



Joint Task Force National Capital Region Medical INSTRUCTION

NUMBER 8460.02
JUN 20 2012

J-6

SUBJECT: Virtual Private Network (VPN)

References: See Enclosure 1

1. PURPOSE. This Instruction, in accordance with the authority in References (a) through (d), establishes policy on the VPN. Additionally, this Instruction:

a. Provides basic security guidelines for ensuring compliance with DoD access control policies related to the protection of Information Technology (IT) assets, including associated data, hardware, software, and communications.

b. Ensures compliance with DoD policies including, but not limited to, the DoD Security Implementation Guides on Access Control and Secure Remote Computing (References (e) and (f)), as well as National Institute of Standards and Technology Special Publications 800-113, and 800-52 (References (g) and (h)).

2. APPLICABILITY. This Instruction applies to:

a. This Instruction applies to the Joint Task Force National Capital Region Medical (JTF CapMed), JTF CapMed Headquarters, Walter Reed National Military Medical Center (WRNMMC), Fort Belvoir Community Hospital (FBCH) [hereinafter WRNMMC and FBCH are referred to as Medical Treatment Facilities (MTFs)], and the Joint Pathology Center (JPC).

b. All users associated with those facilities.

3. POLICY. It is JTF CapMed policy to:

a. Provide security measures for remote access commensurate with the security requirements of the network. Users requesting JTF CapMed VPN access must:

JUN 20 2012

(1) Utilize only Government-Furnished Equipment (GFE). VPN access from non-GFE (e.g., personally owned machines) is prohibited.

(2) Maintain antivirus updates per the JTF CapMed system image by logging into the VPN every 14 days.

(3) Report to a JTF facility at least once every 60 days and physically connect the machine to the network to ensure receipt of all relevant security updates. There may be circumstances where this is not practical or may require special shipping and coordination of equipment. These situations will be handled on a case-by-case basis by the host MTF or Center Information Security Officer.

(4) Complete annual Information Assurance (IA) and Privacy training appropriate for the position duties as instructed in the JTF CapMed IA training policy and maintain Automated Data Processing Level II Permission.

b. Protect the integrity of the JTF network, JTF CapMed, and the supporting MTFs or the JPC. These MTFs and the JPC shall:

(1) At all times maintain compliance with DoD Security Technical Implementation Guide Recommendations for VPN and Remote Access referenced in this Instruction.

(2) Create a centralized point of access and authentication close to the network edge. Both the accessing device and user must be verified prior to allowing access to network resources on the internal Local Area Network. The remote access servers must be installed outside of the secured private network.

(3) Manage remote access connections with a remote access server placed within the demilitarized zone or within a screened subnet along the VPN gateway.

(4) Employ an Intrusion Detection System at the enclave perimeter.

(5) Employ Router Access Control Lists based on the policy of Deny by Default.

(6) Utilize a Network Access Control Appliance to control access through the VPN.

4. RESPONSIBILITIES. See Enclosure 2

5. PROCEDURES. To obtain VPN access, users require permission from their department head. Users requiring VPN access should complete the JTF CapMed VPN User Agreement Form and the JTF CapMed GFEVPN User Request Form. Completed forms should be submitted to the MTF or Center Information Security Officer.

JUN 20 2012

6. RELEASABILITY UNLIMITED. This Instruction is approved for public release and is available on the Internet from the JTF CapMed Website.

7. EFFECTIVE DATE. This Instruction is effective immediately.



SCOTT WARDELL

Executive Director for Administrative Operations
By direction of the Acting Commander

Enclosures

1. References
2. Responsibilities

JUN 20 2012

ENCLOSURE 1REFERENCES

- (a) Deputy Secretary of Defense Memorandum, "Establishing Authority for Joint Task Force National Capital Region Medical (JTF CapMed) and JTF CapMed Transition Team (Unclassified)," September 12, 2007
- (b) Deputy Secretary of Defense Action Memorandum, "Civilian and Military Personnel Management Structures for the Joint Task Force National Capital Region Medical," January 15, 2009
- (c) Comprehensive Master Plan for the National Capital Region Medical, April 23, 2010
- (d) Supplement to the Comprehensive Master Plan for the National Capital Region Medical, August 31, 2010
- (e) Department of Defense Security Implementation Guide: Access Control in Support of Information Systems Version 2 Release 3, October 29, 2010¹
- (f) Department of Defense Security Implementation Guide: Secure Remote Computing Version 2 Release 5, July 29, 2011²
- (g) National Institute of Standards and Technology (NIST), Special Publication 800-113, "Guide to SSL VPN," July 2008
- (h) National Institute of Standards and Technology (NIST), Special Publication 800-52, "Guidelines for the Selection and Use of Transport Layer Security Implementations," June 2005

¹ Available at Web site: http://iase.disa.mil/stigs/downloads/pdf/u_access%20control_v2r3_stig_20101029.pdf

² Available at Web site:

http://iase.disa.mil/stigs/downloads/zip/u_secure_remote_computing_v2r4_stig_20110128.zip?ArchiveEntry=U_SR_C_STIG_V2R4_Overview.pdf

JUN 20 2012

ENCLOSURE 2

RESPONSIBILITIES

1. JTF CAPMED, CHIEF INFORMATION OFFICER (CIO). The JTF CapMed, CIO shall enforce the components of this VPN policy and ensure its regular update on an annual basis. The JTF CapMed CIO will also provide written approval of the selected VPN software solution prior to its implementation.

2. MTF OR JPC INFORMATION SECURITY OFFICER. The MTF or JPC Information Security Officer shall:

- a. Appoint Network Security officers to manage the VPN solution and ensure continuous enforcement of the policies contained herein.
- b. Establish local policies and procedures for processing VPN access requests and approvals.
- c. Inform the CIO of security policy updates that must be pushed to remote users and implement the update push once VPN users have been notified.
- d. Ensure that VPN users remain compliant with security requirements stated in this policy, Health Insurance Portability and Accountability Act, Privacy Act, and all other DoD IA policies.
- e. Terminate users who violate VPN access agreements or no longer require VPN access.
- f. Inform the JTF Certifying Authority of any security state changes to the network which may impact this VPN policy.
- g. Implement VPN Remote Access solution per written approval.

3. VPN USER. The VPN user shall:

- a. Sign and submit the JTF CapMed VPN User Agreement Form and JTF CapMed GFE VPN User Request Form before receiving the authority to utilize the VPN.
- b. Follow IA best practices when using the VPN in accordance with this policy.
- c. Use only GFE when connecting to the VPN.
- d. Report any lost or stolen GFE to Network Security Officers immediately.
- e. Be subject to consideration for adverse administrative or disciplinary action for failure to comply with this Instruction.