Defense Health Agency

ADMINISTRATIVE INSTRUCTION

SUBJECT: Video Network Center (VNC) Endpoint Standards

References: See Enclosure 1.

1. <u>PURPOSE</u>. This Defense Health Agency-Administrative Instruction (DHA-AI), based on the authority of References (a) through (c), and in accordance with the guidance of References (d) through (g), provides guidance for video network endpoint standards required for sites to connect to the Defense Health Agency (DHA) VNC network. These standards will help ensure security compliance, efficiency, and best practices are maintained across the DHA network. Meeting certification requirements brings many benefits, including: increased assurances of a successful video teleconference (VTC) experience, full access to bridge and point-to-point calls, and access to peer video networks, including the Department of Veterans Affairs, academia, and industry partners. Compliance with stated standards does not preclude users connecting to other DoD approved networks such as Defense Information Systems Agency Global Video Services.

2. <u>APPLICABILITY</u>. This DHA-AI applies to all of the Defense Health Agency and DHA Components (activities under the authority, direction, and control of DHA).

3. <u>POLICY IMPLEMENTATION</u>. It is DHA's policy, pursuant to References (d) through (g), that all video endpoint devices connecting to the DHA VNC video network will adhere to DHA VNC standards.

4. <u>RESPONSIBILITIES</u>. See Enclosure 2.

5. <u>PROCEDURES</u>. See Enclosure 3.

6. <u>INFORMATION REQUIREMENTS</u>. The DHA Components will provide quarterly reports to the DHA on the status of VTC endpoint compliance efforts by the sites.

7. <u>PROPONENT AND WAIVERS</u>. The proponent of this publication is the Deputy Assistant Director (DAD), Information Operations (IO). When Activities are unable to comply with this publication the activity may request a waiver by providing justification that includes a full analysis of the expected benefits and must include a formal review by the activities senior legal officer. The activity director or senior leader will endorse the waiver request and forward them through their chain of command to the Director, DHA to determine if the waiver may be granted.

8. <u>RELEASABILITY</u>. **Cleared for public release**. This DHA-AI is available on the Internet from the Health.mil site at: <u>https://health.mil/Reference-Center/Policies</u> and is also available to authorized users from the DHA SharePoint site at: <u>https://info.health.mil/cos/admin/pubs/SitePages/Home.aspx</u>.

9. <u>EFFECTIVE DATE</u>. This DHA-AI:

    a. Is effective upon signature.

    b. Will expire 10 years from the date of signature if it has not been reissued or cancelled before this date in accordance with (Reference (c).

/S/
RONALD J. PLACE
LTG, MC, USA
Director

Enclosures
    1. References
    2. Responsibilities
    3. Procedures
Glossary

ENCLOSURE 1

REFERENCES

(a)   DoD Directive 5136.01, "Assistant Secretary of Defense for Health Affairs (ASD(HA))," September 30, 2013, as amended
(b)   DoD Directive 5136.13, "Defense Health Agency (DHA)," September 30, 2013
(c)   DHA-Procedural Instruction 5025.01, "Publication System," August 24, 2018, as amended
(d)   DoD Instruction 8100.04, "DoD Unified Capabilities (UC)," December 9, 2010
(e)   Defense Information Systems Agency Security Technical Implementation Guides [1]
(f)   Video Network Center System Requirements and Information[2]
(g)   Public Law 104-191, Sections 261-264, "Health Insurance Portability and Accountability Act of 1996"
(h)   DoD 6025.18-R, "DoD Health Information Privacy Regulation," January 2003
(i)   DHA-IPM 18-009, "Military Health System (MHS) Enterprise Architecture," September 19, 2018, as amended

---

[1] This reference can be found at: https://iase.disa.mil/stigs/Pages/index.aspx
[2] This reference can be found at: https://vnc.health.mil

ENCLOSURE 2

RESPONSIBILITIES

1. <u>DHA DAD-IO</u>. The DHA DAD-IO will:

    a. Provide overall management and control of the DHA video network to ensure security compliance, efficiency, and best practices are maintained.

    b. Work with the Services to develop and implement a plan to bring all VTC endpoints connecting to the VNC into compliance.

    c. Provide guidance and recommendations for compliant hardware and maintenance requirements.

    d. Assist sites to certify their endpoints when they are installed or upgraded.

    e. Continue to provide VTC bridge access on a case-by-case basis as sites upgrade their equipment.

    f. Maintain a website with current system requirements, a list of compliant systems, technical support, and Frequently Asked Questions.

2. <u>DHA COMPONENTS</u>. The DHA Components will:

    a. Work with the DHA DAD IO to ensure all of their endpoints connecting to the VNC are in compliance with References (d) and (e) and in accordance with the guidance of Reference (f).

    b. Develop a plan for all sites to be compliant or actively working to become compliant within 180 days post publication of this DHA-AI. Endpoints must:

        (1) Be compatible with an internet protocol (IP)-based network.

        (2) Use current equipment on the DoD Approved Products List.

        (3) Be in compliance with latest approved firmware upgrade for Information Assurance compliance.

