ARMY NATIONAL GUARD

INFORMATION ASSURANCE PROGRAM

POLICY

Date: 31 January 2007

DISCLAIMER

The use of trade names in this document does not constitute an official endorsement or approval of the use of such commercial hardware or software. Do not cite this document for advertising.

CHANGES

Refer any requests for changes to this document to the Designated Approval Authority (DAA) for the Army National Guard (ARNG), Information System Division, Arlington, VA, 22204.

PROTECTION OF INFORMATION INSTRUCTIONS

The contents of this document are considered Sensitive information, which warrants a degree of protection and administrative control in accordance with (IAW) Army Regulation (AR) 25-2. This document's content also meets the criteria for exemption from mandatory public disclosure under the Freedom of Information Act (FOIA), AR 25-55.

DISPOSITION INSTRUCTIONS

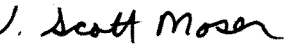
Safeguard this document in a manner that precludes unauthorized personnel from access to its contents. Destroy this document IAW established security guidelines as stated in AR 25-2 and AR 380-5.

ARMY NATIONAL GUARD INFORMATION ASSURANCE PROGRAM POLICY

By Order of the Director Army National Guard:

Clyde A. Vaughn
LTG, Director Army National Guard

Official:



W. SCOTT MOSER
Colonel, GS
G6, Army National Guard

Summary. This Policy provides Information Assurance (IA) policies and mandates procedures for implementing the Army National Guard (ARNG) IA Program. The ARNG IA program will implement the Department of Defense (DoD) IA program, DoD Instruction (DoDI) 8500.2, "Information Assurance Implementation," IAW Army Regulation (AR) 25-2, "Information Assurance" chapter 1 g-8 to support the DoD Information Management Strategic Plan, (IMSP). This Policy supports the Federal Information Security Management Act, (FISMA) 2002 and any other federal guidelines as needed; and shall be consistent with today's technological advancements, in a generic fashion to avoid dependency on specific technology.

This Policy shall:

- Establish policies and assign responsibilities for achieving acceptable levels of Information Assurance in engineering, implementation, operation, and maintenance for all information systems connecting to all ARNG Networks, to include GuardNet Wide Area Network (WAN).
- Provide administrative and systems security requirements, including those for interconnected systems.
- Define and mandate the use of risk assessments and the DoD Defense in Depth Strategy.
- Use the principle of least privilege to ensure that users and administrators get only the access that they require.
- Describe the roles and responsibilities of the individuals who constitute the Information Assurance security community and its users, and outlines training and certification requirements IAW DoDI 8500.2, DoDI 8570.1, and AR 25-2.
- Require a life-cycle management approach to implementing Information Assurance requirements and requires the implementation of a configuration management process IAW AR 70-1.
- Establish a procedure to document the status of generic accreditations for all information systems fielded by the ARNG.
- Establish requirements to ensure that ARNG Designated Approving Authorities (DAAs) meet the system accreditation requirements of this Policy before fielding or testing any system that requires connection to ARNG Networks IAW DoD Directive (DoDD) 8500.1, DoDI 8500.2, DoDI 5200.40, and AR 25-2.

For the purpose of this Policy, the following terms all refer to the Joint Forces Headquarters J-6 (JFHQ J-6) of each State and/or Territories: Director of Information Management (DOIM), Deputy Chief of Staff for Information Management (DCSIM), Chief Information Officer (CIO), or other term used to refer to the Director of Information Management within your State and/or Territories.

Applicability. This Policy applies to all users, information, information systems, and networks connecting to all ARNG Networks. This Policy remains in effect, without change, during mobilization, deployment, or national and state emergency.

Proponent and exception authority.
The proponent for this Policy is the ARNG G6. The proponent has the authority to approve exceptions to this Policy that are consistent with controlling law and regulation. The proponent may delegate this

approval authority, in writing, to an individual within the proponent agency in the grade of Colonel or the Information Assurance Program Manager (IAPM) of the ARNG.

Supplementation. This Policy may be supplemented. If supplemented, it must be coordinated with the ARNG G6.

Exceptions and waivers. Exceptions and waivers to this Policy must be in writing submitted to the ARNG G6.

Interim Changes. Interim changes to this Policy are not official unless authenticated by the ARNG G6. Interim changes will be destroyed on their expiration dates unless sooner rescinded or superseded.

Suggested Improvements. The proponent of this regulation is the ARNG G6. Users are invited to send comments and suggested improvements directly to ARNG G6, ATTN: IAPM, 111 S. George Mason Drive, Arlington, VA 22204-1373.

TABLE OF CONTENTS

INFORMATION INSTRUCTIONS II
ISIGNUTURE INFORMATION III
TABLE OF CONTENTS V
CHAPTER 1 - GENERAL 1
1-1. Purpose. 1
1-2. Objectives 1
1-3. Responsibilities. 1
CHAPTER 2 - ARNG INFORMATION ASSURANCE POLICY 5
2-1. General User Policy 6
2-2. Software Policy 6
2-3. Hardware Policy 9
2-4. Network Security Policy 8
2-5. Minimum Information Assurance Requirements. 10
2-6. Information Assurance Vulnerability Management (IAVM) Policy 11
2-7. Remote Access 12
2-8. Wireless ARNG Networks. 12
2-9. Configuration Requirements. 12
2-10. Virus Protection. 13
2-11. ARNG Network Password Control. 13
2-12. Tactical Systems. 14
2-13. Physical Security Considerations. 14
CHAPTER 3 - CERTIFICATION & ACCREDITATION (C&A), PORT ACTIVATION, AND PROTOCOL PROCESSES 14
3-1. Certification and Accreditation. 14
3-2. Port Activation Process. 15
CHAPTER 4 - PERSONNEL SECURITY 16
4-1. Personnel Security Investigation and Clearance. 16
4-2. Personnel Security Training. 16
CHAPTER 5 – SIPRNET/CLASSIFIED PROCESSING PROCEDURES 16
CHAPTER 6 - INCIDENT REPORTING 18
6-1. Incident and Intrusion Reporting. 18

APPENDICES

APPENDIX A - APPOINTMENT OF INFORMATION ASSURANCE SECURITY OFFICER (IASO) LETTER A-1
APPENDIX B – AUTHORIZED USER AGREEMENT B-1
APPENDIX C – LAPTOP CERTIFICATE OF USE C-1
APPENDIX D– ARNG IAVM REPORTING PROCESS D-1
APPENDIX E – FPA PROCESS E-1
APPENDIX F – INCIDENT RESPONSE PROCEDURES AND FORM F-1
APPENDIX G – GLOSSARY OF ACRONYMS AND DEFINITIONS ..... G-ERROR! BOOKMARK NOT DEFINED.
SECTION I: GLOSSARY OF ACRONYMS G-1
SECTION II: DEFINITIONS G6

CHAPTER 1
GENERAL

1-1. Purpose.
This Policy provides guidance for the ARNG Information Assurance (IA) Program.

1-2. Objectives.
The objective of this Policy is to provide uniform procedures to:

a. Ensure the proper training, resources, equipment, and guidance is provided and implemented for secure access to all ARNG Networks.

b. Ensure ARNG compliance with current National Guard Bureau (NGB), Department of Army (DA), and DoD Regulations and Directives.

1-3. Responsibilities.

a. To provide the most efficient application of the ARNG IA program, the following responsibilities are assigned.

b. ARNG G6 will:

(1) Establish and issue ARNG IA policy and procedures, provide approval of staff/unit IA requirements, and serve as the focal point for ARNG IA and COMSEC programs and funding, IAW AR 25-2 and all DoD IA Directives.

(2) Ensure that all IA support personnel at the enterprise level are appointed on orders for all certification and accreditation positions in the ARNG, to include appointing the Designated Approving Authority (DAA) and Certifying Authority (CA).

(3) Appoint an Information Assurance Program Manager (IAPM) at the enterprise level. This individual will be the ARNG G6's representative for all IA matters.

c. NGB-AIS:

(1) NGB-AIS will:

a. Ensure that all DoD, DA, and ARNG, information assurance, network security, and certification and accreditation policies are implemented into the operational support of ARNG Networks.

(2) AIS-CO Branch Chief will:

a. Ensure that all ARNG network security equipment and applications are configured and implemented IAW DoD, DA, and ARNG policies.

b. Provide help desk support for information assurance and network security of the GuardNet WAN enterprise.

c. Ensure network security task orders are disseminated to all appropriate states and territories.

d. Ensure that ARNG Networks are accredited and certified, IAW DoD and DA instructions and regulations.

e. Ensure that SIPRNET connections for the ARNG are coordinated through the ARNG classified system security manager ((703) 607-7999), as directed in paragraph c of CHAPTER 5 – SIPRNET/CLASSIFIED PROCESSING PROCEDURES of this Policy.

(3) AIS-System Engineering (SE) Branch Chief will:

a. When developing ARNG specific applications, ensure security, certification, and accreditation are incorporated into the applications, as directed by DoD and DA Security Regulations.

b. Ensure that all applications and systems are reported to the DoD and DA applications registrations databases, where applicable.

c. Ensure Enterprise applications and systems within the ARNG are registered with the Army Portfolio Management Solution (APMS) registry/database.

(4) AIS-Configuration Management (CM) will:

a. Ensure certification and accreditation documentation are maintained and available in a repository for all applications and systems that operate on the ARNG Enterprise.

b. Ensure that the DISA Security Technical Implementation Guide (STIG) is available for all application developers within the ARNG enterprise at ***https://iase.disa.mil/techguid/stigs.html***.

d. ARNG State J-6s will:

(1) Appoint on orders the following positions (see Appendix A for appointment letter format) within each State and/or Territories at the appropriate subordinate command armories: Information Assurance Manager (IAM), Information Assurance Network Manager (IANM) or Information Assurance Network Officer (IANO), Information Assurance Security Officer (IASO), and State and/or Territories System or Network Administrators (SA/NA).

(2) Position IA personnel organizationally to provide a balance between the security and operational missions.

(3) Establish data ownership and responsibilities (including accountability, access, and special handling requirements) for each Automated Information Systems as required.

(4) Ensure that copies of these orders (see 1-3d1 above) are forwarded to the ARNG IAPM (NGB-AIP-IA@us.army.mil).

(5) Ensure personnel (listed in 1-3d1) meet the requirements as stated in AR 25-2 (Chapter 3, Army IA Program Personnel Structure) and this Policy, and enter their completed training into Asset & Vulnerability Tracking Resource (A&VTR).

(6) Ensure that all IA personnel receive the necessary technical (e.g. operating system, network, security management, system administration) and security training to carry out their duties and maintain certifications, clearances, entries into A&VTR, IAW AR 25-2 and DoDI 8570.1.

e. ARNG IAPM will :

(1) Be accountable for establishing, managing, and assessing the effectiveness of all aspects of the IA program within the ARNG.

(2) Develop, manage, and maintain a formal IA security program that includes defining the IA personnel structure and ensuring the appointment of that structure at all levels within the ARNG.

(3) Develop, and implement, DoD, DA, and ARNG IA policy.

(4) Ensure that IA personnel receive, review, and implement all IA and security bulletins and advisories that affect the security of their Automated Information Systems.

(5) Serve as the primary point of contact for IA-related actions. This includes Information Assurance Vulnerability Management (IAVM) reporting, compliance, vulnerability assessments, and feedback to the ARNG staff on current and upcoming IA policies.

(6) Provide the ARNG State and/or Territories IA personnel and the NGB-AIS-CO with guidance and priorities.

(7) Provide oversight, guidance, and ensure implementation of the ARNG Certification and Accreditation (C&A) program.

(8) Ensure the development of system C&A documentation by reviewing and endorsing such documentation and recommending action to the ARNG DAA.

(9) Ensure that the IAVM process is implemented per this Policy (see Ch. 2-5).

(10) Ensure DA approved procedures are in place for clearing, purging, and releasing system memory, media, output, and devices.

(11) Ensure that a system is in place to report security violations and incidents to the NGB Integrated Service Center (ISC) (helpdesk@us.army.mil, or 800.821.3097) IAW Ch. 6-1 and APPENDIX H of this Policy.

(12) Establish, conduct, and oversee a command program of announced and unannounced IA assessments.

(13) Administer an IA management control evaluation program separate from, or in support of, Force Protection Assessment Teams (FPATs).

(14) Serve as a member of the ARNG Information Technology Requirements Control Board (ITRCB).

f. State Information Assurance manager (IAM) will:

(1) Not hold any other IT position, within the state, above the level of the IAM position (i.e. DAA, DOIM, DCSIM, J-6, etc.) to ensure there are no conflicts of interest with the security of networks and systems within the command.

(2) Develop, maintain, implement, and enforce a formal IA security and training program.

(3) Implement ARNG IAVM dissemination, reporting, compliance, and verification procedures within the State and/or Territories.

(4) Report security violations and incidents to the NGB ISC (helpdesk@us.army.mil, or 800.821.3097) IAW Ch. 6-1 of this Policy.

(5) Ensure implementation of periodic security inspections, assessments, tests, and reviews.

(6) Manage each States' IANM, IAM, and IASOs, as required, to establish the scope of responsibilities and the technical and security training requirements.

(7) Conduct semi-annual reviews of all Automated Information Systems and networks to ensure no relevant security changes have been made to invalidate the States System Security Authorization Agreement (SSAA).

(8) Negotiate C&A issues with the State and/or Territories DAA, or his or her designated representative, for incoming systems and make recommendations to the State J-6 on acceptance or rejection of Automated Information Systems.

(9) Maintain training and certification records for IA personnel and user IA awareness training, within the State and/or Territories.

(10) Ensure appropriate procedures are in place for clearing, purging, destroying, and releasing system memory, media, and devices within their State and/or Territories, IAW applicable regulations.

(11) Maintain a repository of system C&A documentation and modifications, version control, and management of GOTS, COTS, and non-developmental Items (NDIs) for his or her State and/or Territories.

(12) Ensure that all Automated Information System within the scope of responsibility are properly certified and accredited IAW DoD Information Technology Security Certification and Accreditation Process (DITSCAP/DIACAP) and configuration management policies and practices before operating or authorizing the use of hardware and software on an Automated Information System or network within their State and/or Territories.

