

**Program Executive Office Ammunition**

**(PEO AMMO)**

**Information Assurance (IA) Policy for Developmental Systems**

**DRAFT**



A handwritten signature in black ink, appearing to read "P. S. Izzo", written over a horizontal line.

**Paul S. Izzo**  
**Brigadier General, USA**  
**Program Executive Officer for AMMO**

3 Dec 2003  
Date

## Table Of Contents

Applicability.....	3
1.0 Introduction.....	3
1.1 Purpose.....	3
1.2 References.....	3
1.3 Responsibilities.....	5
1.4 IA Training.....	9
2.0 IA Policy.....	9
2.1 General Policy.....	9
2.2 Minimum Requirements.....	9
2.3 Marking.....	11
2.4 Mission Assurance Category, Confidentiality Level, Level of Total System Exposure and Mode of Operation.....	11
2.5 Software Security.....	11
2.6 Physical Security.....	12
2.7 User Identification and Password Control.....	13
2.8 Personnel Security.....	13
2.9 Systems Media.....	14
2.10 Miscellaneous Provisions.....	14
2.11 Secure Configuration.....	14
2.12 Command and Control (C2) Protect Tools (C2P Tools).....	15
2.13 Information Assurance Vulnerability Alert Process.....	15
3.0 Certification and Accreditation.....	16
4.0 Communications Security (COMSEC).....	16
6.0 Encryption and Key Management.....	17
Appendix I - Acronyms and Abbreviations.....	18
Appendix II - Definitions.....	21
Appendix III - Additional Reference Documents.....	25
Appendix IV - Information Assurance Resource Links.....	26

**Summary.**

This document establishes policies and procedures for achieving acceptable levels of information assurance for all developmental Information Systems (IS) administered by the Program Executive Office Ammunition (AMMO) Information Assurance (IA) Program, and reflects the objectives and requirements of AR 25-1, AR 380-5 and AR 380-19. When this policy conflicts with individual systems security policies, Army, or DoD policy, the more stringent policy will apply.

**Applicability.**

This policy applies to all parties who access the PEO AMMO developmental Automated Information Systems to include assigned personnel, contractor representatives, and data communications systems. This policy does not apply to business enterprise information systems.

**1.0 Introduction.**

**1.1 Purpose.**

- a. This policy establishes the PEO AMMO IA Program to ensure that appropriate measures are taken for the integration of security in the development and operation of automated information systems, and to protect sensitive and critical information and information resources.
- b. This policy addresses and implements Department of the Army (DA) policies for the protection of sensitive and critical information and information resources, as established by AR 25-1, AR 380-5 and AR 380-19.

**1.2 References.**

The following publications are the regulatory sources for the information and guidance provided in this document:

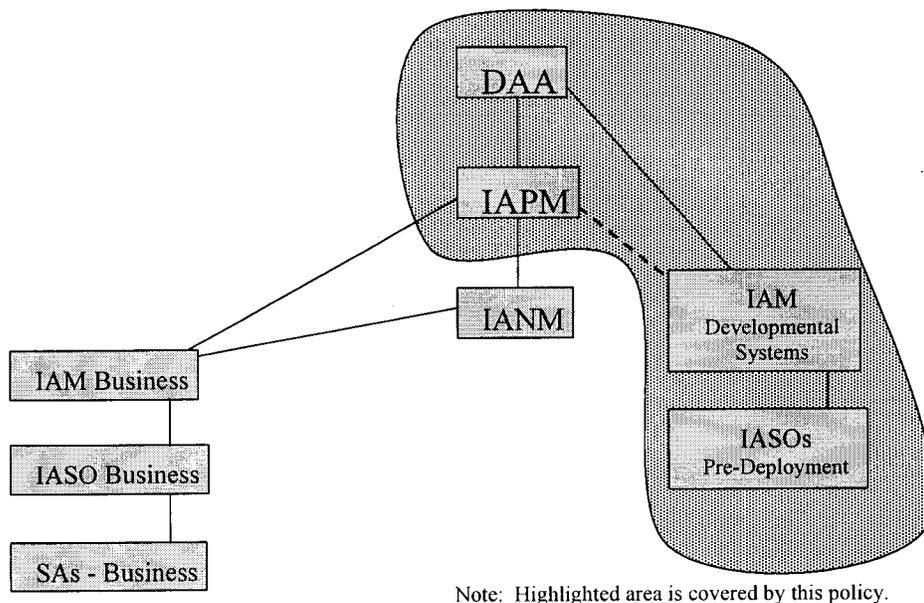
- a. DoD 5000.2-R, Mandatory Procedures for Major Defense Acquisition Programs (MDAPS) and Major Automated Information Systems (MAIS) Acquisition Programs, 5 April 2002.
- b. DoD Directive 8500.1, Information Assurance, 24 October 2002.
- c. DoD Instruction 8500.2, Information Assurance Implementation, 6 February 2003.
- d. DoD Instruction 5200-40, DoD Information Technology Security Certification and Accreditation Process (DITSCAP), 30 December 1997.

