, etc.). Webcams are not to be used within Commercial Off-The-Shelf (COTS) solutions (i.e. Vidyo, Facebook Live, Google Hangouts, Zoom, etc.) while connected to a DoD information system.

e. With the approval of the USAR Program Information Systems Security Manager (ISSM (P)), webcams may be enabled for the following: SGS, O-6/GS-14 or above, CSM/SGM, Unit Commander, critical Operations Officers or NCOs, or if a user is occupying a qualifying duty position (i.e. MSG performing SGM duties). Webcams may also be approved for extenuating circumstances like official distance learning courses, remote medical consultations, or virtual promotion boards. Additional specific information for webcams and COVID-19 is located at https://xtranet/usarc/g6/EOD/CUOPS/Operations%20COVID19/Home.aspx.

f. To request an Exception to Policy (ETP) to have a webcam enabled follow steps in Reference e. of paragraph 1.

g. Web cameras will support Public Key Infrastructure (PKI), digital certificates, Federal Information Processing Standards (FIPS), or National Security Agency (NSA) validated cryptographic modules or data encryption standards appropriate for the classification level of the information processed.

h. Web camera systems will implement identification and authentication measures at both the device and network levels if the AO grants approval.

i. All hardware and software used in conjunction with a web camera must have a USARC CIO/G-6 Certificate to Operate (CTO). Separate requests will be submitted if external webcams are needed.

j. USARC CIO/G-6 prohibits personally owned web camera devices for use on USAR managed networks or for use in official communication.

k. Annually, USAR personnel are required to complete the DoD Cyber Awareness Challenge Training (https://cs.signal.army.mil) and sign an Acceptable Use Policy (AUP).

l. USARC CIO/G-6 enforces the following preventive measures for conference room and office users:

(1) Ensure sensitive or classified information is not displayed on walls within view of the camera(s).

(2) Ensure sensitive or classified information is not placed on a table or desk within view of the camera(s) without proper protection (e.g., a proper cover sheet).

(3) Ensure sensitive or classified information is not read or viewed at such an angle that the camera(s) could focus on the information.

(4) Ensure sensitive or classified information is not discussed, or rendered in any audible medium, in the space in which a laptop camera / microphone is employed.

(5) Turn off computer and peripheral devices used in conference room, video teleconferencing, and kiosk environments when not in use. Turn off computer and peripheral devices when not in use for an extended period of absence such as vacation and holidays.

m. USARC CIO/G-6 may temporarily limit access to Internet-based capabilities to address bandwidth constraints. This includes disabling web camera usage to preserve network bandwidth.

5. Effective Date. This policy is effective upon signature and will remain in effect until revised or superseded by the point of contact.

AFRC-CI
SUBJECT: Use of Web Cameras on United States Army Reserve Managed Network Policy

6. The point of contact for this policy is Mrs. Kimberly Register, Chief, USARC CIO/G-6 Cybersecurity Program Management Division, (910) 570-8653 or kimberly.m.register.civ@mail.mil.

BROWN.TONRI.COREL.1068145550

Digitally signed by BROWN.TONRI.COREL.1068145550
Date: 2020.10.29 15:03:51 -04'00'

Enclosures
1. Exception to Policy Procedure
2. Template ETP Request for Webcam

TONRI C. BROWN
Colonel, GS
Deputy Chief of Staff, G-6

DISTRIBUTION:

MAJOR SUBORDINATE COMMANDS:
1 MSC
3 MCDS
63 RD
-USAG-FHL
75 TNG CMD (MC)
76 ORC
79 TSC
-USAG-FHL
80 TNG CMD (TASS)
81 RD
-USAG-Fort Buchanan
84 TNG CMD (UR)
85 USAR SPT CMD
88 RD
-USAG-Fort McCoy
99 RD
-ASA-Dix
108 TNG CMD (IET)
200 MP CMD
335 SC (T)
377 TSC
412 TEC
416 TEC
807 MCDS
ARAC

AFRC-CI
SUBJECT: Use of Web Cameras on United States Army Reserve Managed Network Policy

ARCD
AR-MEDCOM
LEGAL CMD
MIRC
USACAPOC (A)
USARIC
USAR SPT CMD (1A)

ARECs:
EUSA
USARAF
USARCENT
USAREUR
USARNORTH
USARPAC
USARSOUTH

ARA:
I CORPS
III CORPS
XVIII ABC
USARJ

COPY FURNISH:
7 MSC
9 MSC
311 SC (T)
USARC XOs
USARC DIR/DEP/CH/ASST
OCAR Directors & Deputies


Enclosure 1,
Exception to Policy Pr


Enclosure 2,
Template ETP Reques