(13) Verify that IA personnel are maintaining and auditing access and log data.

(14) Provide policy and guidance to all IAMs/IANMs and IASOs within their State and/or Territories.

(15) Prepare, disseminate, and maintain plans, instructions, and standing operating procedures (SOPs) concerning network security within their State and/or Territories.

(16) Advise the ARNG G6, State J-6, ARNG IAPM, and GuardNet DAA on the use of specific network security mechanisms.

(17) Ensure the ARNG IAVM process is enforced as indicated in Chapter 2-5 and APPENDIX E, of this Policy.

(18) Ensure state specific applications and systems are registered with APMS.

g. State Information Assurance Network Manager or Officer (IANM/IANO) will:

(1) Provide direct support to the State IAM on matters of Computer Network Defense (CND) and the State IA program.

(2) Develop and oversee operational (technical) IA implementation policy and guidelines.

(3) Evaluate threats and vulnerabilities to ascertain the need for additional safeguards.

(4) Assess changes in the network, its operational and support environments, and operational needs that could affect its accreditation.

(5) Ensure procurement actions, installations, and modifications to existing infrastructure comply with ARNG and DA approved IA architectural guidance.

(6) Ensure ARNG Networks within the State and/or Territories for which they are responsible are planned, installed, managed, accredited, maintained, and operated per the security requirements of this Policy, AR 25-1, AR 25-2 and the standards required for connectivity and classification of the network concerned.

(7) Develop and issue network security policy, guidance, and countermeasure implementation instructions to assigned users within the State and/or Territories.

(8) Oversee periodic use of authorized scanning and assessment tools.

(9) Assist the State IAM in monitoring and enforcing the IAVM process within their State and/or Territory.

h. State Information Assurance security officer (IASO).

(1) The same IASO may be appointed for multiple AISs.

(2) An Alternate IASO will be designated and perform the duties of the IASO when the primary is not available for duty.

(3) State IASOs will perform duties IAW AR 25-2 and:

a. Disseminate and ensure implementation of IA policy, guidance, and training requirements within their area of responsibility.

b. Ensure implementation of IAVM dissemination, reporting, and compliance procedures to the State IAM.

c. Report security violations and incidents to the State IAM, and then the NGB ISC (helpdesk@us.army.mil, or 800.821.3097), IAW Ch. 6-1 of this Policy.

d. Serve as the interface between the functional user/unit and the higher Headquarters (HQs) IASO for all IT activities.

e. Notify the State IAM/IANM immediately of any problems encountered with the Automated Information System (e.g., hardware, software, communications, etc.)

f. Request additional hardware/software IAW procedures identified in paragraph 2-2 and 2-3 of this Policy.

g. Provide resource management by:

(1) Ensuring all users are documented, have a "need to know" for the information they are accessing, and have a clearance commensurate with the level of work being done.

(2) Ensuring all users are briefed on security measures and regulations pertaining to proper operation of equipment that processes classified data.

(3) Ensuring proper physical security measures are in place to protect equipment from theft or vandalism.

(4) Maintain a list of computers, peripherals, and devices under their control.

h. Provide user assistance and training by:

(1) Determining what IA assistance and training is needed by users. The IASO will be normally considered the "technical advisor" to the Commander's/Staff Directorate. Day-to-day oversight and coordination with the end users of the system will allow for developing training and assistance requirements to effectively support the users of the system.

(2) Ensure all Automated Information System users in their area of responsibility have taken annual IA training as required, and Authorized User Agreements (AUA) (see Appendix B) are signed and updated annually.

i. State SAs or NAs, and Privileged Users will:

(1) Implement the Automated Information System security guidance policies as directed by the State and/or Territories IAM and perform IASO duties when necessary.

(2) Enforce system access policy, operation, maintenance, and disposition IAW all DA, ARNG, and State and/or Territories local policies and practices.

(3) Report security violations and incidents to the State IAM, and then the NGB ISC (helpdesk@us.army.mil, or 800.821.3097), IAW Ch. 6-1 of this Policy.

(4) Ensure secure configurations include all pertinent patches and fixes by routinely reviewing vendor sites, bulletins, and notifications and proactively updating systems with fixes, patches, definitions, and service packs with the State IAM or ARNG IAPM approval.

(5) Ensure any system changes that result from updating or patching an Automated Information System are documented with the State IAM.

(6) Implement and report IAVM compliance IAW locally established policy to the State IAM.

(7) Review Automated Information System and network logs, and report anomalous or suspicious information to the State IAM, and then the NGB ISC (helpdesk@us.army.mil, or 800.821.3097), IAW Ch. 6-1 of this Policy.

(8) Notify the State IAM or ARNG IAPM when a system no longer processes sensitive or classified information, or when changes occur that might affect C&A, to obtain disposition or resolution instructions.

(9) Establish audit trails, conduct reviews, and create archives as directed by the State IAM.

j. Authorized Users will:

(1) Comply with the guidelines established in AR 25-2 and this Policy when making personal use of government-owned Automated Information Systems.

(2) Participate in initial and annual IA training inclusive of threat identification, physical security, acceptable use policies, malicious content and logic, and non-standard threats such as social engineering.

(3) Mark and safeguard files, output products, and storage media per the classification level and disseminate them to authorized individuals.

(4) Protect Automated Information Systems and Automated Information System peripherals located in their respective areas IAW physical security and data protection requirements.

(5) Practice safe network and Internet operating principles and take no actions that threaten the integrity of the system or network.

(6) Safeguard and report any unexpected or unrecognizable output products to the local IASO, IANM/IANO, IAM, or NGB CND.

(7) Report any software programs received via media (e.g. CD-ROM, USB storage device, floppy disk, etc.) to the IAM or SA, as appropriate, for authorization to use.

(8) Use anti-virus (AV) products on all files, attachments, and media before opening or introducing them into the Automated Information System.

(9) Report all known or suspected security incidents, spam, chain letters, and violations of access as directed in the incident reporting guidance.

(10) Comply with password or pass-phrase policy directives and protect passwords from compromise, IAW AR 25-2.

(11) Adhere to the minimum access control requirements of this Policy (Ch. 2-4 c (7)) at all times.

(12) Access only authorized data, control information, software, hardware, and firmware for which they are authorized access and have a need to know, and assume only authorized roles and privileges.

(13) Have a favorable background investigation, hold a security clearance, or access approvals commensurate with the level of information processed or available on the system, IAW AR 25-2. See Appendix B, Authorized User Agreement.

CHAPTER 2
ARNG INFORMATION ASSURANCE POLICY

2-1. General User Policy.

a. The ARNG G6 has the authority to approve Automated Information System resources in response to mission needs that cannot be economically satisfied by current automation capabilities and which do not duplicate or alter the configuration of existing application systems. Software acquired in support of the above referenced functions will not duplicate present or planned ARNG Standards

Systems or existing ARNG automated systems. Additionally, newly acquired Automated Information System will be compatible with currently installed microcomputer systems. Any automation equipment that either directly or indirectly connects to ARNG Networks must be accredited, certified, and approved in writing, from the State DCSIM/J-6, GuardNet DAA, or ARNG G6.

b. Acceptable Use Policy (AUP). See Appendix B: Authorized User Agreement.

(1) Users will be advised that there is no expectation of privacy while using ARNG Automated Information Systems or accessing ARNG resources.

(2) Users must review and acknowledge the ARNG AUP annually and IASOs will maintain documented records.

(3) DoD policy states that Federal Government communication systems and equipment (including Government-owned telephones, facsimile machines, electronic mail, internet systems, and commercial systems), when use of such systems and equipment is paid for by the Federal Government, will be for official use and authorized purposes only.

(a) Official use includes emergency communications and communications necessary to carry out the business of the Federal Government. Official use can also include other use authorized by a commander for soldiers and civilian employees deployed for extended periods away from home on official business.

(b) Authorized purposes include brief communications by employees while they are traveling on Government business to notify family members of official transportation or schedule changes.

c. Prohibited activities. The following activities are specifically prohibited:

(1) Use of government owned Automated Information Systems for personal commercial gain or illegal activities.

(2) Use of government owned Automated Information Systems in any manner that interferes with official duties, undermines readiness, reflects adversely on the ARNG, or violates standards of ethical conduct.

(3) Intentionally send, store, or propagate sexually explicit, threatening, harassing, political, or unofficial public activity (that is, spam) communications. Law Enforcement and Counterintelligence (LE/CI) investigators, attorneys, or other official activities, operating in their official capacities only, may be exempted from this requirement.

(4) Participate in on-line gambling or other activities inconsistent with public service.

(5) Release, disclose, or alter information without the consent of the data owner.

(6) Attempt to strain, test, circumvent, bypass security mechanisms, or perform network line monitoring or keystroke monitoring.

(7) Modify the system equipment or software, use it in any manner other than its intended purpose, introduce malicious software or code, add user-configurable or unauthorized software (as indicated in 2-2 and 2-3 of this Policy), or download music, video, or other media for personal use.

(8) Relocate or change AIS equipment or the network connectivity of Automated Information System equipment without proper security authorization.

(9) Share personal accounts and passwords or permit the use of unauthorized remote access capabilities by any individual.

(10) Disable or remove security or protective software, or mechanisms, and their associated logs.

d. Classified or Privacy Act Information.

(1) Classified Information: Classified information is not authorized for processing on any unclassified ARNG network. Classified information will only be processed on computers that are accredited for the level of classification required.

(2) Personal Data: All users must safeguard systems with personal data according to the Privacy Act of 1974, Public Law 93-597, and Title 5 USC. The ARNG IAPM will provide guidance to develop and implement Privacy Act operating instructions.

2-2.
Software Policy.

a. Training and maintaining commercial- off-the-shelf (COTS) software is the responsibility of functional users.

b. Software Piracy.

(1) Laws. Users will read and comply with all software license agreements. This includes prohibitions against copying materials (media and manuals) legally protected by copyrights. If multiple copies are needed, they must be purchased.

(2) Shareware. Software distributed under the "Shareware Concept" is still copyrighted and requires purchasing a license to use. Shareware software is not FREE or the same as Public Domain software. Shareware will not be installed on government owned computers. Questions on use of approved software will be directed to the ARNG IAPM.

(3) Freeware, Public Domain Software, and Open Source Software is unauthorized unless approved in writing by their respective DAA, State DCSIM/J-6 or ARNG G6.

(4) Copying. Some licenses allow a user a backup or archival copy of the original media to have on hand in case the program media is damaged. Making copies to share with other computer users, or copying a program at work for personal use, is forbidden.

c. Procedures for Safeguarding Software

(1) Original software will be protected from loss or theft.

2-3. Hardware Policies.

a. Organizational, government owned computers. The government provides computer resources for the accomplishment of official duties. The use of government owned computers in support of private/ personal programs/endeavors are expressly forbidden. Such programs/endeavors are defined to include personal use, use by clubs or other organizations, companies, games, or any other activity, which does not specifically support the daily conduct of business for the ARNG. Violations will be reported through the incident reporting process stated in Ch. 6 of this Policy, and APPENDIX K of the GuardNet SSAA.

b. Prior to connecting to any ARNG network, all Government owned laptops will have a signed certificate of use, per APPENDIX D, and have the latest anti-virus definitions, IAVAs, and security patches, per AR 25-2 and this policy.

c. Laptops connecting to any ARNG network, will not be software firewall enabled; however, when connected to a non-government network (e.g. at a hotel or conference center), laptops will be software firewall enabled.

d. All ISs processing ARNG information in a mobile computing environment shall provide a capability to protect data at rest (DAR) and in transit. This can be accomplished by using "whole disk" encryption tools or "file system" encryption tools, such as Windows XP Encrypting File System (EFS) or third party encryption capability for sensitive or unclassified information as available on the Army Information Assurance Approved Products List (AIAAPL). When EFS is used, be sure to enable encryption on Folders, not just files as all files that are placed in that folder will then be encrypted. Further technical details are available in the Army's BBP for DAR (Data-At-Rest Protection Mobile Devices using EFS Implementation, Version 1.0, 12 Oct 2006)

e. Storage devices (e.g. USB device "thumb drive", external hard drive, external read/write device, etc.).

(1) These devices will only be authorized for NIPRNET use. See Chapter 5 for guidance on SIPRNET use.

(2) Use of these devices is only authorized when the device meets the requirements of the XP STIG (formatted with (New Technology File System (NTFS) , appropriate Access Control Lists (ACLs) on the device, and encryption when they contain sensitive information).

a. The only exception to this policy is within the Visual Information (VI) community, who are authorized to utilize the File Allocation Table File System (FAT16 and FAT32) media devices due to technology not allowing NTFS. At no time will classified or sensitive imagery been stored on any of these devices. This action will be coordinated with the State Information Assurance Manager.

(3) At no time will DoD/FOUO data placed on removal media from a system be allowed to be transferred to a Non-DoD system (I.E. Home System, Contractor System, etc).

f. Personal and contractor owned computers.

(1) The connection of personally owned computers to any ARNG network is strictly forbidden, and there will be no government sensitive information on personally owned systems.

(2) Contractor owned computers, specified in the contract statement of work, may be permitted when approved by the appropriate DAA and are subject to ARNG configuration management policies.

(3) Use of personally owned computers is authorized if work is conducted through a VPN solution, and the computer meets the security requirements of this policy and all DoD and DA policies for use on a DoD Network.

2-4. Network Security Policy.

The following policy applies to all ARNG Networks, to include the GuardNet WAN, and any ARNG networks for future use. All requirements as described in AR 25-2, chapters 4-19 Cross-Domain Security Interoperability and Chapter 4-20 Network Security, will be adhered to in addition to the following.

a. Restrictions. Users, IAMs, and State J-6s will:

(1) Ensure transmission of classified or sensitive information via applicable secure means.

(2) Manage authorized commercial ISP connections, and ensure that those connections do not touch the NIPRNET or SIPRNET.