- e. DoD 5220.22-M, National Security Program Operating Manual (NISPOM), January 1995.
- f. DoD 8510.1M, DoD Information Technology Security Certification and Accreditation Process (DITSCAP) Application Document.
- g. AR 25-1, Army Information Management, 31 May 2002.
- h. AR 25-XX, Information Assurance (Draft).
- i. AR 25-55, The DA Freedom of Information Act Program, 1 November 1977.
- j. AR 380-5, Department of the Army Information Security Program, 29 September 2000.
- k. AR 380-19, Information Systems Security, 27 February 1998.
- l. AR 380-40, Policy for Safeguarding Controlling Communications Security (COMSEC) Material, 1 September 1994.
- m. AR 380-67, Department of the Army Personnel Security Program, 9 September 1988.
- n. AR 381-14 (S), Technical Surveillance Countermeasures (TSCM and TEMPEST) (U).
- o. AR 530-1 Operational Security (OPSEC), 15 October 1985.
- p. Controlled Access Protection Profile (CAPP), Information Systems Security Organization, National Security Agency (NSA), 8 October 1999.
- q. Common Criteria for Information Technology Security Evaluation, August 1999.
- r. DA PAM 25-380-2, Security Procedures for COMSEC Controlled Items, 10 January 1991.
- s. NSTISSI #4009, National Security Telecommunications and Information Systems Security Council (NSTISSI), "National Systems Security (INFOSEC)" Glossary, September 2000.
- t. NSTISSP No. 11, National Information Assurance Acquisition Policy.
- u. FIPS 140-2, Security Requirements for Cryptographic Modules

- v. Message, HQDA, SAIS-IAS, 111300ZJUN99, subject: Army Network Security Improvement Program (NSIP) - Army Policy For The Implementing Of The Information Assurance Vulnerability Alert (IAVA) Process.
- w. Message, HQDA, SAIS-IAS, 61837ZAUG99, subject: Modification To The Dissemination Of Information Assurance Vulnerability Data.
- x. Message, HQDA, SAIS-IAS, 011530ZNOV00, subject: New Information Assurance (IA) Personnel Structure – Interim ISS Policy Change.
- y. Message, HQDA, DACS-ZB, 151830ZMAR00, subject: Information Assurance Vulnerability Alert (IAVA) Compliance.

### **1.3 Responsibilities.**

- a. The PEO AMMO is the senior IA authority for the command and is responsible for administering all aspects of the Army Information Assurance Program (AIAP). The PEO has established an IA Program personnel structure through the appointment of the Chief Information Officer as Information Assurance Program Manager (IAPM), and the delegation of Certification Authority to the Communications & Electronics Research Development and Engineering Center, Space and Terrestrial Communications Directorate (CERDEC, S&TCD) Information Assurance Product Director (IA PD). Product Managers (PdMs) fulfill the role of the DITSCAP Project Managers (PM). A hierarchical structure of functional IA positions (See Figure 1) will be implemented within subordinate PMs as follows:



**Figure 1. PEO AMMO Information Assurance Structure**

- (1) Information Assurance Program Manager (IAPM). The IAPM will promulgate IA requirements and implementation guidance within PEO AMMO developmental community, specifically, the IAPM will:
- a. Develop, manage, and maintain a formal IA security program that includes defining the IA personnel structure and ensuring the appointment of an Information Assurance Manager (IAM) and an Information Assurance Security Officer (IASO) at subordinate units as appropriate.
  - b. Develop, implement, and enforce Army and command-unique IA policy.
  - c. Ensure that IA personnel review and implement bulletins and advisories that affect the security of their information systems.
  - d. 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.
  - e. 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 Army staff on current and upcoming IA policies.
  - f. Ensure the DITSCAP program is implemented.

- g. Ensure the development of system C&A documentation by reviewing and endorsing such documentation and recommending action to the DAA.
- (2) An IAM will be appointed at PEO AMMO headquarters for developmental systems. The IAM will serve as the senior IA official and focal point of contact for all other appointed IA personnel. An IAM for Developmental Systems will be appointed and report directly to the DAA for matters involving Certification and Accreditation (C&A) of developmental and tactical systems. The IAM will be the focal point for all matters concerning IA as specified below:
- a. Develop, maintain, implement, and enforce a formal IA security and training program.
  - b. Implement IAVM dissemination, reporting, compliance, and verification procedures.
  - c. Manage IASOs, as required, to establish the scope of responsibilities and the technical and security training requirements.
  - d. Maintain training and certification records for IA personnel.
  - e. Review all IA C&A support documentation packages, and system fielding, operations, or upgrades requirements to ensure accuracy and completeness, and that they meet minimal risk acceptance standards.
  - f. Maintain, as required, a repository for all systems C&A documentation and modifications and version control.
  - g. Ensure that all ISs within the scope of responsibility are properly certified and accredited IAW DITSCAP and configuration management policies and practices before operating or authorizing the use of hardware and software on an IS or network.
  - h. Assist the IAPM to identify and validate IA resource requirements.
  - i. Provide input to the IAPM for management controls.
- (3) Information Assurance Security Officer (IASO). An IASO will be appointed for each developmental program. All PEO AMMO managed developmental systems shall have a designated Pre-deployment IASO. IASOs must be IA certified, and maintain the certification. The IASO(s) shall ensure systems within their area of responsibility are developed, operated, and maintained securely. Additionally, the IASO will perform the following:
- a. Disseminate and ensure implementation of IA policy, guidance, and training requirements.
  - b. Ensure implementation of IAVM dissemination, reporting, and compliance procedures.
  - c. Prepare, distribute, and maintain plans, instructions, and SOPs concerning system security.

