



REPLY TO
ATTENTION OF

DEPARTMENT OF THE ARMY
HEADQUARTERS, V CORPS
UNIT 29355
APO AE 09014

AETV-CS

7 January 2002

MEMORANDUM For Distribution A

SUBJECT: V Corps Digital Rules of Engagement

1. The V Corps Digital Rules of Engagement have been established to provide a baseline for computer network operation in Garrison and Field environments.

2. It is imperative that all Commanders, SA/IMOs and Users understand and comply with the rules established below. Protection of V Corps interests is our top priority and no distinction should be made between personal force protection and data force protection.

3. Listed below is the DROE standard:

a. Computer Certification.

(1) System Administrators and IMO's (personnel with elevated system privileges) must insure that computers connecting to the ANIPR or ASIPR data networks meet the below minimum software requirements:

(a) Operating system must be either Windows 2000 or Windows NT 4.0. Windows 95/98/ME systems may still be used until replaced but not later than May 2002. No Windows 95/98/ME systems will be placed on the ASIPR network. No Windows 95 systems will be given A-NIPR access.

(b) Current service packs are installed (currently SP2 for Windows 2000 and 6a for NT 4.0)

(c) Norton Anti-Virus installed and configured with current virus definition update (latest version is 7.6 build 28).

(d) Internet Explorer 6.0 or IE 5.5 with service pack 2.

(e) RCERT-E security baselines for Windows 2000 and NT are installed.

(f) C4ISR systems not running the above baseline are required to have accreditation packets on file with the V Corps Information Assurance Manager/Computer Network Defense (CND) (COMPUSEC), Mr. Vigil DSN 370-5634, before placing those systems on the network.

AETV-CS
SUBJECT: V Corps Digital Rules of Engagement

This is necessary to cover down on non-standard operating systems and software (i.e. Unix/Linux and Netscape).

(2) Computer will be labeled indicating that they have been certified by the IMO to be placed on the ANIPR or ASIPR. Label will include the following:

Operating System (OS): _____, Service Pack (SP): _____
Antivirus Version: _____, Virus Definition Date: _____
Internet Explorer Version: _____, SP: _____
Certified by: _____, Date: _____

An electronic copy of this label can be found at:

http://www.vcorps.army.mil/G6/ia/Downloads/Computer_Certification_Labels.doc

(3) Computer must have the Green "UNCLASSIFIED" or Red "SECRET" sticker affixed to the PC/laptop. In lieu of the sticker, the SA/IMO may apply the digital version of the UNCLASSIFIED or SECRET stickers as the system wallpaper/background. The SECRET ASIPR PCs must use the SECRET wallpaper. If a user has one system with an UNCLASSIFIED drive and a SECRET drive, then the UNCLASSIFIED and SECRET wallpaper is mandatory. Hard drives not physically stored in the computer must also be labeled appropriately. Unclassified and Classified wallpaper can be found at:

(a) Unclassified:

<http://www.vcorps.army.mil/G6/ia/wallpaper/Unclass/Unclassified.bmp>

(b) Classified:

<http://www.vcorps.army.mil/G6/ia/wallpaper/Secret/Secretwp.bmp>

(4) For computers connecting to the V Corps HQ CP MAIN, TAC and REAR LANs, the organizational IAO will provide a list of certified computers to the G6 Automation Section for assignment of switch ports for those computers to connect to when deployed.

(5) Failure to meet the requirements above will delay/prevent their computers connecting to the network.

b. Force Protection.

(1) Defense in depth. Computers are protected by a layered defense in depth approach. Figure 1 serves as a model providing a better understanding on where V Corps falls into this

model and how IAOs, IMOs, Users and leaders can ensure that their computers are protected.

(2) Network Connectivity. As stated above, IAOs/IMOs must provide a list of computers that meet minimum software baseline standards to their higher automation management section (i.e. MAIN/TAC and REAR clients must have their IAOs/IMOs submit to V Corps G6 Automation their list) before those computers will be allowed to connect to the network.

(3) Road-Side Checks. These checks will occur at random and will check the compliance state of any computer (tactical or garrison) that connects to either the ANIPR or ASIPR networks. Computers found that are not in compliance with established baselines will be immediately disconnected from the network and brought to baseline standard by their IMO before being allowed to reconnect to the network.

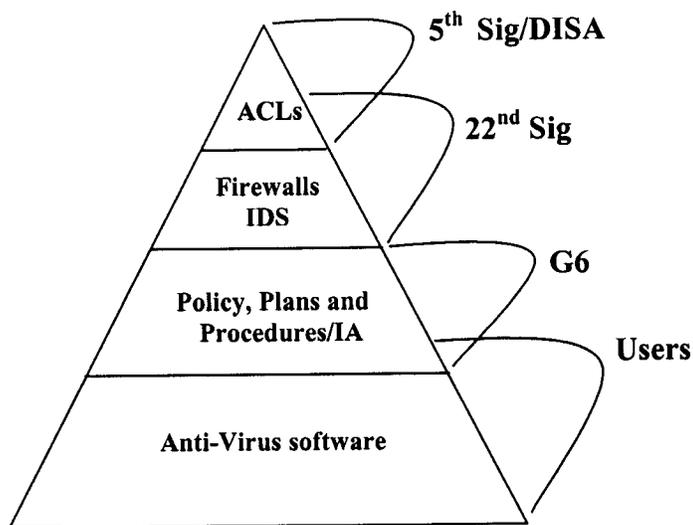


Figure 1. Network Defense in Depth

(4) Passwords. IAOs must ensure strong passwords are implemented at the server and client level. Passwords must be at least 8 characters in length and must include characters from at least 2 of the 4 character sets below.