(3) Prohibit cross-connections directly between the Internet and NIPRNET of Automated Information Systems. For example, do not permit a multifunction device (copier/fax, printer/scanner) with a modem, to connect to a commercial ISP or service, while the Automated Information System is also connected to the NIPRNET.

(4) Ensure all non-organic Automated Information Systems have accreditation documentation when connecting to any ARNG network.

b. The DA policy (ALARCT 225/05 NETPROTECT) on network defense requirements promulgates network security incidents due to improperly configured systems. The increased interconnectivity of application and services, information technology (IT) assets that are non compliant with the latest information assurance vulnerability alerts (IAVA) or that do not have the most recent antivirus signature files pose a risk to the Army's global network. The DOIM is the State or Territory information manager and is required to periodically scan all State or Territory assets and devices, implement protective measures, and report non-compliance in order to ensure the highest degree of compliance with computer network defense requirements at the State or Territory level. Review and comply with the NETPROTECT policy letter (26 May 2006), as the following tenant responsibilities in the policy state:

(1) "Each tenant in the State or Territory that is connected to GuardNet will provide their DOIM with local administrator access to all IT assets to be scanned."

(2) "No tenant will block a scanning or enterprise systems management (ESM) tool used by the State DOIM/J6 to verify IAVA or antivirus compliance."

c. Security protection between enclaves (that portion of the network outside of GuardNet). Utilize the following processes on routers, switches, firewalls, and other networking devices to provide protection from external networks.

(1) Firewalls. Utilize and configure firewalls with least-privilege access controls. Layer firewalls at the boundaries between border and external networks and as needed throughout the architecture to improve the level of assurance. NGB CND will approve firewall implementation guidance for use within the GuardNet .

(2) Ports, Protocols, and Services (PPSs). Permit only ports, protocols, and services as authorized by applicable authority. DoDI 8551.1

a. ARNG Enterprise and Enclave boundary firewalls and firewall-like devices will restrict the use of ports, protocols, and services IAW APPENDIX I-19 of the GuardNet SSAA, and DoD Ports, Protocols, and Services (PPS) Assurance Category Assignment List (CAL). The DoD

PPS Assurance CAL is posted on the DISA website (http://iase.disa.mil/ports/index.html), and NGB considers PPSs not listed on the DoD PPS Assurance CAL as "deny by default".

b. PPSs designated as "high-risk" are unacceptable for routine use. Prohibit high-risk PPSs unless expressly approved by NGB-AIS-CO for a specific implementation with defined conditions and risk mitigation strategies.

c. PPSs designated as "medium-risk" have an acceptable level of risk for routine use when used with required mitigation strategies.

d. PPSs designated as "low-risk" are recommended as best security practices and advocated for use by DoD. Not all low-risk PPSs are acceptable under all implementations and may require approval.

e. NGB-AIS is responsible for PPS for the ARNG management and will approve and publish Army-wide mitigation strategies for PPSs.

(3) Domain Controllers (DCs). NGB-AIS-CO monitors DCs for compliance and adherence to DC policies. NGB-AIS-CO provides network-based intrusion detection monitoring for GuardNet .

(4) Virtual private networks (VPNs). VPNs across GuardNet requires an approval from the GuardNet DAA. For further information, see the APPENDIX I-19 of the GuardNet SSAA.

d. Protection of internal networks (portion of the network that is directly controlled by NGB CND).

(1) Establish trusts IAW GuardNet C&A. There will be no trusted relationships established with any other domains or networks until approved by GuardNet DAA or the ARNG G6.

a. The DAAs of the participating domains or networks will sign a Memorandum of Understanding (MOU) or Memorandum of Agreement (MOA).

b. The DAA's approval will include a description of the classification and categories of information that can be sent over the respective networks.

(2) Connection between accredited Automated Information Systems must be consistent with the sensitivity level and any other restrictions imposed by the accredited Automated Information Systems. Unless the Automated Information System is accredited for multilevel operations and can reliably separate and label data, the Automated Information System is assumed to be transmitting the highest level of data present on the system during network connection.

(3) Employ identification, authentication, and encryption technologies when accessing network devices.

(4) Employ layered protective, filtering, and monitoring devices (e.g., firewalls and/or IDSs) at enclave boundaries, managed access points, and key connection points.

(5) Periodically scan all external connections to GuardNet , implement protective measures, and report non-compliance as required.

(6) GuardNet internet access will be monitored through NGB CND.

e. E-mail security. ARNG E-mail systems and the use of those systems will be IAW AR 25-2, Paragraph 4-20.

f. Internet, Intranet, Extranet, and WWW security.

(1) Users are authorized to download Government approved programs, graphics, and textual information to a Government-owned Automated Information System, as long as doing so does not violate DoD, DA, and NGB regulations, acceptable use, and local policies.

(2) Extranet and intranet servers will provide encryption and user authentication, as directed in AR 25-2 (para. 4-20 g (8), Network Security), or Better Business Practices (BBPs).

(3) Extranet servers and access will be approved through the GuardNet and/or State IAM, and respective DAA.

(4) All Automated Information Systems that connect to publicly accessible networks, such as the Internet, will employ a combination of access and security controls (e.g. firewalls, access controls, routers, host-based Intrusion Detection Systems (IDSs)) to ensure the integrity, confidentiality, accessibility, and availability of all Automated Information Systems and data.

(5) ARNG State IAMs and/or J-6s are responsible for complying with Federal, DoD, and DA Web site administration policies and implementing content-approval procedures that include OPSEC and PAO reviews before updating or posting information on public Web sites.

(6) Protect publicly accessible DoD Web sites by placing them behind a reverse Web proxy server.

(7) All private (non-public) Web sites that restrict access with password protection or specific address filtering are required to implement Secure Sockets Layer (SSL) protocols utilizing a Class 3 DoD Public Key Infrastructure (PKI) certificate as a minimum. NGB-AIS/NETCOM issues and manages these certificates.

(8) ARNG State IAMs and J-6s will periodically review OPSEC requirements of all organizational Web sites.

g. Information Assurance tools. Use only IA security software listed on the IA Tools list on Army systems and networks. The list of Army approved IA tools is available through the Army Computer Emergency Reaction Team (ACERT) or the Communcation Security Logistical Agency (CSLA) Web site. Requests for consideration and approval for additional security software packages to be added to the Army IA tools list must be submitted through NETCOM channels ATTN: NETC–EST–A, ATTN: IAD to G–6.

(1) State J-6 IAM-designated and Army-certified IA personnel may conduct network vulnerability scans and tests under stringent conditions coordinated (at a minimum) with the State J-6, IAM, and NGB CND.

(2) ARNG IAPM approval, and advance notification to the servicing NOSC, is required before certified IA personnel may utilize public domain vulnerability assessment tools.

(3) IA personnel are prohibited from conducting penetration testing or attempts on Automated Information Systems utilizing hacker tools or techniques. This restriction is applicable to operational networks and does not apply to those personnel or techniques used in a testing environment for C&A, vulnerability assessments of developmental systems, or used in a training environment for personnel certifications on isolated networks.

(4) State IAMs can request penetration testing of their State and/or Territories networks through the NGB-AIS-CO.

h. Other tools. Other tools employed by the Army include:

(1) Vulnerability scanners. Only individuals trained and certified will use assessment software. Before conducting mapping or scanning of a network, the IAM must notify the State J-6 and the NGB-AIS-CO with the purpose, start, and duration of the scanning activity. The only exception to this is IAVA scanning tools authorized by DoD/DA for scanning IAVA compliance (e.g., Retina, Harris STAT, etc.).

(2) Scan results will be provided to NGB CND, ARNG IAPM, and ARNG G6.

(3) Lack of expertise. State J6 Staff that do not have the expertise, requisite certification level, or resources to scan their own networks may request a vulnerability scan through the NGB-AIS-CO.

(4) Unauthorized scans. Treat unauthorized scans of networks as potential intrusions and report upon detection to the NGB-AIS-CO. Persons conducting unauthorized scans of ARNG, DA, and DoD networks may be subject to administrative actions or punishment, IAW UCMJ, or civil authority.

2-5. Minimum Information Assurance Requirements.

a. Configure Automated Information Systems to implement the principle of least privilege through automated or manual means. All risk will be evaluated for possible vulnerabilities and adverse security effects on the associated Automated Information Systems and networks within the appropriate areas of responsibility. Although manual procedures are acceptable when an automated safeguard is not feasible, embed automated security safeguards into the design and acquisition of new or updated Automated Information Systems to ensure a secure infrastructure. Employ technical capabilities to achieve these requirements to the greatest extent possible.

b. All ARNG networks will be secured according to DoD, Army, and ARNG Network Infrastructure regulations and DISA STIGs prior to being allowed to connect to the GuardNet XXI WAN.

c. Access control. Implement controls to protect Automated Information Systems from compromise, unauthorized use or access, and manipulation. IA personnel will immediately report unauthorized

accesses or attempts of such systems to the State IAM, and then the NGB ISC (helpdesk@us.army.mil, or 800.821.3097), IAW Ch. 6-1 of this Policy.

(1) All ARNG systems will validate that systems authenticate users through the use of the Common Access Card (CAC) as a two-factor authentication mechanism. The CAC has certificates on the Integrated Circuit Chip (ICC), and will be used as the primary user identifier and access authenticator to systems.

(2) Access to ARNG Automated Information Systems or networks is a revocable privilege.

(3) Approval processes will be developed and determined for specific groups and users.

(4) Individuals will meet security investigation (or approved interim access) requirements before Automated Information System access.

(5) Systems will automatically generate an auditable record or log entry for each access granted or attempted.

(6) Identify all users through unique user identification (USERID).

(7) Authenticate user access to all systems with a minimum of a USERID and an authenticator. An authenticator may be something the user knows (password), something the user possesses (token), or a physical characteristic (biometric). The most common authenticator is a password.

(8) Lock the workstation if you intend to leave the workstation for more than 3 minutes; password-protect screen savers, screen locks, or other lockout features to prevent unauthorized access on all Automated Information Systems during periods of temporary non-use; configure such mechanisms to automatically activate when a terminal is left unattended for no longer than 10 minutes (establish a shorter period if appropriate). Log off of Automated Information Systems at the end of each workday, but do not power down the Automated Information System, so security patches can be updated during non-duty hours.

(9) The use of group accounts is generally prohibited. Permit exceptions only on a case-by-case basis that support an operational or administrative requirement such as Network Security Operations helpdesk accounts, or that permit continuity of operations, functions, or capabilities. IAMs will implement procedures to identify and audit users of group accounts through other operational mechanisms such as a duty logs.

(10) Limit the number of user failed log-on attempts to three before denying access (locking) to that account.

(11) A security alert will be generated and investigated when the maximum number of password attempts is exceeded.

(12) Access will be reinstated only after the appropriate IA (e.g., SA/NA) personnel have verified the reason for failed log-on attempts, and have confirmed the access-holder's identity.

(13) Password reset tools are only authorized for specific operating systems, as listed on the ACERT website (https://www.acert.1stiocmd.army.mil/tools/).

(14) Implement mandatory audit trails to record all successful and unsuccessful log-on attempts.

(15) Disable all accounts on ARNG/State networks of deploying for longer than 60 days.

(16) Ensure all deployed soldiers cancels forwarding of Army Knowledge Online email accounts while deployed.

(17) All accounts that do not meet the 60 day password change requirement will be removed/deleted.

(18) Enable, log, and protect physical access control events (e.g., card reader accesses) and audit event logs for physical security violations or access controls to support investigative efforts as required.

2-6. Information Assurance Vulnerability Management (IAVM) Policy.

a. All current and future-connected ARNG networks that are used to enter, process, store, display, or transmit information, regardless of classification or sensitivity will adhere to the policy outlined in the IAVM process documented in APPENDIX E in this Policy.

b. Reporting. All state ARNG IAVM policy and compliance matters will be reported to the ARNG IAPM/IAVM Manager according APPENDIX E in this Policy.

c. Responsibilities. The ARNG IAPM will be the Point of Contact (POC) to acknowledge receipt (within five days) of DoD Computer Network Defense (CND) issued IAVMs, aggregate compliance and waiver data, and report (within 30 days or as directed) to DA.

d. All ARNG State IAMs will acknowledge receipt of all IAVBs and IAVAs through Asset and Vulnerability Tracking Resource (A&VTR). All ARNG State IAMs will report compliancy of all IAVAs to A&VTR and the ARNG IAVA Manager, by the suspense date indicated on the IAVA.

e. Until all states have the capability to report properly to A&VTR, follow directions in APPENDIX E (Para. 6: Interim Compliance Verification Reporting).

f. Systems and processes for collecting detailed information and for implementing IAVM are the responsibility of every IA person.

g. Asset and Vulnerability Tracking Resource.

(1) An Army Knowledge Online (AKO) account is required to initially log into Asset and Vulnerability Tracking Resource (A&VTR). All users are required to have an AKO account. IAMs should request an A&VTR account on the A&VTR login page. The current A&VTR web addresses is: https://newia.us.army.mil.

(2) Approval of all A&VTR accounts will be made by the ARNG IAVA Manager. Any questions or concerns can be addressed to the ARNG IAVA Manager.

2-7. Remote Access (RA)

a. Any Automated Information System being used for remote access will employ host-based security and AV software before authorization to connect to any remote access server.

b. Encrypt log-in credentials as they traverse the network as required for the level of information being accessed or required for need-to-know separation.

c. Encrypt all RA for network configuration or management activities regardless of classification level, device, or access method.

d. Disable remote device password save-functions incorporated within software or applications to prevent storage of plain text passwords.

e. Remote access users will read and sign security and end-user agreements for remote access annually as a condition for continued access. This will be accomplished through the AUP process.

2-8. Wireless ARNG Networks.