- d. Review and evaluate the effects on security of system changes, including interfaces with other ISs and document all changes.
  - e. Ensure that all ISs within their area of responsibility are accredited. Develop or coordinate the development and support of C&A requirements, and initiate re-accreditation as required.
- b. The Security Manager, PEO AMMO, will assist the IAPM with program management and implementation in the areas of physical security, personnel security, document security, secure storage, COMSEC, and Special Access Programs (SAPs), IAW existing regulations and policies.
- c. Program Managers (PM) shall manage and engineer information systems using the best processes and practices known to reduce security risks, including the risks to timely accreditation. Accordingly each PM shall conduct a risk assessment, incorporate appropriate countermeasures, demonstrate effectiveness of those countermeasures through the certification process conducted in accordance with the DITSCAP during Developmental Test and Evaluation (DT&E), ensure that the Designated Approving Authority (DAA) accredits the system before fielding, and incorporate existing, or develop new, protection profiles to consolidate security-related requirements, and provide effective management oversight of the overall security program in accordance with (IAW) DoD 5000.2-R, 5 April 2002, Mandatory Procedures for Major Defense Acquisition Programs (MDAPS) and Major Automated Information Systems (MAIS) Acquisition Programs. PMs shall plan, program, and budget the resources required to ensure security requirements are met, certification is timely, and system security is maintained throughout the lifecycle of their systems consistent with DoD, Army, and PEO AMMO policy.
- d. The Designated Approving Authority (DAA) is an appointed official that has the authority to approve or disapprove information systems for operation or use, and is responsible for the overall security of the information systems under his purview. The PEO AMMO is the DAA for all PEO AMMO systems processing information up to and including the Secret sensitivity level.
- e. The Certification Authority (CA) shall support the DAA for the comprehensive evaluation of the technical and non-technical security features of the information system. When tasked by the DAA, the CA is responsible for preparation of the SSAA, and the software, hardware, TEMPEST, COMSEC, physical, and procedural evaluations. The CA shall be independent from the organization responsible for the system. Organizational independence of the CA eases the potential of conflicts of interest and permits an impartial evaluation. The CA shall have staff who are technically knowledgeable in information system design, security design, and the security policies and procedures that satisfy the IA requirements. Although all the technical capabilities may not be available in the CA's organization, the CA is responsible for obtaining the necessary support and providing the necessary oversight of the certification effort. Security teams may be formed to support the C&A or any

portion of the process; e.g., security testing. The composition, roles, responsibilities, schedules, and funding of those teams should be defined in the SSAA.

#### **1.4 IA Training.**

- a. Requirements. All personnel who manage, design, develop, maintain, or operate IS will undergo an initial and annual training and awareness program commensurate with their duties as follows:
  - (1) The IAPM/IAM must complete the IAM course within 6 months of appointment, and maintain a record of course completion.
  - (2) IASOs must complete an IASO course within 6 months of appointment by completion of Web Based training at <http://ia.gordon.army.mil>, CD ROMs, or other MACOM sponsored courses.
  - (3) Refresher training for IAM and IASO positions will mandated through attendance at an Army Information Assurance Workshop every 18 months.

#### **2.0 IA Policy**

##### **2.1 General Policy.**

Classified and Unclassified Sensitive Information residing on, or derived from, information systems will be protected against unauthorized disclosure, modification, destruction or denial of use. As such, the following requirements will be followed:

- a. All systems will be accredited under a set of security requirements and safeguards approved by the DAA prior to operation, IAW DoD Information Technology Security Certification and Accreditation Process (DITSCAP).
- b. An Interim Approval to Operate (IATO) may be granted pending completion of a formal accreditation.

##### **2.2 Minimum Requirements.**

- a. All systems processing classified or unclassified sensitive information will achieve the minimum requirements IAW AR 380-19, or AR 25-XX, Information Assurance, when published, as outlined below. The security requirements that a particular system must meet will be determined and agreed to by the DAA, Certification Authority (CA), PM, and the User Representative during Phase 1 of the DITSCAP process.

- b. Safeguards will be in place to ensure that each person having access to systems will possess the “need to know”, and requisite security clearance. They must also be held accountable for their actions through the use of audits. The audit trail will be of sufficient detail to reconstruct events in determining the cause or seriousness of compromise or damage to the system. Exceptions to this policy will be documented in the System Security Authorization Agreement (SSAA) portion of the DITSCAP and approved by PEO AMMO.
- c. IAW 380-19, each system will have access controls that will include features or procedures to ensure the identity of each authorized user is established before granting access to that system.
- d. All personnel accessing PEO AMMO information systems will have received security awareness training. All IA management personnel shall be trained, screened, and certified IAW current Army policy. Refer to Message, HQDA, SAIS-IAS, 011530ZNOV00, Subject: New Information Assurance (IA) Personnel Structure – Interim ISS Policy Change, or as stated in AR 25-XX, Information Assurance, when published.
- e. Hardware, software, documentation and all data processed by PEO AMMO systems will be protected to prevent unauthorized disclosure, destruction or modification. Software development and related activities will incorporate appropriate security measures.
- f. All systems will function so that each user has access to only the information to that he or she is entitled, established by virtue of security clearance or formal access approval.
- g. A contingency plan will be developed so that recovery procedures are available if data is modified or destroyed, or if the integrity of a system is suspect. The contingency plan should include Continuity of Operations Plan (COOP) and an emergency destruction plan. A contingency plan shall cover emergency response, back-up operations, and post-disaster recovery. The plan shall also consider natural disasters, enemy actions, and malicious attacks.
- h. Copyright Laws will be strictly adhered to, and those personnel violating such laws will be subject to disciplinary action under United States Code 17, section 504 and 506, United States Code 18-2319, and the Universal Code of Military Justice (UCMJ).
- i. Secure configuration policy (SCP) and technical policy outlined in PEO AMMO technical policy and HQDA technical policy as well as policy messages will be implemented so as to reduce the risk to the interconnected Global Information Grid (GIG). Technical requirements will be captured in the System Security Requirements Traceability Matrix (SRTM).

### **2.3 Marking.**

Markings on classified or unclassified sensitive hardware, software, or output (including media and documents) will reflect the sensitivity of the information as required by existing regulations or directives. AR 380-5 contains requirements for security classification and applicable markings for classified information. AR 25-55 contains requirements for "For Official Use Only" information. All media will be marked and protected commensurate with the requirements for the highest security classification level, and the most restrictive category of information ever stored on the media until it is declassified, destroyed or downgraded.