- UPPERCASE letters from A-Z
- lowercase letter from a-z
- numbers from 0-9
- special characters including !#\$%^&*(), etc.

c. Network Management/Server Administration.

(1) Only the Corps and Divisional Signal units (22nd Signal Brigade, 121 Signal Battalion, 141 Signal Battalion and associated CAMO/DAMO sections) will operate network analysis tools. The Corps G6 CAMO will approve all divisional BATCON's network tools (all software/tools will conform to AR 380-19, Appendix G).

(2) G6 CAMO must approve operation of any Commercial Off-the-Shelf (COTS) software and servers operating on the Corps' tactical network.

(3) Tactical Servers will only be deployed by units not co-located with any of the three Corps CPs (MAIN, TAC and REAR). Units co-located with the Corps CPs will utilize the Exchange and File Servers provided by G6.

(4) All garrison and deployed servers will conform to the security baselines established by RCERT-E at the following links:

(a) For Windows NT Server:

<https://www.rcerte.5sigcmd.army.mil/SecurityConfig/NTsecurity/FtpFiles/WindowsNT4.0SrvandWksBaseline10.pdf>

(b) For Windows 2000 Server:

<https://www.rcerte.5sigcmd.army.mil/SecurityConfig/NTsecurity/FtpFiles/Windows2000SrvandProBaselineVersion1.2.pdf>

d. Network Usage.

(1) E-mail/FTP.

(a) FTP files and email attachments are not to be larger than 1MB. Anything over 1MB will be zipped, not to exceed 1MB. Software to zip all files will be made available by G6 CAMO. Web-based hyperlinked files larger than 1MB will also be zipped.

(b) Software will not be downloaded over the tactical network. Exceptions are packages made available by G6 CAMO on a Corps web page download site. When possible, e-mail messages should contain a hyperlink (hot link) to a zipped file, which can be stored on a file server or web page.

(c) Do not broadcast messages to distribution lists containing "all users." Messages should only be sent to the intended recipients.

(d) All tactical e-mail will be provided via tactical e-mail servers (no reach-back). IMO's need to provide the G6 a list of user names that will reside at each Corps CP to ensure mail from garrison to tactical servers is properly forwarded. Individual reach-back capability for high profile users will be worked on a case-by-case basis.

(2) Web-pages.

(a) Tactical web pages will have a plain white background and be free of any graphics (less operational information).

(b) IMO/Webmasters will verify links and accuracy of information daily.

(c) Only the IMO/Webmaster or designated representative is authorized to post information to web pages. G6 CAMO will grant administrative privileges only to designated IMO/Webmasters.

(d) Additional information on web page design and implementation can be found at the following links:

<http://www.army.mil/webmasters/faq/basic.htm>
<http://www.defenselink.mil/webmasters/>

(3) Video.

(a) No full motion video over the tactical network. G3 will approve exceptions on a case-by-case basis.

(b) No IP based VTC sessions are authorized without G6 approval. IP based VTC sessions (i.e. Netmeeting) that must occur will be limited and scheduled IAW the G3 battle rhythm.

(4) Chat. No network chat software (AOL Instant Messenger, Yahoo Messenger, AKO Messenger...) is authorized for use on the ANIPR network. AKO Messenger is authorized for use only on the ASIPR network.

e. Degraded Network Conditions.

(1) Network conditions and bandwidth constraints may trigger the G6 to implement bandwidth conservation measures/minimization procedures. Once implemented, the following will occur:

(a) Level 1. All personal use of E-mail or web resources will be suspended (i.e. Hotmail and reach-back services will be restricted to mission critical systems).

(b) Level 2. All access to other than “dot mil” domain addresses will be blocked. Only mission essential E-mail attachments will be permitted. Collaborative tools will be restricted to local LAN segments only.

(2) Any other conditions will be issued IAW INFOCONS under established EUCOM directive (see RCERT-E IAPM Web page, Policies and Publications EUCOM Directives).

f. Command Responsibilities. Each IMO has overall responsibility for implementation of the published DROE. G6 (Ops and CAMO) will assist the G3 in enforcement of the DROE at all Corps-level command posts. Therefore, each command, down to battalion level, must designate an Information Assurance Manager/Information Assurance Office (IAM/IAO) representative, IMO or IM NCO and an alternate. Subordinate unit IM representatives are responsible for implementing control measures from the Signal Entrance panel to the inside of their TOCs to support the DROE. These control measures include:

(1) Ensuring their Local Area Network (LAN) is installed properly.

(2) Periodically checking client workstations to ensure compliance with DROE.

(3) Properly utilizing passive network management tools to identify violators on their LAN segment only.

(4) Identifying and eliminating software tools that slow down the network.

(5) Synchronizing their TOC updates around the Corps battle rhythm.

4. Provided below are locations to online resources to allow SA/IMOs to monitor and maintain compliance with established baselines provide in the DROE:

a. Policy and Publications.

<http://www.vcorps.army.mil/G6/ia/default.htm>

<https://www.rcerte.5sigcmd.army.mil/iapmweb/IAPM.htm>

b. Anti-Virus Updates.

<https://www.rcerte.5sigcmd.army.mil/newdefault.asp>

c. Security Baselines.

<https://www.rcerte.5sigcmd.army.mil/SecurityConfig/sectop.htm>

AETV-CS

SUBJECT: V Corps Digital Rules of Engagement

5. This document will be reviewed/updated annually or updated when major changes to baselines or CND policy warrants a change.

6. The POC is MAJ Fox, DSN 370-5645 or e-mail g6automgroff@hq.c5.army.mil.



KENNETH J. QUINLAN

Brigadier General, USA

Chief of Staff