All personal, local, metropolitan, or wide area wireless Automated Information Systems (computers, Personal Electronic Devices (PEDs), etc.) that connect to any ARNG network, will be approved by the local and/or ARNG DAA, and meet the following minimum configuration and security requirements:

a. DoDD 8100.2

b. DoDD 8500.1

c. AR 25-2, Chapter 4-29

d. The Army Better Business Practices (BBPs) (22 June 2004) requirements, outlined in sections 8 & 11.

e. DISA Wireless Security Technical Implementation Guides (STIGs)

2-9. Configuration Requirements. The following policy will be the minimum used for the configuration management of all ARNG systems.

a. Hardware and software changes to accredited Automated Information Systems with an established baseline will be documented through the configuration management process.

b. The Configuration Control Board (CCB) or the Configuration Management Board (CMB) for a site must approve modifying or reconfiguring the hardware of any computer system. Hardware will not be connected to any ARNG system or network without the express written consent of the IAPM and the CMB or CCB. In the absence of a CCB or CMB, the appropriate DAA or IAM will provide the consent.

2-10. Virus Protection. Implement the virus protection guidance provided below on all ARNG Automated Information Systems and networks, regardless of classification or purpose.

a. Scan all files and software, including new "shrink-wrapped" COTS software, with an AV product before introducing them onto any ARNG Automated Information System or network.

b. To minimize the risks of viruses, implement the following countermeasures.

(1) Ensure all Automated Information Systems have a current enterprise authorized version of the AV software provided by the Army, and configured to provide real-time protection.

(2) Install an AV product for every remote access Automated Information System.

(3) IA personnel should take the multilevel approach to virus detection by installing one AV package on the workstations and a different AV package on the servers.

(4) Update virus definitions as a minimum weekly, or as directed by the Army CERT (ACERT) for immediate threat reduction. Virus definition availability is based on vendors' capabilities, and IA personnel will institute processes to automatically update definitions as published or available from authorized DoD or Army sites.

(5) Train users to scan all software, downloaded files, and e-mail attachments to prevent malicious logic installation.

(6) Train users to recognize and report virus symptoms immediately, and take actions as directed in Ch. 6 (Incident Reporting) of this Policy.

c. IAMs will implement virus-reporting procedures to support DoD, DA, and ARNG reporting requirements.

2-11. ARNG Network Password Control.

a. The State IAM or designee is responsible for overseeing the password generation, issuance, and control process.

b. Implement two-factor authentication techniques as the access control mechanism in lieu of passwords. Use CAC as the primary access credential, or biometric or single-sign on access control devices only when the IS does not support CAC

c. The holder of a password is the only authorized user of that password.

d. All users must change passwords IAW AR 25-2 (60 days).

e. Configure Automated Information Systems to prevent displaying passwords in the clear.

f. Generate passwords as follows:

(1) The minimum requirement is a 10-character case-sensitive password. Passwords or phrases longer than 10 characters are recommended when supported by the Automated Information System. Password expiration will not be more than 60 days.

(2) The password will be a mix of uppercase letters, lowercase letters, numbers, and special characters, including at least two of each of the four types of characters (e.g., x$TIoTBn2!) and can be user generated.

(3) Enforce password policy through implementation or enhancement of native security mechanisms.

(4) Passwords should not include such references as social security account numbers (SSAN), birthdays, USERIDs, names, slang, military acronyms, call signs, dictionary words, consecutive or repetitive characters, system identification, or names; neither will they be easy to guess (e.g. MYpassword12#$, ABcdel234%^, etc.).

(5) Password history configurations will prevent reutilization of the last 10 passwords when technically possible. State IAMs, will approve and manage procedures to audit password files and user accounts for weak passwords, inactivity, and change history. Conduct quarterly auditing of password files on a stand-alone, secured system with limited access. Encrypt password files for transit if auditing at a centralized location.

g. Deployed and tactical systems with limited data input capabilities will incorporate password control measures to the extent possible.

h. Implement other authentication techniques (e.g., biometrics, access control devices, or smart cards) as viable alternatives in conjunction with passwords as tested or approved by Army Network Enterprise Technology Command/9th Army Signal Command (NETCOM) and G6.

i. Remove or change default, system, factory installed, function-key embedded, or maintenance passwords.

j. Unauthorized scans. Treat unauthorized scans of networks as potential intrusions and report upon detection. Report any detection of such scans as stated in Ch. 7 (Incident Reporting).

2-12. Tactical Systems.

a. Tactical systems, including first responder communication systems. (e.g. ISISCS or JISCC) or weapon systems and devices, or integral to weapon or weapon support systems, that include features normally associated with an Automated Information System will implement the requirements of this regulation and DoDI 5200.40 (DITSCAP/DIACAP).

b. Tactical networks connecting to ARNG networks must be compliant with all security requirements (e.g., configurations, approved software, C&A, IAVAs) before connection. They will be protected by access controls and intrusion detection systems in the same manner.

2-13. Physical Security Considerations.

a. General. All computer areas will be secured upon the completion of the duty day or at any time the facility is unoccupied, such as during a fire drill, bomb threat, etc. Only authorized users are allowed to use hardware in conjunction with his/her duties. Double barrier security for Automated Information System should be provided wherever possible.

b. Security of CPU, Printer, and Keyboard. Computer equipment must be secured by a minimum single barrier security when left unattended. LOCKED doors will, at a minimum, secure the Automated Information System and any peripherals at the end of the duty day.

c. Use of government-owned computers at homes or other facilities is authorized providing the following:

(1) Work on the systems must be for official use only.

(2) No software will be installed to allow connection to the internet (i.e. AOL, SBC-Yahoo, etc) and the minimum IA requirements outlined in 2-3a are adhered to.

(3) Anything introduced or produced on the system becomes property of the ARNG.

(4) No IT or IT resources shall be left unsecured.

(5) Use of wireless devices must meet all requirements as outlined in Section 2-8 of this Policy.

CHAPTER 3
CERTIFICATION & ACCREDITATION (C&A), PORT ACTIVATION, AND PROTOCOL PROCESSES

3-1. Certification and Accreditation.

a. C&A of all ARNG Automated Information Systems will be IAW AR 25-2, AR 73-1, all DA IA BBPs, DoD Directives 8500.1, 8500.2, and 5220.22, DoD Instructions 8500.2 & 5200.40, DoD Manuals 8510.1-M, 5220.22M, and DoD 5220.22–M–SUP, P.L. FISMA Act 2003, and OMB Circular A–130.

b. Before any application or system may connect to any ARNG Network and GuardNet WAN, it must obtain an ARNG Certificate to Operate (CTO). The process for attaining a CTO is given in App. I of this Policy.

c. Certification. Security certification is a comprehensive evaluation of the technical and non-technical security features of an Automated Information System and other safeguards made in support of the accreditation process. It establishes the extent to which a particular design and implementation meets a set of specific security requirements.

d. Tailoring. The time and labor expended in the C&A process must be proportional to the system size, criticality, and mode of operation, data sensitivity, and number of users. The activities defined in the four phases of the DITSCAP/DIACAP are mandatory. However, tailor implementation details of these activities and, where applicable, integrate with other acquisition activities and documentation.

e. Accreditation. Accreditation is the official management authorization to operate an Automated Information System or network and is based, in part, on the formal certification of the degree to which a system meets a prescribed set of security requirements.

(1) Accreditation documentation.

a. The Authority To Operate (ATO) or the Interim Approval To Operate (IATO) and complete C&A documentation for all Enterprise ARNG, DA, and DoD Automated Information Systems will be forwarded to the ARNG IAPM for review.

b. Upon acceptance, the ARNG IAPM will publish an IATO or ATO memorandum with the DAA's signature.

c. If an IATO or ATO is already present and meets security requirements after review by the ARNG IAPM, an ARNG CTO will be issued IAW the ARNG CTO process, as indicted APPENDIX F of this Policy.

(2) Re-accreditation. All Automated Information Systems will be re-accredited within three years of its latest C&A. Re-accreditation procedures will begin at six months prior to the end of the expiration date of the ATO.

(3) If none of the events listed below has occurred, this re-accreditation may consist of a simple review and update of the accreditation documentation. A completely new or updated accreditation is required beginning with Phase 1 of the DITSCAP/DIACAP process if any of the following events occurs—

a. Addition or replacement of a major component or a significant part of a major system.

b. A change in classification level of information processed.

c. A change in security mode of operation.

d. A change in interfacing systems.

e. A significant change to the operating system or executive software.

f. A breach of security, violation of system integrity, or any unusual situation that appears to invalidate the accreditation.

g. A significant change to the physical structure housing the Automated Information System or environment of the Automated Information System that could affect the physical security described in the accreditation.

h. A significant change to the threat that could adversely affect Army systems.

i. A significant change to the availability of safeguards.

j. A significant change to the user population.

f. Designated Approving Authority. A DAA will be appointed for every application and network.

(1) The ARNG DAA, appointed on orders by the DA G6, will be a General Officer (GO) for all ARNG enterprise applications and systems.

(2) The ARNG DAA will appoint all State J-6 as the DAA for their State and/or Territories. If the J-6 does not fill this position, then a GO from each respective State and/or Territories will.

(3) The Director, Defense Intelligence Agency (DIA), is the DAA for those systems processing SCI with connection to the Joint Worldwide Intelligence Communications System (JWICS).

3-2. Firewall Port Activation (FPA) Process. See APPENDIX G: FPA Process.

a. The purpose of the FPA Process is to control ports and protocols and to ensure that NGB-AIS personnel are protecting the GuardNet WAN from internal and external threats using vulnerable ports and protocols as access to the network.

b. FPA Process for installing new ARNG-managed or NGB CND managed firewalls, and modifying existing NGB CND-managed firewalls. ARNG users may request changes in configuration of the NGB CND-managed firewalls that are not under current configuration baseline. They must submit a

request to their DOIM with the information necessary for the DOIM POC to forward the FPA change to the NGB ISC helpdesk. When submitting an FPA change/request, the following criteria must be met:

(1) Installed firewalls that have not been reported shall follow the reporting process for new ARNG-managed firewalls and NGB CND-managed firewalls.

(2) New ARNG-managed firewalls shall be reported to NGB-AIS-CO.

(3) ARNG organizations requesting modifications to current NGB CND-managed firewalls shall complete and submit the NGB FPA form to NGB-AIS-CO, via NGB ISC Helpdesk. See Appendix G of this policy for the sample of FPA form. Examples of a reportable change or modification include:

a. New releases of OS or firewall software

b. New firewall hardware

c. New protocols and services through the firewall, support for additional security functionality on the firewall (e.g., use of hardware tokens, VPNs, third-party products)

d. Implementation of additional devices or computer systems that provide supplemental firewall services

CHAPTER 4
PERSONNEL SECURITY

4-1. Personnel Security Investigation and Clearance.

All personnel requiring access to any ARNG Network shall meet the requirements stated in AR 25-2, Section V.

4-2. Personnel Security Training.

a. All new users will take and pass the user security training. Users will accomplish this training via one of two options:

(1) Utilize a designated workstation to complete the User Security Awareness training. Upon completion, users will be issued an account username/password.

(2) Assign user an account username/password set to expire in 5 business days after creation, unless the user completes the User Security Awareness training on line, or by approved method.

(3) This training can be conducted through online training through the Fort Gordon, GA website (http://ia.gordon.army.mil/ia_courses.htm) or one generated at the State and/or Territories level.

b. All IA User training will be documented and maintained by the state IAM/IANM/IASO as directed by the State IA Policy.

c. All IA support personnel will follow DoDD 8570.1, AR 25-2 (Ch.4-3), and the guidelines set forth in the DA BBP for IA Training Guide, V1.0, (05-PR-M-0002, dated 13 SEP 2005); specifically, numbers 8 & 11.

CHAPTER 5
SIPRNET/CLASSIFIED PROCESSING PROCEDURES

a. The level of protective measures applied to all Automated Information Systems should be commensurate with the environment and sensitivity of information being processed at all times.

b. The users of Automated Information Systems are responsible for the physical security and environmental safeguards for the equipment, media, and data processed. They shall properly secure sensitive information and media to protect against unauthorized access, destruction, or damage.

c. The States SIPRNET IASO will ensure that all classified Automated Information Systems are properly prepared for processing at the level of classified information required.

d. Protection

(1) Personal Security. Positive controls must be established over all personnel with access to remote access devices and adjacent areas. More restricted access controls must be imposed over the locations holding the SIPRNET servers.

(2) Physical Security. Any area operating SIPRNET equipment must be equipped with an Automated Entry Control System (AECS), or a cipher lock to control admittance, installed in accordance with paragraph 8, Appendix G, DOD Regulation 5200.1-R/AR 380-5. All SIPRNET equipment will be protected at the Secret level in accordance with DOD 5200.1-R/AR 380-5.

(3) Terminal Area Workstations, Non-Removable Hard Drives, Secure Laptops. SIPRNET and Global Command and Control System (GCCS) workstations with non-removable hard drives and not under the personal control of an authorized user 24 hours every day shall be guarded or stored in a locked security container, vault, room, or area as outlined in DOD 5200.1-R/AR 380-5, Chapter 6 and in Annex C.

(4) SIPRNET Terminal Access. Access to the SIPRNET terminals will be restricted to registered SIPRNET users. A terminal access roster shall be posted within two feet of the terminal. Access rosters shall be updated every three months, as a minimum, by the site IASO and a copy provided to the SIPRNET IASO.

(5) Equipment Location. The SIPRNET terminal equipment (e.g., terminals, monitors, printers) must be positioned to preclude inadvertent disclosure of information being processed or displayed to individuals without a valid need-to-know for the information. No terminal shall be relocated without prior coordination, which will require a site survey for approval. The site IASO is responsible for coordinating any relocation of SIPRNET equipment within their assigned area.

e. Removable media on classified systems.

(1) At this time, the use of any removal media device is unauthorized on any Classified/SIPRNET network unless a waiver is approved by the GuardNet XXI DAA, ARNG G6, or State/Local DAA.

(2) Data that is to be moved by these devices potentially impose a security risk or spillage of classified material onto the unclassified network if not properly managed within applicable regulations.

(3) At no time will USB Flash/Thumb Drives be authorized for use on any ARNG Classified/SIPRNET system without an approved waiver by the GuardNet XXI or Local DAA.

(4) With an approved waiver only 1-2 machines will be authorized in any secure area to utilize removal media devices, and usage will be controlled by a log of what data is transferred to the media.