### **2.4 Mission Assurance Category, Confidentiality Level, Level of Total System Exposure and Mode of Operation.**

- a. PEO AMMO information systems will be categorized based on the sensitivity of information for which the system is authorized to process and/or store. As such, systems processing unclassified but sensitive information will be designated as FOUO IAW AR 380-5. Those systems processing classified information will be designated by the highest security classification, e.g., CONFIDENTIAL, SECRET, TOP SECRET, TOP SECRET/Sensitive Compartmented Information. (TS/SCI).
- b. All PEO AMMO information systems will be accredited IAW the DITSCAP and AR 380-19 or AR 25-XX, Information Assurance, when published, to meet the requirements of their mode of operation (near term) or level of total system exposure (objective). Most PEO AMMO Systems are expected to meet the AR 380-19 requirements for operation in the systems high security mode of operation at the Secret or Unclassified sensitivity level in the near term. The objective is for PEO AMMO systems to meet the corresponding level of total system exposure appropriate for their system at the confidentiality level and mission assurance category required by DoD 8500.1 IA policy. Since the Trusted Computer Security Evaluation Criteria (TCSEC) has been superseded, a valid Common Criteria (CC) protection profile will be used. The mode of operation or level of concern and level of robustness appropriate for a system will be determined and agreed upon during the Phase 1 of the DITSCAP.

### **2.5 Software Security.**

- a. Controls will be implemented to protect system software against compromise, subversion or unauthorized manipulation. As such all software used on PEO AMMO systems will be approved by the appropriate DAA, or the appropriate DAA'S representative, prior to installation and operation. All IA enabled Information Technology products (to included operating systems) shall be fully compliant with NSTISSP No. 11, National Information Assurance Acquisition Policy.

- b. Software will be kept under strict control and continuous configuration management controls from the time of its creation or introduction to any development or integration environments, at the earliest opportunity, to lessen the risk of introducing viruses, preventing theft, compromise, and untested or malicious software.
- c. AIS equipment shall be supported with a configuration distribution plan that provides for the proper and authorized physical distribution of media and related items. Further, if a configuration distribution system is to be used for software dissemination, the configuration distribution plan will document the access and downloading procedures and interfaces.

## 2.6 Physical Security

- a. Physical security requirements must be considered and selected based on the sensitivity and security classification of data being processed. Adequate physical security standards must be based on an analysis of wartime and peacetime mission criticality, sensitivity levels of the information processed, overall value of the information to the mission, local criminal and intelligence threat, and value of equipment. The PEO AMMO IA Program will include physical security measures designed through an in-depth application of barriers and procedures to accomplish the following:
  - (1) Safeguard personnel.
  - (2) Prevent unauthorized access to equipment, facilities, material, media or documents.
  - (3) Safeguard against espionage, sabotage, damage and theft.
  - (4) Reduce exposure to threats that could cause a denial of service or unauthorized alteration of data.
  - (5) Protect those unattended systems with non-removable media which process classified defense information that have not been properly declassified IAW 380-5.
- b. Workstations and personal computers will be configured to use the "idle lockout/screen saver" feature, and all users will log-off or activate the password protected screen saver when they leave their workstation or personal computer. An exception to this requirement will be made for those tactical systems that because of the function and design of the system this requirement is impractical. This situation will be addressed in the System Security Authorization Agreement (SSAA) portion of the DITSCAP as well as in the accreditation approval memorandum signed by the DAA.

## **2.7 User Identification and Password Control**

User identification (userID) and password control meet the minimum requirements of system accountability, access control, least privileged, and data integrity. As such the following guidelines will be followed:

- a. After creation, passwords will be handled at the same sensitivity level of data contained on the system.
- b. Root and/or administrator passwords will be restricted to the absolute minimum number of personnel necessary to manage the system.
- c. All users will be briefed on password security guidelines when userIDs and passwords are assigned. Password security guidelines and userID passwords will be incorporated into local SOPs, IAW AR 380-19, or 25-XX when approved.
- d. Systems which process classified or unclassified sensitive information will limit the number of user log-on attempts to three before denying access to that user. An exception to this requirement will be made for those tactical systems that because of the function and design of the system this requirement is impractical. This situation will be addressed in the SSAA as well as in the accreditation approval memorandum signed by the DAA.
- e. The password complexity rules and other technical requirements will be IAW current Army policy.

## **2.8 Personnel Security**

- a. All individuals who are appointed to IA duties must complete IA training equal to the duties assigned them.
- b. All personnel who manage, design, develop, maintain or operate information systems will undergo IA training that will consist of threats, vulnerabilities, risks associated with the system, and information security objectives.
- c. Personnel who require access to systems processing classified information will possess a security clearance based on the appropriate personnel security investigation as delineated in AR 380-67. Exceptions to this policy will be documented in the DITSCAP, and approved by the DAA.
- d. Foreign national employees will not be assigned position granting them access to classified information prior to meeting the provisions for a limited access authorization under the provisions of AR 380-67.

## 2.9 Systems Media

- a. General requirements for accountability, receipting, transmission and all other measures for classified material prescribed in AR 380-5 will apply to systems media as appropriate to its classification. As such, users of classified media will handle and protect such media in accordance with the procedures of AR 380-5 until the media is properly declassified or destroyed.
- b. All media will be properly marked according to the highest accreditation level of the system in which they are operating IAW AR 380-5.

