Annex Q to OPORD 19-025

NETWORK DEFINITIONS AND CATEGORIZATION

The following information provides a general description of the technical aspects of various network connectivity for Information Systems. (Based in part on HQDA EXORD 069-19 Annex A) There are three categories of networks.

INSTRUCTIONS: Enter the APMS # and System Acronym. Network types are separated into 3 categories, each with sub categories. Check the box next to the sub category that applies to the system being submitted.

APMS # and System Acronym

Candidate #15175 - MS365 EDU SFMWR

☐ **1) Standalone Information Systems (SIS)**

☐ a) No Media. Physically separated from all networks and other systems, with no external media devices except a single-purpose printer directly connected to the information system. (Type I SIS)

☐ b) Standalone System with Media. Physically separated from all networks and other systems, but external or removable media are permitted (e.g., USB drive, external hard drive, CD, CD-R, etc.). (Type II SIS)

☐ c) Standalone Network. A collection of computers used to process and exchange information internally, under the control of a single authority and security policy, but not connected to any other system or network (Internet, ISP, DREN, NIPRNet, SIPRNet). (Type III SIS)

☐ **2) Closed Restricted Networks (CRN)**

☐ a) Communicates using DoD-approved encryption, and comply with DISA technical requirements or NSA-approved encryption devices. CRNs also are cryptographically isolated; this means an encryption method that does not allow entry to or exit from the CRN without proper encryption. As an example, a VPN does not qualify for being isolated in this manner.* (Type IV CRN)

☐ **3) Open Networks which have connectivity to other networks, specifically:**

☐ a) Commercial Wired Networks leased. These are generally provided by a telecommunication company like AT&T, Verizon, Telekom or a Cable TV franchise like Comcast, Spectrum, SuddenLink or TKS. Generally uses layer 1 physical infrastructure on the installation or a separate physical plant owned by the contractor. (Type I Open Network (ON))

☐ b) Commercial Wireless Networks leased. These are networks that deliver services using wireless technology provided by telecommunications companies using portable electronic devices like MiFi wireless hotspots, or through service providers that do wired connectivity and then use wireless to distribute the network. Companies like Century Link, Boingo and TKS. Generally uses commercial signal towers to transmit or via a point of presence on the installation to terminate a wired circuit (Type II ON)

☐ c) Government Owned and managed networks. These are networks that are owned managed and secured by an official government agency and usage is approved by the managing activity. Most of these in the Army are managed by NETCOM. Examples (NIPR, SIPR, DREN) (Type III ON)

☐ **4. Software as a Service (SaaS)**

☑ a) Software-as-a-Service (SaaS) allows end users to access software from any device to include but not limited to, desktop, laptop, workstation or mobile device with a web browser and an Internet connection. The software is located on externally hosted server(s) (aka the Cloud) rather than on server(s) located on premises. SaaS is typically provided as a subscription based service, accessed by users logging into the system, using a username and password. Examples of SaaS, include Google Gmail and MS Office 365.

**Closed restricted network requires NIST FIPS 140-2 or NSA-approved device encryption. Logical separation doesn't qualify for CRNs (software-configured, VLAN, VPN, sub-netted, etc.). Type IV also uses cryptography to encrypt data for transport only over other networks. CRNs cannot receive any services from the transport network other than physical transport. The boundary device between the CRN and the transport network must prevent any traffic originating from outside the CRN from interacting with the CRN. Remote administration of a CRN is not authorized. Although VPNs can securely use a public network (i.e., Internet) to transmit, weaknesses exist upon entering and exiting the VPN, which disqualifies a VPN from becoming a CRN. VLANS don't qualify due to the inability to encrypt.*