(5) Users that need to transfer unclassified or declassified data from the SIPRNET to an unclassified/NIPRNET network must print out the documents from the SIPRNET and then scan the documents into the unclassified network.

(6) At this time, there are no approved methods of transferring electronic data from any ARNG Classified system to any ARNG Unclassified network.

g. Automated Information System Labeling. A label or sign should be placed on the each Automated Information System (regardless of classification level) indicating the highest level, which may be processed on that Automated Information System.

h. Classified Information Processing Procedures. These procedures are intended for use between the levels of classified processing (such as, between SECRET and CONFIDENTIAL) as well as between classified and unclassified. The procedures below must be adhered to when classified defense information is processed:

(1) Ensure that the computer is approved for processing the level of classified information required.

(2) Display a placard indicating the classification level of the processing in progress.

(3) Ensure that the work station screen is positioned to prevent viewing by unauthorized persons.

(4) When the session is completed, the following procedures will be followed, when not in a certified Sensitive Compartmented Information Facilities (SCIF) or Classified open storage area:

a. Physically disconnect any communications lines or modems from the Automated Information System.

b. Physically disconnect any other resources (i.e., separate hard drive, printer, additional workstations, plotter, etc.) used during the session.

c. Remove all media, clear the system as described in local procedures, and power down the system.

d. Store all classified systems, hard drives, laptops, printers, and documents in a secure area/facility or safe.

i. Classified Printers. Classified printers are required to have physical security present at all times.

NGB-AIS-CO SIPRNET Contact List
Business Office Classified Systems Security Manager/SIPRNET IASO
(703) 607-7999
DSN: 327-7999

SIPRNET Operations Manager
(703) 607- 9783/7632

SIPRNET Administrator/Technical Representative
(703) 607-9612
DSN: 327-9612

DMS Administrator
(703) 607-7636
DSN 327-7636

RSA Montgomery Web Site: WWW.Mont.DISA.Mil

CHAPTER 6
INCIDENT REPORTING

Incidents may result from accidental or deliberate actions on the part of a user or external influence. Protect Automated Information System incident reports as a minimum FOUO or to the level for which the system is accredited. Evidence or suspicion of an incident, intrusion, or criminal activity will be treated with care, and the Automated Information System maintained without change, pending coordination with NGB CND, as stated in APPENDIX K in the GuardNet WAN SSAA, or APPENDIX H of this Policy. Ensure users are aware of the policy governing intrusion reporting.

6-1. Incident and Intrusion Reporting.

a. Report all potential or malicious incidents immediately.

(1) Isolate the system (unplug the network cable), but DO NOT SHUT DOWN the system.

(2) Notify the next reachable level of CND in the State's reporting chain (i.e. User → IASO→ IAM → State J-6 →NGB CND). If any of the aforementioned is unreachable, then call the NGB ISC helpdesk ((800) 821-3097). The purpose is to compile supporting evidence, impact assessments, associated costs, containment viability, and eradication and reconstruction measures necessary to effectively manage the breach and provide evidentiary material for prosecution.

(3) Additionally, ensure that the respective State's JOC contacts the NGB JOC to report the nature of the incident, and courtesy copy them on any incident reports (see APPENDIX H of this policy).

b. Report all Automated Information System incidents or events including, but not limited to:

(1) Known or suspected intrusion or access by an unauthorized individual.

(2) Authorized user attempting to circumvent security procedures or elevate access privileges.

(3) Unexplained modifications of files, software, or programs.

(4) Unexplained or erratic Automated Information System responses.

(5) Presence of suspicious files, shortcuts, or programs.

(6) Malicious logic infection (e.g., virus, worm, Trojan).

(7) Receipt of suspicious e-mail attachments, files, or links.

(8) Spillage incidents or violations of published AR 25-2 BBP procedures.

c. A Serious Incident Report (SIR) will be generated and reported by NGB CND to the Army Regional Computer Emergency Response Team (RCERT), per AR l90-40, under the following conditions.

(1) The incident poses grave danger to the Army's ability to conduct established information operations.

(2) Adverse effects on the Army's image such as Web page defacements.

(3) Access or compromise of classified or sensitive information (e.g., soldier identification information (SSN), medical condition or status, patient-client or attorney-client privilege).

(4) Compromise originating from a foreign source. Compromise of systems that may risk safety, life, limb, or has the potential for catastrophic effects, or contain information for which the Army is attributable (e.g., publicly accessible waterways navigational safety information from the United States Army Corps of Engineers (USACE).

APPENDIX A
APPOINTMENT OF INFORMATION ASSURANCE SECURITY OFFICER (IASO) LETTER

SAMPLE

APPROPRIATE UNIT LETTERHEAD

OFFICE SYMBOL (25-2) DATE

MEMORANDUM FOR (Individual's Name, Rank, SSN, Unit and Address)

SUBJECT: Appointment of Additional Duties

1. Effective _____, (Individual's name)(rank)(SSN), (unit or Section Address), is appointed the following additional duty:

IASO for the _____ (Directorate/Division Staff/BDE/BN Designation)

2. Purpose. Manage the information management program and advise the Commander/Director on establishing the command priorities for information management. Serve as the interface between the functional user/unit and the ARNG G6 for all microcomputer/data communications activities.

3. Period. Indefinite.

4. Special Instructions. Will perform those duties and functions outlined in Army Regulation 25-2.

5. Authority. AR 25-2

(SIGNATURE BLOCK)
(BDE/BN CDR or DIR STAFF)

CF:
Individual
Unit
USPFO
ARNG G6
201 File
OPF Tech Pers

SAMPLE

APPENDIX B
AUTHORIZED USER AGREEMENT

COMPUTER USER AGREEMENT

1. **NOTICE AND CONSENT**: I understand that the use of any Government Computer (GC) or Telephone System constitutes my consent to monitoring (AR 380-53) of my use of the ARNG network and systems. I will use this technology responsibly. The contents and communications of this information system, including electronic mail (E-Mail) and Internet access, may be monitored for appropriate use. I understand that there is NO expectation of privacy in using Government computers or resources. I understand that inappropriate use may result in disciplinary action up to and including termination of employment.

2. **PURCHASE AND ACQUISITION**: I understand that the Director of Information Management (DOIM) will review all purchase requests and acquisition of telephone, fax, computer equipment, peripherals and software for each State and/or Territories JFHQ Army National Guard in order to meet user, security, and network requirements. All activities, directors, units or training facilities must coordinate with the DOIM through the appropriate channels for purchase of telephone, fax, computer systems, or software and the use of personal software (e.g., use of AOL on a Government notebook computer). Violations of this policy may result in disciplinary actions.

3. **TELEPHONE/COMPUTER USE POLICY**:
   b. I understand that government provided hardware and software are for conducting official government business. Leaders and supervisors may authorize personnel to use government resources to further professional and technical knowledge if it is determined to be in the best interest of the government.
   c. I understand that I have the primary responsibility to safeguard the information contained in the ARNG network from unauthorized or inadvertent modification, disclosure, destruction, denial of services, and use.
   d. Access to this network is for official use and authorized purposes and as set forth in DoD 5500.7-R, "Joint Ethics Regulation" or as further limited by DoD Policies, ARs and other federal requirements.
   e. Access to ARNG resources is a revocable privilege and is subject to content monitoring and security testing.
   f. I will use Army information systems (computers, systems, and networks) only for authorized purposes.
   g. I will maintain an Army Knowledge Online (AKO) account (www.us.army.mil) (military network only)
   h. I will not import any Government-owned software or install hardware on any Government Computer (GC) (e.g., client-workstation or server) without first getting written approval from my DOIM, IAM, or IASO.
   i. I will not load any software onto my GC, Government information technology (IT) system, or network without the approval of IA, IANM, SA or IASO. I will not try to access data or use operating systems or programs, except as specifically authorized.
   j. I know I will be issued a user identifier (user ID) and a password to authenticate my computer account. After receiving them:
      (1) I will not allow anyone else to have or use my password. If I know that my password is compromised, I will report to my SA for a new one.
      (2) If my account is on a classified network, I understand that my password is classified at the highest level of information on that network, and I will protect it in the same manner as that information.
      (3) I am responsible for all activity that occurs on my individual account once my password has been used to log on. If I am a member of a group account, I am responsible for all activity when I am logged on a system with that account.
      (4) If I have a classified account, I will ensure that my password is changed at least once every 45 days or if compromised, whichever is sooner.

(5) If I have an unclassified account, I will ensure that my password is changed at least every 60 days or if compromised, whichever is sooner.
(6) I will not store my password on any processor, microcomputer, PDA, PED, or on any magnetic or electronic media.
(7) I will not tamper with my GC to avoid adhering to Army password policy.
(8) I will never leave my unclassified and/or classified GC unattended while I am logged on, unless the GC is protected by a "password protected" screensaver.

k. I know that it is a violation of policy for any computer user to try to mask or hide his or her identity, or to try to assume the identity of someone else.

l. I know that if connected to the Secret Internet Protocol Router Network (SIPRNET), my system operates at least in the Secret, "system-high" mode.
(1) Any magnetic media used on the system must be immediately classified and protected at the system-high level, regardless of the implied classification of the data (until declassified or downgraded by an approved process). In other words, any disk going into a Secret system is now classified as Secret and must be handled accordingly.
(2) I must protect all material printed out from the SIPRNET at the system-high level until I or someone with the appropriate clearance personally reviews and properly classifies the material.
(3) I will not enter information into a system if the information has a higher classification than that for which the system is rated. I will not enter information that is proprietary, contractor-excluded, or otherwise needs special protection or handling, unless approved in writing by the IASO.
(4) If connected to the SIPRNET, only U.S. personnel with a security clearance are allowed unescorted access to the system.
(5) Magnetic disks or compact disks will not be removed from the computer area without the approval of the local commander or head of the organization.

m. My local IASO has informed me of TEMPEST (Red/Black) separation requirements for system components, and I will ensure that those requirements are met.

n. I will not move hardware or alter communications connections without first getting approval from the SA or IASO (if applicable).

o. I will scan all magnetic media (e.g., disks, CDs, tapes) for malicious software (e.g., viruses and worms) before using it on a GC, IT system, or network.

p. I will not transfer information using magnetic media from a classified system to an unclassified system.

q. I will not forward chain email or virus warnings. I will report chain email and virus warnings to my IASO and delete the message.

r. I will not run "sniffers" (utilities used to monitor network traffic, commonly used to Spy on other network users and attempt to collect their passwords) or any hacker-related software on my GC, Government IT system, or network.

s. I will not download file-sharing software (including MP3 music and video files), peer-to-peer software (i.e. Kazaa, Napster) or games onto my GC, Government IT system, or network.

t. I will not connect any personal IT equipment (e.g., PEDs and PDAs (such as Palm Pilots), personal computers, and digitally enabled devices to my GC or to any Government network without the written approval of my DOIM, IAM, IASO, or Information Management Officer (IMO).

u. I will not utilize ARNG or DoD provided Automated Information Systems for commercial financial gain or illegal activities.

v. I will ensure that my anti-virus software on my GC is updated at least weekly.

w. I will not use Internet "chat" services (e.g., America Online, Microsoft Network (MSN) Instant Messenger, Yahoo) from my GC. If chat service is needed, I will use my Army Knowledge Online (AKO) account or unless approved by the DOIM and or Public Affairs Officer at the Adjutant General's Department.

x. If I observe anything on the system I am using that indicates inadequate security, I will immediately notify the site IASO. I know what constitutes a security incident and know that I must immediately report such incidents to the IASO.

y. I will comply with security guidance issued by my SA and IASO.
z. If I have a Public Key Infrastructure (PKI) certificate installed on my computer (e.g., software token), I am responsible for ensuring that it is removed when no longer required. If the certificate is no longer needed, I will notify my SA and the issuing trusted agent of local registration authority.
aa. I know that my actions as a user can greatly affect the security of the system and that my signature on this agreement indicates that I understand my responsibility as a user requires that I adhere to regulatory guidance.
bb. I know I am subject to disciplinary action if I violate DoD and Army policies. For U.S. military and government personnel, this means that if I fail to comply with this policy, I may be subject to adverse administrative action or punishment under Article 92 of the Uniform Code of Military Justice (UCMJ). If I am not subject to the UCMJ, (State employees) I may be subject to adverse action under the United States Code or Code of Federal Regulations.

ACKNOWLEDGEMENT

I have read the above requirements regarding use of the ARNG network and systems. I understand my legal responsibilities regarding these systems and the information contained in them.

I understand that I must undergo a favorable review of local personnel records check, and an initiation of a NACIC (for civilians), or a National Agency Check (NAC) (for military and contractors) Background Investigation, with favorable results or have a current security clearance prior to obtaining and maintain network access (as directed in AR 25-2, Section V). I further understand that if I refuse to submit to a NAC, or if I have a negative result from the NAC, I will be denied network access. I understand that all network access is a revocable privilege. _____ (initial and date).

If I am requesting access to classified systems I understand that I will be required to obtain a Security Clearance at least commensurate with the level of access I require to perform my official duties, and that I must execute a Non-Disclosure Statement, and have favorable security status BEFORE being granted such access. _____ (initial and date)

Your system administrator (SA) or information assurance security officer (IASO) will ask you to sign a copy of this agreement before issuing you a password.

Supervisors/Commanders will maintain this signed document in an appropriate filing system. This completed agreement is subject to inspection.

Computer-User Name (Typed or Printed):_____

Computer-User Signature:_____

Date:_____

Security Officer Name (Typed or Printed):_____

Security Officer Signature:_____

Date:_____

APPENDIX C
LAPTOP CERTIFICATE OF USE

DEPARTMENT OF THE ARMY NATIONAL GUARD
111 South George Mason Drive
Arlington, VA 22204

NGB-AIP-IA

Date

MEMORANDUM FOR WHOM IT MAY CONCERN

SUBJECT: Laptop Certificate of Use

1. AR 25-2 requires Automated Information Systems that process unclassified information be accredited to operate. Accreditation takes into account the risks associated with operating the computer in its office environment and the countermeasures taken to protect the information's confidentiality, integrity, or availability.