## 2.10 Miscellaneous Provisions

- a. Remote systems and devices will be secured consistent with the mode of operation and information that the remote terminal is authorized to access.
- b. Laptop, notebook computers, or any other computer used as a part of developmental/tactical systems and designed to all allow periodic relocation, must be accredited in accordance with this policy. Classified processing may be done on mobile computers if it is accomplished in normal work areas acceptable for the storage, preparation, or discussion of classified material.
- c. Ports, protocols, and services (PPS) that are not required will be denied at the network level and disabled at the system level. Systems connecting to the Secret IP Router Network (SIPRNET) or Unclassified but sensitive (N-level) Internet Protocol Router Network (NIPRNET) must meet current Army and/or DISA Connection Approval Process policy.
- d. The acquisition and use of wireless communication solutions and PEDs (data enabled cellular phones, tow-way pagers, personal digital assistants (PDA), and handheld/laptop computers with wireless connectivity capabilities) shall comply with the U.S. Army Wireless Local Area Networks (LAN) and Wireless Portable Electronic Devices (PED) Policy.

## 2.11 Secure Configuration

- a. The system developers, integrators and IASOs will ensure that the configuration of their systems conform to the guidance found in DoD and Army technical policies and guides
- b. IASOs will subscribe to the Army Knowledge On-line (AKO) and monitor it on a routine basis for updated policy that they will implement for their systems. It is

expected that IASOs will continually manage risks to their systems throughout the system's lifecycle.

- c. In certain instances, implementation of a technical security policy requirement using a specified procedure or incorporating a mandated fix results in unacceptable impacts to mission critical functionality. If a required fix or configuration is not integrated for this reason, then the resultant vulnerability must be addressed and countermeasures identified in the system's Residual Risk Assessment Results (RRAR) submitted as part of the systems accreditation or IATO package. The deviation must be approved IAW current Army and PEO AMMO policy, which is outlined in the PEO AMMO Secure Accreditation and Management Plan (SAMP), which outlines the procedural details unique to PEO AMMO developmental and tactical systems.

### **2.12 Command and Control (C2) Protect Tools (C2P Tools)**

All systems will incorporate C2 Protect Tools and Antivirus software IAW Army policy. IASOs shall obtain the agreement of the PEO AMMO IAM, as the DAA representative, or the applicable DAA, to establish which tools they must integrate into their systems. This agreement will be accomplished during Phase 1 of the DITSCAP described in DoD Instruction (DoDI) 5200.40. C2 Protect Tools and Antivirus Software will be configured and maintained IAW Army policy. Other IA tools that will be incorporated into the systems shall comply with Army Chief Information Officer/G-6 (CIO/G-6) policy and be approved by the system's DAA representative before the tools are integrated into the system's baseline.

### **2.13 Information Assurance Vulnerability Alert Process**

- a. Computer Network Attack (CNA) is one of the significant threats identified in the Army Battle Command System (ABCS) and GIG Capstone Requirements Documents (CRDs). CNA includes operations that an enemy undertakes to disrupt, deny, degrade or destroy information resident in computers and computer networks, and involves the use of network and computer hacking techniques to deny, modify, or disclose information in an unauthorized manner.
- b. All PEO AMMO IASOs will register with the Army Computer Emergency Response Team (ACERT)/Computer Network Operations Division (CNOD), <https://www.acert.lstiocmd.army.mil/ACERTmain.htm> so that they receive IAVA Alerts and Bulletins. They will also ensure that their system developers, maintainers and integrators monitor the ACERT/CNOD for IAVA alerts and bulletins and implement the fixes necessary to ensure that the security of their system is maintained and proper reporting is conducted for all systems.

- c. The PEO and PMs must ensure that subordinate units/elements/activities/ programs maintain a configuration baseline on systems for which they have post production software support (PPSS) responsibilities.
- d. The PEO and PMs are responsible for comparing IAVA messages against system baselines and taking appropriate action to ensure the system meets the IAVA directed standard.

### **3.0 Certification and Accreditation**

- a. Accreditations will be accomplished using the DITSCAP. A System Security Authorization Agreement (SSAA) shall be prepared during each of the four phases of development namely; definition, verification, validation and post accreditation. Accreditations will also address each system's external connection perimeter, its accreditation boundary, and its relationship to other systems and networks. System equipment and peripherals within the system perimeter must be specifically identified in the SSAA accreditation document, and equipment or peripherals accessing the system from outside the system perimeter must also be addressed in the SSAA. The procedures and requirements for Certification and Accreditation (C&A) under the DITSCAP process for developmental systems are contained in the PEO AMMO SAMP. The SAMP outlines the procedural details unique to PEO AMMO developmental and tactical systems. Since IA technical policy and best practices are constantly being improved, the detailed procedures and templates implementing the DITSCAP for PEO AMMO systems will be posted to the IA site on the Army Knowledge Online (AKO). This assures that the best and most current practices are being used while maintaining consistency in the high-level policy and approach.
- b. The certification and accreditation of systems is a technical evaluation of the effectiveness of system security features, which support the accreditation decision. Certifications will verify that security functions are correctly implemented and sufficient to support the mode of operation and the security policy for the system in an intended operational environment. All certification efforts will address software, hardware, and firmware security measures, as well as procedural, physical and personnel security measures. The CA shall ensure that the certification team has members with composite expertise in the whole span of activities required for certification and accreditation who are independent of the system developer or product manager. Since the CA should be independent from the organization responsible for the system development or operation, CERDEC, S&TCD IA PD will act as certification authority for all PEO AMMO systems.