        (4) Endpoint managers must have assurance of access to manufacturer firmware upgrades. VNC policy (Reference (f)) follows DoD guidance (References (c) and (d)) to ensure a maintenance agreement is in place and activated to provide assurance of network security compliance. The VNC will provide guidance on obtaining vendor-provided agreements; however, it is the endpoint managers' responsibility to procure contracted agreements.

(5) Provide quarterly status checks to the DHA until all sites are compliant.

c. Ensure sites establish maintenance contracts to provide site managers ability to perform required firmware upgrades in accordance with DoD and DHA standards (References (c) through (e)). Normal procurement provide only 1 year of firmware upgrades. A maintenance contract for video endpoints provides assurance of firmware upgrades for the equipment lifecycle.

ENCLOSURE 3

PROCEDURES

All amplifying information and points of contact for the following procedures can be found on the VNC website (https://vnc.health.mil).

1. <u>COMPATIBILITY</u>. Utilize the VNC website (https://vnc.health.mil) to ensure current equipment, or equipment to be purchased, meets DoD network device approval and VNC Enterprise Infrastructure compatibility requirements. Contact the VNC for compatibility verification of endpoints not listed on the VNC website (https://vnc.health.mil).

2. <u>ENDPOINT EQUIPMENT</u>. Contact the VNC to register and certify endpoint equipment with the VNC. In accordance with References (d) through (h):

3. <u>DHA VIDEO NETWORK ENDPOINT STANDARDS</u>. The VNC requires all video endpoints operating on the DHA video network to meet DoD standards for currency, assured security, and sustainment. Further, the VNC uses established best practices and procedures for maintaining the integrity and quality of the video network.

   a. <u>Endpoints</u>. All systems must be current on the DoD Approved Products List and compatible with the VNC Enterprise VTC Infrastructure (see VNC website, or contact VNC for endpoint compatibility verification).

   b. <u>Firmware</u>. Systems must be in compliance with latest approved firmware upgrade for Information Assurance compliance.

   c. <u>Maintenance</u>. In order to provide assurance of firmware upgrades to meet Information Assurance and Cyber compliance, customers must have a maintenance contract in place.

   d. <u>Transport</u>. The VNC operates on an IP-based network. Integrated Services Digital Network transport is not supported by the VNC. Endpoints must be IP compatible.

   e. <u>Compression and Encryption</u>. The VNC network utilizes the highest standards of compression, transport, and encryption for DoD and Health Insurance Portability and Accountability Act support. To meet Health Insurance Portability and Accountability Act standards, the VNC encrypts all network connections.

4. REGISTRATION. All video endpoints must be registered with the VNC for video services. Registration provides client and traversal licensing and connection throughout the DHA video network and through neighbored networks such as the Defense Information Systems Agency Global Video Services, Department of Veterans Affairs and the U.S. Army 7th Signal video network. Users must also ensure compliance with the enterprise architecture. The architecture function will be required to prepare a series of Department of Defense Architecture Framework, i.e., project-specific views of the enterprise architecture that illustrate how the enterprise architecture impacts major projects within the organization in accordance with the guidance of Reference (i).

5. CERTIFICATION. All video endpoints must conduct a one-time certification for multipoint video bridging. Certification is a best practice that provides the highest degree of quality and reduces common errors, issues, and problems. Procedures for certification are found on the VNC website.

6. DECERTIFICATION. Endpoints exhibiting issues or problems that cause interruptions or degrade a multipoint call will be decertified. Once the customer has rectified the issue, the site can re-certify the endpoint with the VNC.

7. EXCEPTIONS. With the understanding that customers may need time to procure new systems, maintenance contracts, or conduct local network approvals for IP-based video, the VNC grants exceptions with the following stipulations:

   a. Customers must provide a plan for compliance with the VNC Chief of Technical Support or VNC Chief of Operations. The plan must include the following:

      (1) Non-compliant endpoint (devices must be within hardware life cycle as identified in Reference (f)). The VNC will not approve access or waivers to endpoints that are not approved for DoD networks or past manufacturers' end of service/support date per Reference (f). These endpoints should be discarded and new equipment procured using host organization's life cycle management procedures.

      (2) Reason for non-compliance.

      (3) Steps taken to become compliant.

      (4) Estimated date of compliance.

   b. The VNC will grant a 90-day waiver for the endpoint(s) via memorandum between the VNC Chief and the site Chief Information Officer or equivalent.

   c. Exceptions are normally for 90 days.

d. Exceptions for longer than 90 days will need DHA DAD-IO approval to extend waiver with the VNC.

e. Endpoints under waiver will be provided access to participate in multi-point calls. However, as with all endpoints, the VNC reserves the right to mute or disconnect any endpoint that is unstable, disruptive, or non-responsive to VNC bridge communication and direction.

GLOSSARY

ABBREVIATIONS AND ACRONYMS

DAD	Deputy Assistant Director
DHA	Defense Health Agency
DHA-AI	Defense Health Agecy-Administrative Instruction
IO	Information Operations
IP	internet protocol
VNC	Video Network Center
VTC	video teleconference