2. Purpose of this certification/accreditation is to ensure that unclassified sensitive information processed by the computer is:
   a. Protected from disclosure to unauthorized persons.
   b. Protected from destruction/alteration by hackers or other unauthorized personnel.
   c. Updated with the latest anti-virus definitions, IAVAs, and security patches to protect from corruption or destruction by computer viruses.
   d. Software firewall enabled.
   e. Protected by each operator who will comply with the security controls stated in paragraph 3 below and the ARNG IA Program Policy.

3. In accordance with AR 25-2, the computer system(s) identified within the attached List of Equipment as Stand-alone is/are accredited to process and store Unclassified in the Dedicated Security Mode. The following conditions are acknowledged, understood, and complied with by the Authorized User Agreement at the computer operators' higher headquarters.

   a. The processing and/or storage (includes transmission without a (modem) of classified information on this system is prohibited.
   b. The system will be used only for official government purposes.
   c. All ISs processing ARNG information in a mobile computing environment shall provide a capability to protect data at rest (DAR) and in transit as directed in the Army National Guard Information Assurance Program Policy, Section 2-3, paragraph d., and in the Army's BBP for DAR (Data-At-Rest Protection Mobile Devices using EFS Implementation, Version 1.0, 12 Oct 2006)
   d. Only software that has been specifically developed or approved for use or has been purchased or leased by an authorized U.S. Government representative and listed on the List of Equipment, will be used with this computer.
   e. The operator will ensure the confidentiality of Privacy Act and FOUO information by preventing unauthorized access to the computer equipment, media, and printed material.
   f. The operator is responsible for the physical security of the computer and its associated equipment.
   g. If a laptop is lost or stolen it is the operator/owner to report this incident to the operators IASO/IAM/DOIM.

I (the undersigned) acknowledge and understand the conditions and responsibilities of operating the computer(s) identified in paragraph 3 above and will comply with all of the conditions.

Typed _____
(Name & Title of operator/owner)

Signature _____ _____
(dd/mm/yy)

Typed _____
(Name & Title of IASO)

Signature _____ _____
(dd/mm/yy)

APPENDIX D
ARNG IAVM REPORTING PROCESS

1 Program Requirements and Purpose

1.1 Both DoD and Army policy have deemed IAVA compliance a force protection issue. Senior Army leadership actively monitors IAVA compliance, and has stressed that IAVA compliance is a Commander's responsibility. Senior Army leadership requires mandatory compliance with IAVA reporting, and the Asset & Vulnerability tracking Resource (A&VTR) is their means to track progress in protecting Army networks and systems.

1.2 The purpose of this policy is to increase network security by tracking the state's responsiveness to IAVA suspense dates. This policy establishes specific Information Assurance Vulnerability Alert (IAVA) reporting procedures for IAVAs, IAVBs, and IATTs IAW the previously stated references.

1.3 The IAVM program supersedes the IAVA Program. IAVM is a DoD process that disseminates vulnerabilities, technical information, and tracks compliance within DoD.

2 Responsibilities

2.1 It is the responsibility of each States IAM to comply with the process detailed in this document.

2.2 The IAVM Manager will report total ARNG IAVA compliance status to NETCOM on a weekly basis.

2.3 The ARNG IAVM Manager will report to the ARNG IAPM on all ARNG organizations failing to meet an IAVA or IAVB reporting suspense dates.

2.4 Failure to submit the required data or meet an established compliance date is cause to be disconnected from the GuardNet XXI WAN.

2.5 The ARNG IAPM will report all ARNG organizations failing to meet an IAVM reporting suspense dates to the GuardNet DAA.

3 The IAVM Notification System

The IAVA notification system has three levels which are described below:

3.1 Alerts

An Information Assurance Vulnerability Alert (IAVA) is sent when a new vulnerability poses an immediate, potentially severe threat to DoD systems. Reporting requirements to DoD for this level are:

- Acknowledgment of receipt within 5 days from the date of the message or by date designated in IAVA message.
- Compliance fulfillment no later than date designated in IAVA message.

3.2 Bulletins

An Information Assurance Vulnerability Bulletin (IAVB) addresses new vulnerabilities that do not pose an immediate threat, but are significant enough that not complying with the corrective action could escalate the threat. The reporting requirement for this level is acknowledgment of receipt no later than date designated in IAVA message. IAW AR25-2, Para 4-24 section (b), states that IAVBs corrective actions are required to be completed but not reported.

3.3 Technical Tips

An Information Assurance Technical Tip (IATT) (Army designation) identifies existing low risk vulnerabilities. IAW AR25-2, Para 4-24 section (c), states that IATTs (Tech Tips) corrective actions are required to be completed but not reported.

4 IAVM Compliance Procedures

IAVM compliance is the absolute minimum standard for all IS, not the preferred end state, and is a proactive methodology of maintaining, patching, and updating systems before exploitation. IAVM

requires the completion of four distinct phases to ensure compliance. These phases are:

1. Vulnerability identification, dissemination, and acknowledgement
2. Application of measures to affected systems to make them compliant
3. Compliance reporting
4. Compliance verification.

5 Asset and Vulnerability Tracking Resource (A&VTR)

5.1 An Army Knowledge Online (AKO) account is required to initially log into A&VTR. IAMs are required to have an AKO account. IAMs should request an A&VTR account on the A&VTR login page. The current A&VTR web addresses is: https://newia.us.army.mil.

5.2 A&VTR compliance data entries are mandatory. When the IAVA compliance component of A&VTR is fully operational, initial compliance data will be entered into the A&VTR as soon as assets (network applications — software/hardware) are brought into compliance IAW the IAVA message.

5.3 Updates will be submitted as required, e.g., additional assets are identified, non-compliant assets are brought under compliance, or disconnected from the network, or extension dates are changed.

5.4 A Frequently Asked Questions (FAQs) section is posted on the A&VTR web page. A draft Standard Operating Procedure (Policy) is available on the IA web page under the A&VTR folder at https://informationassurance.us.army.mil.

6 Interim Compliance Verification Reporting

Until A&VTR is fully operational, each state and territory will email their compliance verification reports to ARNG IAVM Manager at ngb-aip-ia@us.army.mil.

7 Interim Measures for Submitting a Mitigation Action Plan (MAP) for the 58 States and Territories (including NCR, Enterprise, VADPU, and Willow Oaks)

7.1 Until the MAP component of the A&VTR is fully operational, a MAP must be submitted (Enclosure 1 of this Appendix) when the IAVA suspense date cannot be met. The MAP will be submitted to the ARNG IAVM Manager prior to the IAVA suspense date. The ARNG IAPM will review the request, if appropriate grant approval, or forward the MAP to the NETCOM.

7.2 All MAPs will be emailed to ngb-aip-ia@us.army.mil.

7.3 Telephone NGB-AIP-IA at 703-607-9719 or DSN 327-9719, if no other means are available.

7.4 The NGB IAPM may approve extensions up to 30 days from the compliance date on the IAVA message.

7.5 The Network Enterprise Technology Command (NETCOM) Information Assurance Directorate (IAD) Director may approve extensions up to 60 days from end date of the NGB IAPM granted 30-day extension. Mitigation Action Plans may not exceed 90 days.

7.6 A copy of all MAPs and approvals will be furnished to the ARNG IAPM and to NETCOM IAD via email.

8 Compliance Enforcement

8.1 If a reporting activity has not annotated the required compliance reporting date on the IAVA reporting web page on A&VTR or reported to the ARNG IAVM Manager, the NGB-AIP-IA office will initiate the following actions:

1. 1st Notice: A status update notice is sent once a week from IAVA original release date until state reports compliance. All extensions are reviewed for approval.
2. 2nd Notice: NGB-AIP-IA team will contact state DOIM.
3. 3rd Notice: ARNG G6 will contact state TAG.

8.2 The ARNG State IA Team will be notified within 24 hours, after the established suspense date has

expired, when an IAVA or IAVB acknowledgement of receipt has not been annotated on the A&VTR web page.

8.3 Point of contact is the NGB-AIP-IA office and the email address is provided by ngb-aip-ia@us.army.mil or NGB-AIP-IA (Global address).

8.4 Failure to comply with this IAVM policy will result in the NGB DAA evaluating the customer's connection to GuardNet WAN and the security risk associated with continued service.

8.5 State J-6s and DCSIMs can expect the ARNG G6 to take proactive measures to prevent the exploitation of identified vulnerable systems.

8.6 Measures include proactive scanning of networks for this vulnerability.

8.7 Systems that have been identified as vulnerable will be blocked from access to the network until corrective actions to mitigate the risk have been taken and verified.

8.8 Failure to meet IAVA compliancy will require NGB-AIS-CO to implement options 1, or 2 listed below, with the approval of the ARNG G6.

9 Under Options below, the term 'non-compliant State' can include any of the 58 States and Territories (including NCR, Enterprise, VADPU, and Willow Oaks)

Option 1: Implement the Access Control List (ACL) on routers blocking port 80 under administrative control. NGB-AIS-CO will implement the ACL on the NGB security routers. NGB-AIS-CO will block any port 80 traffic at the network perimeters for non-compliant
Option 3: ARNG IAPM will recommend that state network be blocked from the ARNG network.

APPENDIX D

ENCLOSURE 1 : MITIGATION ACTION PLAN FORMAT

RETURN ALL MITIGATION ACTION PLANS VIA YOUR CHAIN OF COMMAND TO THE NGB-AIP-IA OFFICE AT NGB-AIP-IA@US.ARMY.MIL FOR TECHNICAL REVIEW AND FORWARDING TO NETCOM/HQDA IA FOR APPROVAL

(All fields are required)

1. Organization Requesting Extension:
2. RCIO/MACOM/PEO/PM: National Guard Bureau
    a. IAPM or Alternate: ARNG IAPM (Provide information of ARNG IAPM name)
    b. Email Address: ARNG IAPM@us.army.mil (Provide information of ARNG IAPM name)
    c. Telephone: 703-607-9632 DSN 327-9632
3. IAVA #:
    a. IAVA Issue Date:
    b. ARMY Suspense for Compliance:
    c. Total number of Assets for which the Extension is requested:
    d. Target Date for Compliance:

*****A COPY OF ALL MITIGATION ACTION PLANS AND APPROVALS WILL BE FURNISHED TO THE ORGANIZATION'S NEXT HIGHER COMMAND TO INCLUDE RCIO/MACOM IAPM AND NETCOM IAD VIA EMAIL*****

4. Reason for Mitigation Action Plan: Justification must include the following items:
    a. Reason the systems are not patched (technical or procedure issues).
    b. What is being done to get the systems patched?
5. Alternate Security Actions To Be Implemented During Duration of Extension:
    a. Operational Impact if Assets are taken offline:
    b. Mitigation/Security Actions to be implemented during duration of MAP (Extension):

**NOTE: Every extension must be accompanied by a detailed explanation of all actions taken to mitigate the vulnerability for the duration of the extension. Examples include but are not limited to: increased monitoring of system logs and host-based intrusion detection systems (IDS), closure of ports and turning off of services.

**No extension will be granted without a clear explanation of mitigating actions and results from current STAT scan.

6. Substantive POC:

NOTE: To match this Mitigation Action Plan to compliance reporting, this name must be the person who enters asset-reporting numbers e.g., the number of assets affected, in compliance, and requested extensions into the Army's IAVA Compliance Reporting Database.

    a. Name:
    b. Email Address:
    c. Telephone:

7. Alternate POC:
    a. Name:
    b. Email Address:
    c. Telephone:

APPENDIX E
FPA PROCESS

INSTRUCTIONS FOR PREPARING THE FPA REQUEST FORM

ARNG users who want to request change in configuration of the NGB-managed firewalls that is not under current configuration baseline must submit a remedy ticket and FPA form via NGB ISC Helpdesk. **If there is not enough information provided, the form will be returned to you. The request will be delayed for as long as it takes to provide the required information.**

1. Block 1. FPA Number: (Leave blank)
2. Block 2. Trouble Ticket Number: (Assigned remedy ticket number for this request)
3. Block 3. Priority: (Same as the priority assigned on the remedy ticket number)
4. Block 4. Requester Name/Phone/E-mail: (This will be J-6 POC for submitting remedy tickets or designated representative to include contact information (i.e. phone # and email), this person is responsible for submitting this form to NGB-AIS-CO and for responding to follow-on questions during the review and approval process.)
5. Block 5. Request Date: (self explanatory)
6. Block 6. State/Agency. (self explanatory)
7. Block 7: Fill out this block completely. Provide as much detail as possible, including all available information on the ports, protocols, applications, source and destination IP addresses, and any additional information that is applicable. Provide the following required information:
8. Item a. POC name, phone, email address and organization (if different from requester)
9. Item b. Source IP addresses (recommend source to destination IP address, but no higher than Class C subnet)
10. Item c. Destination IP addresses (recommend specific IP address and include fully qualified domain name)
11. Item d. Ports (provide the port number and description, i.e., 25/SMTP)
12. Item e. Protocols (i.e., TCP, UDP, GRE)
13. Item f. Associated Applications (include acronym and long title)
14. Item g. Is the application AKO- or GKO-enabled? YES/NO
15. Item h. Application DAA name/phone/email
16. Item i. Is the application used by all 54 states, territories, and DC? YES/NO
17. Item j. Is this Application accredited? YES/NO (If answer YES, POC must forward a copy of ATO; If answer NO, per DoD policy-application will be disapproved for operations on the network until accredited)
18. Item k. Is there a CTO for this application? YES/NO
19. Item l. Is the application or system IAVA compliant? YES/NO
20. Item m. Provide detailed justification for this request
21. Item n. Provide a detailed description of the requirement/problem or any additional comments necessary to illustrate the issue (i.e. include diagrams, drawing, documents as necessary)
22. Please note that when specifying a port number that the well known ports are those from 0 through 1023. The registered ports are those from 1024 through 49151. Dynamic and/or private ports are those from 49152 through 65535.
23. Blocks 8 thru 30 will be completed by NGB-AIS.

Submit this form to the NGB ISC Helpdesk. They will attach it to your trouble ticket.