### **4.0 Communications Security (COMSEC)**

- a. Communications security techniques will be applied to the extent necessary to deny information to unauthorized personnel and to effectively defend against interception, traffic analysis and deception. As such, COMSEC objectives will be an integral part of program planning for all telecommunications systems.
- b. AR 380-40 and DA PAM 25-380-2 govern safeguarding and controlling COMSEC material.
- c. Only NSA endorsed COMSEC products shall be used to protect Confidential, Secret, Top Secret and SCI.
- d. Cryptographic systems or products intended for the protection of unclassified sensitive information and systems shall employ cryptographic modules that have been validated under the National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) as meeting, at a minimum, Level 2 security requirements of the Federal Information Processing Standard 140-2 (FIPS 140-2). Note: Per AR 25-XX, Information Assurance, all tactical information systems are considered as being critical to the direct fulfillment of military or intelligence missions, and therefore are regarded as national security systems. Therefore, they will require the use of NSA endorsed COMSEC products.

## **5.0 Transmission Security and TEMPEST**

- a. Transmissions will be protected by the application of measures designed to protect the information from interception and exploitation by means other than crypto-analysis IAW NSTISSI 4009.
- b. All data paths will be protected from "red" and "black" data contamination or unobserved emanations IAW NSTISSAM TEMPEST/1-92 and NACSEM 5112. Emanation security shall comply with the provisions of AR 381-14, Technical Surveillance Countermeasures (TCSM and TEMPEST).

## **6.0 Key Management**

All cryptographic systems employed in the tactical force structure must be capable of being supported by the Army Electronic Key Management System (EKMS)/Key Management Infrastructure (KMI). Systems not capable of being supported by Army EKMS shall be identified as non-compliant and phased out of service as soon as possible. Each approved cryptographic system shall have a Key Management Plan that describes in detail all activities involved in the handling of cryptographic keying material for the system, including other related security parameters (such as ID's and passwords). The plan shall describe accountability over the keying material over the entire life cycle of the systems keys from generation, storage, distribution and entry into the system, through use, deletion, and final destruction.

## **Appendix I - Acronyms and Abbreviations**

<b>AIAP</b>	Army Information Assurance Program
<b>AIS</b>	Automated Information System(s)
<b>AKO</b>	Army Knowledge Online
<b>AMMO</b>	Ammunition
<b>AR</b>	Army Regulation
<b>AV</b>	Anti-Virus
<b>C&amp;A</b>	Certification and Accreditation
<b>C2</b>	Command and Control
<b>C2P</b>	Command and Control Protect
<b>CAPP</b>	Controlled Access Protection Profile
<b>CERDEC</b>	Communications & Electronics Research Development and Engineering Center
<b>CERT</b>	Computer Emergency Response Team
<b>CNA</b>	Computer Network Attack
<b>COMSEC</b>	Communications Security
<b>COOP</b>	Continuity of Operations Plan
<b>CTSF</b>	Central Technical Support Facility
<b>DAA</b>	Designated Approving Authority
<b>DITSCAP</b>	Defense Information Technology Security Certification and Accreditation Process
<b>DoD</b>	Department of Defense
<b>DT&amp;E</b>	Developmental Test and Evaluation
<b>FOUO</b>	For Official Use Only

<b>GIG</b>	Global Information Grid
<b>HQDA</b>	Headquarters, Department of the Army
<b>INFOSEC</b>	Information Security
<b>IA</b>	Information Assurance
<b>IANM</b>	Information Assurance Network Manager
<b>IAPD</b>	Information Assurance Product Director
<b>IAPM</b>	Information Assurance Program Manager
<b>IAM</b>	Information Assurance Manager
<b>IASO</b>	Information Assurance Security Officer
<b>IATO</b>	Interim Approval to Operate
<b>IAVA</b>	Information Assurance Vulnerability Alert
<b>IAVM</b>	Information Assurance Vulnerability Management
<b>IAW</b>	In accordance with
<b>IS</b>	Information System
<b>MAIS</b>	Major Automated Information Systems
<b>MDAP</b>	Major Defense Acquisition Program
<b>NIPRNET</b>	Unclassified but sensitive (N-level) Internet Protocol Router Network
<b>NISPOM</b>	National Security Program Operating Manual
<b>NSTISSAM</b>	National Security Telecommunications and Informations Systems Security
<b>NTISSP</b> Policy	National Telecommunications and Information Security System (NTISS) Policy
<b>OPSEC</b>	Operational Security
<b>PDA</b>	Personal Digital Assistant

<b>PED</b>	Portable Electronic Device
<b>PEO AMMO</b>	Program Executive Officer, Ammunition
<b>PM</b>	Program Manager
<b>PPS</b>	Ports, Protocols, and Services
<b>SIPRNET</b>	Secret IP Router Network
<b>S&amp;TCD</b>	Space and Terrestrial Communications Directorate
<b>SAP</b>	Special Access Program
<b>SAMP</b>	Secure Accreditation and Management Plan
<b>SRTM</b>	System Security Requirements Traceability Matrix
<b>SSAA</b>	System Security Authorization Agreement
<b>TCSM</b>	Technical Surveillance Countermeasures
<b>TS/SCI</b>	Top Secret/Special Compartmented Information
<b>TT</b>	Technology Transition
<b>UIC</b>	Unified Infosec Criteria

## Appendix II - Definitions

**Access** – To view, receive, or derive information from an information system and the work performed thereon.

**Accessibility** – Having the ability to access to an information system or activity, but not necessarily the ability to actually view, receive or derive information.

**Access Control** – Processes and procedures to limit access to the resources of an information system only to authorized personnel.

**Accreditation** – Formal approval by a DAA for the operation or use of an information system; accreditation decisions are based on a review of the threats, vulnerabilities and risks associated with such use, and the security countermeasures implemented or required to reduce or eliminate the risk.

**Accountability** – Software or property that enables auditing of activities on an information system to be traced to persons who may then be held responsible for their actions.

**Audit** – The independent review and examination of the system's records and activities to test for adequacy of the system's controls, to ensure compliance with established policy and operational procedures, or to recommend any needed changes in controls, policy or procedures.

