DEPARTMENT OF THE AIR FORCE
HEADQUARTERS UNITED STATES AIR FORCE
WASHINGTON, DC

MEMORANDUM FOR AIR FORCE CIVIL ENGINEER CENTER

FROM: HQ USAF/A4
1260 Air Force Pentagon
Washington, DC 20330-1260

SUBJECT: Civil Engineer (CE) Community of Interest Network Version 2 (COIN v2) Comply to Connect Requirements

In an effort to reduce overall risk to the Air Force mission, certain minimum criteria must be met for a device, or system of devices, to connect to the COIN v2.

The list of compulsory requirements for connection to COIN v2 is attached. Failure to meet or exceed these requirements may result in Control System (CS) isolation, which may degrade CS functionality. Isolation can be a necessary resolution to protect the Air Force Information Network (AFIN) from unmitigated risk factors.

If a CS supported by CE COIN v2 cannot meet the requirements for operational or other reasons, a waiver request may be submitted to AFCEC/COOI via email (afcec.comi.icshelpdesk@us.af.mil) for consideration. If a waiver is approved, it may be contingent on employment of additional protection mechanisms to reduce overall risk to the CE COIN, the AFIN, and, ultimately, the Air Force mission.

My point of contact for this matter is Mr. Parrish Smith, AFCEC/COOI, DSN 523-6180 or parrish.smith.2@us.af.mil.

DENTINO.DAVID.H.1126570488
Digitally signed by DENTINO.DAVID.H.1126570488
Date: 2023.06.28 20:01:11 -04'00'

DAVID H. DENTINO, SES, HAF
Authorizing Official, CE Control Systems

Attachment:
CE COIN v2 Connection Requirements

CE COIN v2 CONNECTION REQUIREMENTS

The following items are required for connectivity to CE COIN v2:

- All operating systems (e.g., Microsoft Windows, Red Hat Enterprise Linux, AIX, etc.) must be supported by the vendor.

- All devices with traditional operating systems (e.g., Microsoft Windows, Red Hat Enterprise Linux, AIX, etc.) must meet the requirements below:

  -- Be assigned a public Internet Protocol (IP) address utilizing public IP address space assigned to each deployment location by AFCEC

  -- Must have installed the following:

    --- The current AFCEC-managed and provided endpoint security solution

    --- The Microsoft Endpoint Configuration Manager (MECM) client

    --- Any future capability as defined by AFCEC and approved for deployment by the CE Authorizing Official (AO) or CE COIN Configuration Control Board (CCB)

  -- Must be connected to the network when not in use (e.g., field laptops)

  -- Must become members of the ce.af.mil Active Directory domain

- All servers operating a version of Microsoft Windows Server shall use the corresponding DoD Server Core Configuration (DSCC) image. All workstations operating a version of Microsoft Windows shall use the corresponding Standard Desktop Configuration (SDC) or Long-Term Servicing Channel (LTSC) image.

- Workstations and servers shall be scanned for the presence of malware and potentially unwanted programs with an offline anti-malware scanner provided through the DoD Patch Repository using the latest available virus definitions.

- Workstations and servers shall be scanned using the Security Content Automation Protocol (SCAP) Compliance Checker (SCC) tool and the latest available operating system Security Technical Implementation Guide (STIG) benchmarks. System shall be free of any CAT I vulnerabilities as identified by the benchmark scans.

- All systems must have a valid authorization from the CE AO prior to network connection.

- Network printers must be configured in accordance with the Printer and Multi-Function Device STIG (latest version).

- Network devices (e.g., network switches, network routers, wireless access points, etc.) are prohibited unless managed by either the local base Communications Squadron or AFCEC. Network devices must be part of the Base Area Network (BAN) or COIN, respectively, and NOT part of a supported CS.

CE COIN v2 CONNECTION REQUIREMENTS

- All users are required to utilize two-factor authentication (2FA) using the Common Access Card (CAC) or alternate tokens (Alt Tokens) with a personal identification number (PIN). 2FA will be utilized for both privileged and non-privileged accounts.

- All system owners of CS are required to submit to AFCEC/COOI a full and descriptive Ports, Protocols, and Services Matrix (latest edition) prior to system integration.

- All endpoints shall have the TransVerse application removed due to vulnerabilities.

- Any method and/or device (e.g., modem) used for connectivity outside the Air Force network shall be immediately removed from service.