FIREWALL PORT ACTIVATION REQUEST		
1. FPA Number:	2. Trouble Ticket Number:	3. Priority:
REQUESTER/ORIGINATOR INFORMATION		
4. Requester Name/Phone/E-Mail:	5. Request Date:	

	6. State/Agency:
7. Provide the Following **Required** Information: a. POC name, phone, email address and organization *(if different from requester)*: b. Source IP Addresses *(recommend source to destination IP address, but no higher than Class C subnet)*: c. Destination IP Addresses *(recommend specific IP address and include fully qualified domain name)*: d. Ports *(provide the port number and description, i.e., 25/SMTP)*: e. Protocols *(i.e., TCP, UDP, GRE)*: f. Associated Applications *(include acronym and long title)*: g. Is the application AKO- or GKO-enabled? YES/NO h. Application DAA name/phone/e-mail: i. Is the application used by all 54 states, territories, and DC? YES/NO j. Is this Application accredited? YES/NO *(If answer YES, POC must forward a copy of ATO; If answer NO, per DoD policy-application will be disapproved for operations on the network until accredited)* k. Is there a CTO for this application? YES/NO l. Is the application or system IAVA compliant? m. Provide a justification for this request: n. Provide a detailed description of the requirement/problem or any additional comments necessary to illustrate the issue *(i.e. include diagrams, drawing, documents as necessary)*:	
INFORMATION ASSURANCE	
8. What Firewalls Are Impacted By This Request:	
9. Port Definition:	
10. Known Vulnerabilities:	
11. Mitigation Strategy:	
12. Comments:	
13. Approve/Disapprove:	14. Name:
	15. Date:
ENGINEERING	
16. Network Analysis (Provide Impacts on JFHQs => NIPRNet Gateway, NIPRNet Gateway => NIPRNet Gateway, GuardNet => NIPRNet):	
17. Approve/Disapprove:	18. Name:
19. Attachments:	20. Date:
IMPLEMENTATION INFORMATION	
21. Implementation Date:	22. Engineer:

23. Implementation Actions:	
24. Did the rule created enable the desired access? YES/NO	
CM ACTION	
25. ASEIG Recommendation:	26. ASEIG Date:
27. CCB Recommendation:	28. CCB Date:
29. DAA Disposition:	30. Disposition Date:
31. Approving Authority Name:	32. Signature:
33. Date Closed:	34. Reason For Closure:
35. Comments:	

Figure 2 – FPA Request Form

APPENDIX F
INCIDENT REPORTING PROCEDURES AND FORM

The following paragraphs describe the procedures for handling a reported incident.

Incident and Intrusion Response Tips

DON'T:
- ☒ Attempt to access the source or contact the source in any way (finger, telnet, ping)
- ☒ Change the system files on the suspected/compromised system
- ☒ Connect to the system over the network.

DO:
- ☑ Unplug the machine from the network (if mission will allow)
- ☑ Log-on as system administrator at the server console and do a complete dump of the system
- ☑ Make sure not to alter any files on the system
- ☑ Place the complete dump in a secure location
- ☑ Place the suspected/compromised system in a secure place (limit access to the system)
- ☑ Complete the Incident and Intrusion Response Form and contact the ISC.

1. Incident Procedures

Upon detecting an intrusion or suspicious activity, the individual involved will contact the ISC (helpdesk@us.army.mil, (800-821-3097), who will connect the caller to one of the following personnel in the given order:

- The CND Team member or IASO at the site where the incident has taken place
- The NGB CND Team Leader and IASO
- Other personnel designated by this document.

This process allows for a single point of contact with 24-hour coverage to simplify incident reporting by users or outside agencies. At the same time, it also allows the reporting individual to speak directly with a site point of contact to facilitate the best technical resolution of the issue. The site contact will ensure that notification of the incident goes in two directions: to the CND Lead, and to the SA Lead/IASO responsible for the affected system. Their actions are outlined below.

Upon notification, the SA takes the appropriate action to repair the system, in compliance with ACERT/RCERT/CID procedures. The SA notifies site CND member of all actions and communications regarding the incident. The NGB IASO and the local IASO will work with the SA to remedy the situation quickly and effectively. The NGB IASO will notify the NGB IAM of the affected site and the incident. The NGB IASO and local IASO will be copied on all email correspondence to or from the SA.

The local IASO or IAM will notify their Chief of Information Management and Chief of Security. This may be done with a single broadcast email describing the situation, followed by phone calls for verification or clarification as appropriate. If necessary, the local IASO or IAM will contact the individual or agency responsible for discovering the incident in order to check all relevant information. System users affected by the incident will be informed in order to explain any changes or outages in the system.

All communication of status and actions should be done by email whenever practical, with copies furnished to the site CND member. This provides a reference source for actions taken in response to the incident and allows the CND member to monitor the progress of corrective actions so that appropriate personnel may be notified.

The site CND member will issue a report at least once a day providing the status and actions taken until the incident has been resolved. When the SA indicates that the system has been repaired, the CND member will verify with NGB CND and RCERT or other relevant parties that the system is scanned and approved to operate. The CND member will then notify all relevant parties that the incident is closed.

2. Backup Requirements

An IRP in conjunction with locally prepared Continuity of Operations Plans (COOPs) and Emergency Action Plans (EAPs) shall be maintained at each unit to ensure a rapid return to operation, in the event of a security incident (i.e., DOS attacks or other unplanned systems failures). The procedures contained in the unit IRP, EAP, and COOP must be regularly verified and implemented, and shall require training exercises to test their effectiveness. IRPs should include a contact list and procedures for responding to incidents, restoring the system to full operation after a security incident, and preparing the follow-up analysis. COOPs shall include provisions for the following:

a. Scheduled backup of the entire file system
b. Daily backup of changed files
c. Off-site storage of backup media
d. Memorandums of understanding with nearby unit(s) to provide alternative processing location(s)
e. Backup personnel for NGB CERT system administration and Information System Security (ISS) personnel.

3. Audit Trails

A computer security incident can occur at anytime of the day or night. Most of the DOS attacks and other unplanned system failures occur during the off hours when hackers do not expect SAs/managers to be watching the system. Worm and virus incidents can occur at any time during the day. Viruses are not self-replicating, thus, incidents of this nature are not as time critical as worm or hacker incidents. Worms are self-replicating and can spread to hundreds of machines in a matter of minutes; thus, time is a critical factor when dealing with a worm attack. If the type of attack has not been identified, then proceed as if the attack is worm related. Thus, time and distance considerations in responding to the incident are extremely important.

Audit trail records are an essential element of detecting a technical vulnerability. NGB CND components shall be audited according to the standards of AR 25-2 and the NGB CND SOPs and Job Aids. All NGB CND users, service and support personnel, and SAs shall report suspicious activities to their IASO or Information Assurance Network Officer (IANO) for a determination on whether a security incident or technical vulnerability has occurred and what action must be taken. Suspicious activities include:

a. Incorrect logons
b. Dual logons
c. Successful and unsuccessful connections from hosts that do not normally establish connections to other systems
d. Error messages that indicate that users with non command authorization have attempted to execute or obtain these command authorizations
e. A strange process that is running and accumulating a lot of Central Processor Unit (CPU) time
f. An intruder that is logged into your system
g. A virus or worm that has infected your system
h. An unknown remote site that attempts to access the system
i. An authorized user that attempts to access information or areas on the system that exceed their authorized privilege levels.

4. Contamination

If the incident is a possible contamination, the component or system should be isolated from other GuardNet components. Disconnect the system, if necessary. The IANO, with assistance from the NGB IASO and unit IASO, shall attempt to identify contamination symptoms, which may be present based on a baseline of normal system operation.

Technical vulnerabilities shall be reported immediately. Individuals shall contact their IANO or command IASO for the initial reporting of the vulnerability. If the IANO or IASO is not available, contact the IAM. System users should not delay reporting an incident because their IASO personnel are not available. IASOs shall investigate the validity of all possible technical vulnerabilities including contamination and intrusions or attempted intrusions. The format for reporting a technical vulnerability shall be IAW AR 25-2. The report should be thorough and detailed so the vulnerability/incident can be demonstrated and researched.

In addition, the NGB CND shall also be notified of any possible GuardNet technical vulnerabilities or security incidents. This notification shall be conducted securely after discussion with the unit's IASO. The local IASO shall coordinate technical recovery actions based on guidance from their Information Assurance Program Manager (IAPM) and NGB IASO, and shall submit interim and final reports on all security incidents.

5. Incident Reporting Format (Technical Vulnerability)

If unable to report an incident to the appropriate organization through the normal reporting process or if online reporting is not available, use the following tables below in developing an Incident Report.

APPENDIX F

Incident Reporting Form	Email filled-in form to RCERT-CONUS@NETCOM.ARMY.MIL
Classification	
From	
To	RCERT-CONUS, LIWA, Fort Huachuca, Arizona
Incident Number	Assigned by the RCERT-CONUS
Coordination	
Date/Time of Incident	
Reporter	
Contact Information	
Destination IP/Name	
System Involved	
System Mission	
Source of Incident	
Event	
Exploitation Method	
Hacker's Intentions	

APPENDIX F

SAMPLE

The following format will be used by system users for submitting an initial report by other than the on-line reporting form (above). It is recognized that all the requested information will probably not be available for inclusion in the initial report:

Classification	Sensitive But Unclassified at a minimum
From	Organization Name, building number, location
To	RCERT-CONUS, LIWA, Fort Huachuca, Arizona
Incident Number	Assigned by the RCERT-CONUS
Coordination	Other organization or activity knowledgeable of incident
Date/Time of Incident	Date/Time of Incident in Zulu time
Reporter	Reporter's Full Name, Position
Contact Information	Reporter's telephone (DSN/Commercial), e-mail, mailing address
Destination IP/Name	Victim(s) IP Address(es), Resolved Address Name(s)
System Involved	Operating system, hardware/software description
System Mission	System functionality, describe in detail
Source of Incident	IP address, Resolved Address Name, System Information
Event	Explain in Detail the circumstances of the incident
Exploitation Method	If known, describe the exploitation method(s)
Hacker's Intentions	Denial of Service, Probe, Unauthorized Access, etc.

Classification	Sensitive But Unclassified at a minimum
From	DOIM, Fort Huachuca, Arizona
To	RCERT-CONUS, LIWA, Fort Huachuca, Arizona
Incident Number	TBD
Coordination	TNOSC, Fort Huachuca, AZ
Date/Time of Incident	1111400Z DEC 2001
Reporter	John Q. Doe, System Administrator, Network Ops,
Contact Information	Building 1002, DOIM, Fort Brainbright, Iowa DSN 222-0000, Comm (222) 222-0000, Fax: 0000
Destination IP/Name	000.000.000.000, Srvr3-Brain.army.mil
System Involved	Unix, Solaris 8, Sun Enterprise Ultra 450
System Mission	Sensitive/Critical application server
Source of Incident	111.111.111.111, Hacker-at-Large.com
Event	Unauthorized access, root compromise, logs deleted
Exploitation Method	Possible buffer overflow
Hacker's Intentions	Gain unauthorized root access

SAMPLE

APPENDIX G
GLOSSARY OF ACRONYMS AND DEFINITIONS

SECTION I: GLOSSARY of ACRONYMS

Acronym	Definition
1st IOC (L)	1st Information Operations Command – Land
A	
AATS	Automated Architecture Tool Suite
ABIS	Advanced Battlefield Information System, DoD
AC	Area Command
ACCO	Army Case Control Office
ACERT	Army Computer Emergency Response Team
ACL	Access Control List
ACMO	NGB-AIS Configuration Management Officer
ACND	Army Computer Network Defense
ACS	Army Community Service
ACSIM	Assistant Chief of Staff for Installation Management
AD	Active Directory
ADP	Automated Data Processing
AEI	Army Enterprise Infrastructure
AES	Advanced Encryption Standard
AFIWC	Air Force Information Warfare Center, DoD
AFTAC	Air Force Technical Applications Center, DoD
AIAP	Army Information Assurance Program
AII	Army Information Infrastructure
AIP	Automated Information Plans, Programs, and Policies
AIP-IA	Information Systems Division – Information Assurance
AIS	Automated Information System or Army Information Systems
AIS-CM	AIS-Configuration Management
AIS-SE	AIS-System Engineering
AIS/SPP	Automated Information Systems Standard Practice Procedure
AISSP	Army Information Systems Security Program
AISSRP	Army Information Systems Security Resources Program
AITS	Advanced Information Technology Services
AKE	Army Knowledge Enterprise
AKMP	Army Key Management Program
AKO	Army Knowledge Online
AM	Asset Management
AMC	Army Material Command
APMS	Automated Program Management Information System
AMHS	Automated Message Handling System
AMWG	Architecture Methodology Working Group
ANG	Air National Guard
ANGRC	Air National Guard Readiness Center
ANSI	American National Standards Institute
ANSIR	Awareness of National Security Issues and Response, FBI
AOC	Army Operations Center
AODR	Army Operational Data Repository
AP	Application Program
API	Application Program Interface
AR	Army Regulation
ARIN	American Registry for Internet Numbers
ARISS	Army Recruiting Information Support System

ARNG	Army National Guard
ARNG-AIPM	ARNG-Automated Information Program Manager
ARNG-CIO	Army National Guard – Chief Information Officer
ARNGRC	Army National Guard Readiness Center
ARP	Address Resolution Protocol
ARPA	Advanced Research Projects Agency, DoD, predecessor to DARPA
ARPAnet	Advanced Research Projects Agency network, DoD, predecessor to the Internet
ARS	Action Request System
ARSTAF	Army Staff
ASA	Assistant Secretary of the Army
ASA (ALT)	Assistant Secretary of the Army (Acquisition, Logistics and Technology)
ASA (RDA)	Assistant Secretary of the Army for Research, Development and Acquisition
ASAP	As Soon As Possible
ASARC	Army Systems Acquisition Review Council
ASC	Army Signal Command
ASCII	American Standard Code for Information Interchange
ASD	Assistant Secretary of Defense
ASD C3I	Assistant Secretary of Defense for Command, Control, Communications & Intelligence
ASEIG	ARNG Systems Engineering and Integration Group
ASORTS	Army Status of Resources and Training System
ASR	Army Signal (Command) Regulation
ASSIST	Automated Systems Security Incident Support Team (now DoD-CERT)
ASW&R	Attack Sensing, Warning and Response Services (ASW&R)
ATC	Authority to Connect
ATD	Advanced Technology Development
ATDL	Advanced Technology Development Laboratory
ATM	Asynchronous Transfer Mode
ATO	Approval To Operate
ATS	Automated Tactical Systems
AUA	Authorized User Agreement
AUTODIN	Automated Digital Network (now DMS)
AVIC	Army Visual Information Center
A&VTR	Asset and Vulnerability Tracking Resource
AWRAC	Army Web Risk Assessment Cell
AWS	Automated Weapons Systems