**Audit Trail** – A chronological record of system activities to enable the reconstruction, reviewing and examination of the sequence of events and/or changes in an event.

**Certification** – Comprehensive evaluation and agreement of the technical and non-technical security features of an information system and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design and implementation meets at set of specified security requirements.

**Classified Defense Information** – Official information regarding the national security that has been designated top secret, secret, or confidential in accordance with Executive Order 12356.

**Clearing** – Removal of data from an information system, its storage devices, and other peripheral devices with storage capability.

**Communications Security (COMSEC)** – Measures and controls taken to deny unauthorized person information derived from telecommunications and to ensure the authenticity of such telecommunications.

**Configuration Control** – The process of controlling modifications to a telecommunications or automated information systems hardware, firmware, software and documentation to ensure the system is protected against improper modifications prior to, during and after system implementation.

**Declassification** – An administrative procedure resulting in a determination that classified information formerly stored on a magnetic medium has been removed or overwritten sufficiently to permit reuse in an unclassified environment.

**Dedicated Mode** – A mode of operation wherein each user, with direct or indirect access to the system, its peripherals, remote terminals, or remote hosts, has all of the following:

- a. Valid security clearance for all information within the system.
- b. Formal access approval and signed non-disclosure agreements for the information stored and/or processed on the system.
- c. Valid need-to-know for all information contained within the information system.

**Degauss** – Destroy information contained in magnetic media by subjecting that media to high-intensity alternating magnetic fields, following which the magnetic fields slowly decrease.

**Designated Approving Authority** – Official with the authority to formally assume responsibility for operating an information system or network at an acceptable level of risk.

**Firmware** – Software that is permanently stored in a hardware device that allows reading and executing the software, but not writing or modifying it.

**Information Assurance** – The protection of information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. It includes providing for restoration of information systems by incorporating protection, detection and reaction capabilities.

**Information System** – 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.

**Least Privilege** – Principle that requires each person be granted the most restrictive set of privileges needed for the performance of authorized tasks.

**Multilevel (security) Mode** – A mode of operation wherein all the users who have direct or indirect access to the system do not have a valid security clearance for all of the

information processed in that system, or all users have the proper security clearance and appropriate formal access approval for that information to which they have access.

**Multilevel Security** – Concept of processing information with different classifications and categories that simultaneously permits access by users with different security clearances, but prevents users from obtaining access to information for which they lack authorization.

**Need-to-know** –The necessity for access to, knowledge of, or possession of specific information required to carry out official duties.

**Network** – Communications medium and all components attached to that medium whose function is the transfer of information. Components may include AIS, packet switches, telecommunications controllers, key distribution centers, and technical control devices.

**Password** – A protected or private alphanumeric character string used to authenticate an identity or to authorize access to data.

**Purge** – Removal of data from an information system, its storage devices or other peripheral devices with storage capacity in such a way that the data may not be reconstructed. Purging is one prerequisite to declassification of magnetic media.

**Remote Terminal** – A terminal which is not in immediate vicinity of the information system it accesses. Terminals usually can operate in a stand-alone mode.

**Risk** – The probability that a particular threat will exploit a particular vulnerability of an automated information system or telecommunications system.

**Systems High Security Mode** – A mode of operation wherein a system is specifically and exclusively dedicated to and controlled for the processing of one particular type or classification of information, either for full-time operation or for a specified period of time. Additionally, each user, with direct or indirect access to the information system, its peripherals, remote terminals, or remote hosts, has all of the following:

- a. Valid security clearance for all information within an information system.
- b. Formal access approval and signed non-disclosure agreements for all the information stored and/or processed.
- c. Valid need-to-know for some of the information contained within the information system.

**Telecommunications System** – Any system that transmits, receives, or otherwise communicates information by electrical, electromagnetic, electromechanical, or electro-

optical means. A telecommunications system may include features normally associated with computers, in which case it must also meet the requirements for an information system.

**Threat** – Capabilities, intentions, and attack methods of adversaries to exploit, or any circumstance or event with the potential to cause harm to information or an information system.

**Unclassified Sensitive Information** – Unclassified-sensitive information is that which the loss, misuse, or unauthorized access to or modification of, could adversely affect the national interest, the conduct of Federal programs, or the privacy to which individuals are entitled under the Privacy Act.

**User** – A person or process accessing an information system by direct connections, e.g., via terminals, or indirect connections.

**User ID** – Unique symbol or character string that is used by an information system to uniquely identify a specific user.

**Virus** – A self-replicating, malicious program segment that attaches itself to an application program or other executable system component and may or may not leave external signs of its presence.

**Vulnerability** – A weakness in an information system, or components such as system security procedures, hardware design, or internal controls that could be exploited.

### **Appendix III - Additional Reference Documents**

HQDA, SAIS-IAS, Letter 15 April 2002, U.S. Army Wireless Local Area Networks (LAN) and Wireless Portable Electronic Devices (PED) Policy

HQDA, SAIS-IAS, Message 271000ZApr01, SIPRNET Security Policy

HQDA, DAMO-FDC, Letter, Army Policy of Vulnerability Assessment of Information Technology

HQDA, SAIS-IAS, Memorandum 11 May 01, Policy Guidance for Use of Mobile Code Technologies in Department of Defense (DoD) Information Systems

HQDA, DACS-ZB, Message 160453ZJan01, IAVA Compliance

HQDA, DACS-ZB, Message 151830ZMar00, IAVA Compliance

HQDA, SAIS-IAS, Message 99-031, ACERT/CC Information Assurance Vulnerability Alert (IAVA) Compliance Message 99-031, Security Windows NT 4.0 Server Workstation

HQDA, SAIS-IAS, Message 102045ZNov99NSIP, IAVA Compliance Verification Assessment