B

BAS	Battlefield Automation Systems
BASOPS	Base Operations
BBP	Best Business Practices
BGP	Border Gateway Protocol
BI	Background Investigation
BIOS	Basic Input Output System
BLSRs	Baseline Security Requirements
BNCC	Base Network Control Center
BOD	Beneficial Occupancy Date
BOM	Bill of Materials
BPA	Blanket Purchase Agreement
BPR	Business Process Reengineering
BSM	Basic Security Module (part of Solaris)

C

C2	Command and Control
C&A	Certification and Accreditation
CA	Certificate Authority
CC	Coordination Center

CCI	Controlled Cryptographic Item
CCIU	Computer Crimes Investigative Unit
CID	Criminal Investigation Division
CIDAP	Cyber Intrusion Detection Plan
CIO	Chief Information Officer
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CND	Computer Network Defense
COB	Close of Business
COMSEC	Communications Security
CONUS	Continental United States
COOP	Continuity Of Operations Plan
CTTA	Certified TEMPEST Technical Authority

D

DCISM	Deputy Chief of Staff for Information Management
DEPSECDEF	Deputy Secretary Of Defense
DIACAP	DoD Information Assurance Certification & Accreditation Program (supersedes DITSCAP/DIACAP)
DISA	Defense Information Systems Agency
DITSCAP/DIACAP	Department Of Defense Information Technology Security Certification And Accreditation Process (now DIACAP)
DMS	Defense Message System (new AUTODIN)
DoD	Department Of Defense
DOIM	Directorate of Information Management
DOS	Denial of Service
DRSN	Defense Red Switched Network
DSN	Defense Switched Network

E

EAP	Emergency Action Plan

F

FBI	Federal Bureau of Investigation
FIS	Foreign Intelligence Service
FISMA	Federal Information Security Management Act
FOUO	For Official Use Only

G

G6	Signal/Communications Division or Corps Staff Office
GIG	Global Information Grid
GNOSC	Global Network Operations and Security Center
GO	General Officer

H

HQ	Headquarters

I

IA	Information Assurance
IAM	Information Assurance Manager
IANO	Information Assurance Network Officer
IAPM	Information Assurance Program Manager
IASM	Information Assurance Systems Manager
IASO	Information Assurance Security Officer
IAVA	Information Assurance Vulnerability Alert
IAVM	Information Assurance Vulnerability Message
IAW	In Accordance With

IDS	Intrusion Detection Device
INFOSEC	Information Security
INSCOM	U.S Army Intelligence and Security Command
IP	Internet Protocol
IPv6.0	Internet Protocol version 6.0 (more IP addresses in the world)
IRP	Incident Response Plan
IS	Information System
ISC	Integrated Service Center
ISS	Information System Security
ISSO	Information System Security Officer
IT	Information Technology
ITRCB	Information Technology Requirements Control Board
J	
JFHQ	Joint Forces Headquarters
L	
LAN	Local Area Network
LE/CI	
LIWA	LAN Information Warfare Activity (now 1st IOC(L))
LNO	Liaison Office
M	
MDEP	Management Decision Package
N	
NA	Network Administrator
NETCOM	Network Enterprise Technology Command
NGB	National Guard Bureau
NGB CND	NGB Computer Network Defense (Replaced NGB-CERT, NGB-NOSC)
NGB-AIP-IA	National Guard Bureau Information Technology Plans, Programs and Policy Division Information Assurance
NGB-AIS-CO	NGB-AIS-CONOPS
NID	Network Intrusion Detection
NIPRNET	Unclassified but Sensitive Internet Protocol Router Network
NOSC	Network Operations and Security Center
NSA	National Security Agency
NSIP	Network Security Improvement Program
NSTISSP	National Security Telecommunications and Information Systems Security Policy
O	
OCONUS	Outside CONUS
P	
PDA	Personal Digital Assistant
PED	Portable Electronic Device
POC	Point of Contact
PSN	Public Switched Network
R	
RA	Remote Access
RCERT	Regional Computer Emergency Response Team
S	
SA	System Administrator
SAEDA	Subversion and Espionage Directed Against the Army

SCI	Sensitive Compartmented Information
SDD	Secure Data Device
SIPRNET	Secret Internet Protocol Router Network
SIR	Serious Incident Report
SOP	Standard Operating Procedure
SSAA	System Security Authorization Agreement
STE	Secure Telephone Equipment
STIG	Security Technical Implementation Guide
STU III	Secure Telephone Unit version 3.0

T

TS	Top Secret
TNOSC	Theater Network Operations and Security Center

U

URL	Universal Resource Locator
USACE	United States Army Corps of Engineers

W

WAN	Wide Area Network
WPAN	Wireless Personal Area Network

SECTION II: DEFINITIONS

AIS (also called IS) –

(1) An assembly of computer hardware, software, firmware, or any combination of these, configured to accomplish specific information handling operations, such as, communication, computation, dissemination, processing, and storage of information.

(2) Any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data and includes computer software, firmware, and hardware (Note: Included are computers, word processing systems, networks, or other electronic information handling systems, and associated equipment).

Authorized User – Any appropriately cleared individual with a requirement to access a DoD information system in order to perform or assist in a lawful and authorized governmental function.

AUA – The authorized user agreement is an acknowledgement that the signing person understands the requirements and legal responsibilities, they must undergo a favorable review of local personnel records check and initiation of a NACIC or NAC, and that their network access is a revocable privilege.

Certification – Recognition given to individuals who have met predetermined qualifications set by an agency of government, industry or profession. Certification provides verification of individuals' knowledge and experience through evaluation and approval, based on a set of standards for a specific profession or occupation's functional job levels. Each certification is designed to stand on its own, and represents an individual's mastery of a particular set of knowledge and skills.

Commercial Wireless – Devices, Services, and Technologies commercially procured and intended for use in commercial frequency bands.

Contractor – Per the Defense Acquisition University Glossary, "An entity in private industry which enters into contracts with the government to provide goods or services." For DoD IA purposes, an entity is a private sector employee performing IA functions in support of a DoD IS. Private sector employees performing IA functions must meet the same standards for system access or management as Government IA employees.

CTTA – An experienced, technically qualified U.S. Government employee who has met established certification requirements IAW Committee on National Security Systems-approved criteria and has been appointed by a U.S. Government Department or Agency to fulfill CTTA responsibilities.

DAA – The official authorized to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with Designated Accrediting Authority and Delegated Accrediting Authority.

DITSCAP/DIACAP – DITSCAP has been superseded by DIACAP at DoD level, but instructions have not yet been implemented by DA. DITSCAP remains in effect until implemented instructions are published by DA.

DIACAP – The standard DoD approach for identifying information security requirements, providing security solutions, and managing information technology system security.

Enclave – A total network made up of all the interconnected computer systems, communication systems, and network components within some logical boundary, usually a boundary device such as a router or firewall under the control of a single authority and security policy, including personnel and physical security. Enclaves provide standard IA capabilities such as boundary defense, incident detection and response, and key management, and also deliver common applications such as office automation and

electronic mail. Examples of enclaves include local area networks and the applications they host, backbone networks, and data processing centers. (Replaced the term system-of-systems.)

End-to-End – Automated Information System from the end-user device up to the security border of a DoD network and/or between two user devices connected by a DoD/non-DoD network (to include the wireless infrastructures air interface).

Enterprise – Any Automated Information System, network, or application that the ARNG G6 is responsible for.

External Interfaces – Interfaces, including commercial systems (such as a cellular/PCS or pager network not under control of the DAA), capable of carrying traffic between systems under control of the DAA (e.g., the DoD Automated Information System and a DoD wireless device).

Federal Information Processing Standards (FIPS) – The standards issued by the National Institute of Standards and Technology for Federal computer systems (www.itl.nist.gov/fipspubs).

FISMA – Title III of the E-Government Act (Public Law 107-347), passed by the 107th Congress and signed into law by the President in December 2002, requiring each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. FISMA, along with the Paperwork Reduction Act of 1995 and the Information Technology Management Reform Act of 1996 (Clinger-Cohen Act), explicitly emphasizes a risk-based policy for cost-effective security.

GIG – The globally interconnected, end-to-end set of information capabilities associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve Information Superiority. It also includes National Security Systems as defined in 40 U.S.C. 11103(a) (formerly section 5142 of the Clinger-Cohen Act of 1996) (reference (m)). Includes any system, equipment, software, or service that meets one or more of the following criteria:

- Transmits information to, receives information from, routes information among, or interchanges information among other equipment, software, and services.
- Provides retention, organization, visualization, information assurance, or disposition of data, information, and/or knowledge received from or transmitted to other equipment, software, and services.
- Processes data or information for use by other equipment, software, and services.
- Non-GIG IT -- Stand-alone, self-contained, or embedded IT that is not or shall not be connected to the enterprise network.

GuardNet WAN– ARNG backbone, connected to the NIPRNET, for the 54 states and territories.

I&A – Process of accepting a claimed identity and establishing the validity of that claimed identity.

IA – Measures used to protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

IA Certification and Accreditation (C&A) – The standard DoD approach for identifying information security requirements, providing security solutions, and managing the security of DoD information systems.

Information Assurance Vulnerability Alert (IAVA) – The comprehensive distribution process for notifying the Components about vulnerability alerts and countermeasures information.

Information Assurance Vulnerability Management (IAVM) – The IAVAM process provides positive control of the vulnerability notification process for DoD network assets. The IAVM requires COMPONENTS receipt acknowledgement and provides specific time parameters for implementing appropriate countermeasures, depending on the criticality of the vulnerability.

IS — see AIS.

ITRCB - The Army National Guard ITRCB charter was approved in December 2000, and states it will determine investment risks and establish metrics to measure investment success. The charter also states that the ITRCB will validate IT proposals against investment criteria and periodically review validated and funded proposals. In addition, the ITRCB will meet before the Acquisition Planning Board (APB) meets and provide input to the APB, and call additional meetings to work pending issues. National Guard Bureau representatives stated that the ITRCB reviews IT purchase requests with life cycle costs of more than $100,000.

LAN – A network that spans a relatively small area. Most LANs are confined to a single building or group of buildings.

Mobile Code – Software modules obtained from remote systems, transferred across a network, and then downloaded and executed on local systems without explicit installation or execution by the recipient.

Network – Two or more Automated Information System connected.

NIPRNET – The Department of Defense Network that is accredited Sensitive but unclassified.

Organizational, government owned computers – A government Automated Information System that was issued or cleared by the local IA DAA for the accomplishment of official duties.

PDA – A generic term for a class of small, easily carried electronic devices used to store and retrieve information.

PED – Any non-stationary electronic apparatus with the capability of recording, storing, and/or transmitting information. This definition includes, but is not limited to PDAs, cellular/PCS phones, two-way pagers, e-mail devices, audio/video recording devices, and hand-held/laptop computers.

Privileged Users – Authorized users and IA Personnel who have administrative privileges to conduct maintenance and ensure security of the network.

Reverse Proxy Server – Provides a layer of protection against web page defacements by not allowing users to connect to the Web server directly. This is achieved by acting as a proxy for the intranet, to the protected server, brokering service requests on behalf of the external user or server.

SIPRNET – The Department of Defense Network that is accredited SECRET (S).

SCI – Classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of Central Intelligence.

Sensitive Information. Information the loss, misuse, or unauthorized access to or modification of could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of title 5, United States Code, "The Privacy Act" (reference (ad)), but which has not been specifically authorized under criteria established by Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy (Section 278g-3 of title 15, United States Code, "The Computer Security Act of 1987" (reference (ae)).) This includes

information in routine DoD payroll, finance, logistics, and personnel management systems. Sensitive information sub-categories include, but are not limited to the following:

- For Official Use Only (FOUO). In accordance with DoD 5400.7-R (reference (af)), DoD information exempted from mandatory public disclosure under the Freedom of Information Act (FOIA) (reference (ag)).
- Privacy Data. Any record that is contained in a system of records, as defined in the reference (ad) and information the disclosure of which would constitute an unwarranted invasion of personal privacy.
- DoD Unclassified Controlled Nuclear Information (DoD UCNI). Unclassified information on security measures (security plans, procedures and equipment) for the physical protection of DoD Special Nuclear Material (SNM), equipment, or facilities IAW DoD Directive 5210.83 (reference (ah)). Information is Designated DoD UCNI when it is determined that its unauthorized disclosure could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by increasing significantly the likelihood of the illegal production of nuclear weapons or the theft, diversion, or sabotage of DoD SNM, equipment, or facilities.
- Unclassified Technical Data. Data that is not classified, but is subject to export control and is withheld from public disclosure according to DoD Directive 5230.25 (reference (ai)).
- Proprietary. Information that is provided by a source or sources under the condition that it not be released to other sources.

Tactical Network – The portion of the GIG (or ARNG GuardNet) network which is essential to theater-level and below-theater-level commanders for planning, directing, and controlling operations, providing the conveyance and/or exchange of data and information from one person or force to another.

WAN – A Network that spans a relatively large geographical area. Typically a WAN consists of two or more local-area networks (LANs)

Wireless – Technology that permits the active transfer of information involving emanation of energy between separated points without physical connection. Currently wireless technologies use IR, acoustic, RF, and optical but, as technology evolves, wireless could include other methods of transmission.

WPAN – A system that provides electromagnetic communication connectivity over a few yards. Currently it uses either RF (e.g., Bluetooth) or IR technology.