HQDA, SAIS-IAS, Message 111300ZJun99NSIP, Army Policy for the Implementation of IAVA Process

HQDA, SAIS-IAS, Message 150951Mar99, Procedural Guidance For UNIX Systems

PEO C3S, Policy 7 July 2000, Security Configuration Policy (SCP) For Windows NT Hosts

PEO C3S, Policy 12 March 1999, Secure Configuration Policy (SCP) for UNIX Hosts

These references may also be relevant (analysis is underway):  
National Security Agency Security Recommendation Guides for Windows XP, 2000, and NT, <http://nsa2.www.conxion.com/>

DISA's Information Assurance Support Environment, includes UNIX and Windows XP, 2000, and NT Guidance, <https://iase.disa.mil/documentlib.html#TECHGUIDOCS>

## Appendix IV - Information Assurance Resource Links

U. S Army Computer Emergency Response Team (ACERT) – access to ACERT links requires that users enter the site from a .mil domain, or that users have an active AKO account.

<https://www.acert.belvoir.army.mil/ACERTmain.htm>

<https://www.acert.1stiocmd.army.mil/ACERTmain.htm>

Army Authorized Information Assurance Tool Page:

<https://www.acert.belvoir.army.mil/tools/tools.htm>

Army Blanket Purchase Agreement (BPA) Products:

<https://www.acert.belvoir.army.mil/tools/csla.htm#network>

ACERT Security Service Packs/Patches:

<https://www.acert.belvoir.army.mil/security.htm>

Army on-line Portal (Army Knowledge On-line (AKO)) and form to register for access to AKO and Army Information Assurance – you must register for access:

[https://www.us.army.mil/portal/portal\\_home.jhtml](https://www.us.army.mil/portal/portal_home.jhtml)

Army Information Assurance:

[https://informationassurance.us.army.mil/mem\\_bin/FormsLogin.asp?/](https://informationassurance.us.army.mil/mem_bin/FormsLogin.asp?/)

AMC IA Policy Table with links to DoD resources:

[http://www.amc.army.mil/amc/ci/matrix/policy/policy\\_new.htm](http://www.amc.army.mil/amc/ci/matrix/policy/policy_new.htm)

Army Team C4IEWS:

<http://www.monmouth.army.mil/>

Army Training and Doctrine Digital Library (Field Manuals, Soldier Training Publications, etc.) – must register for access to some portions of this site:

<http://www.adtdl.army.mil/atdls.htm>

Common Criteria Project

<http://csrc.nist.gov/cc/index.html>

Common Operating Environment (COE)

<http://diicoe.disa.mil/coe/>

DoD Chief Information Officer (CIO) Guidance and Policy Memorandums (G&PMs)

This site contains the Global Information Grid (GIG) series policies.

<http://www.c3i.osd.mil/org/cio/gpmlinks.html>

Defense Technical Information Center:

<http://www.dtic.mil/>

Defense Acquisition Deskbook – provides references to acquisition resources some of which are applicable to IA and useful for Pre-deployment IASOs

<http://web2.deskbook.osd.mil/>

DISA Information Assurance Support Environment (Policy and authoritative DITSCAP Information) – must be coming from a .mil domain for access to some portions of the site:

<http://iase.disa.mil/policy.html>

DISA Information Assurance:

<http://iase.iiie.disa.mil/>

Defense Information Systems Agency:

<http://www.disa.mil/>

Defense Security Service:

<http://www.dss.mil/index.htm>

DII COE Documentation:

[https://dod-ead.mont.disa.mil/cm/cm\\_page.html](https://dod-ead.mont.disa.mil/cm/cm_page.html)

DoD Directives and Publications: Washington Headquarters Services Directives and Records Division:

<http://www.dtic.mil/whs/directives/index.html>

Fort Gordon Information Assurance Web Site (Links to Army IA Training)

<http://ia.gordon.army.mil>

GOVBOT – Database of Government Web Sites:

<http://ciir.cs.umass.edu/govbot/>

Information Assurance Technical Framework (authoritative source for Protection Profiles  
[http://www.iatf.net/protection\\_profiles/profiles.cfm](http://www.iatf.net/protection_profiles/profiles.cfm)) – must register for access to some  
portions of this site:

<http://www.iatf.net/>

Joint Electronic Library:

<http://www.dtic.mil/doctrine/>

Microsoft 2000 Hardening

NSA documents <http://nsa1.www.conxion.com/> and Microsoft's Knowledge base,  
<http://search.support.microsoft.com/kb/>

NSTISSAM TEMPEST/2-95, RED/BLACK INSTALLATION GUIDANCE, 12 DEC 95

<http://cryptome.org/tempest-2-95.htm>

National Infrastructure Protection Center:

<http://www.nipc.gov/index.html>

National Security Telecommunications and Information Systems Security Committee:

<http://www.nstissc.gov/html/library.html>

National Information Assurance Partnership (NIAP) Home Page:

<http://niap.nist.gov/>

NIST Computer Security Resource Center:

<http://csrc.nist.gov/>

NIST Registry of Protection Profiles:

<http://niap.nist.gov/cc-scheme/PPRegistry.html>

NIST Cryptographic Module Verification (CMV) Program:

<http://csrc.nist.gov/cryptval/>

PEO C3S Knowledge Center (KC) Public Site – You must go to this site to register before accessing other KC sites:

<http://www.monmouth.army.mil/newpages/vCpeoc3s.html>

Signal Center Doctrine

<http://www.doctrine.gordon.army.mil/>

Secretary of the Army (Acquisition, Logistics and Technology)

<https://webportal.saalt.army.mil>

U.S. Army Publishing Agency Home Page (Authoritative source for Army Regulations and Forms)

<http://www.usapa.army.mil/>