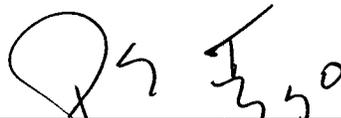


**Program Executive Office Ammunition
(PEO-AMMO)
Security / Accreditation Management Plan
(SAMP)**



Approved:



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

3 Dec 2003
Date

CONTENTS

Section	Page
SECTION 1 INTRODUCTION	4
1.1 SCOPE AND PURPOSE	4
1.2 DOCUMENT ORGANIZATION	4
1.3 REFERENCES AND RELATED DOCUMENTS	4
1.4 SUPERCESSION NOTICE	5
 SECTION 2 THE ACCREDITATION PROCESS	 6
2.1 OVERVIEW	6
2.2 SECURITY PROFILES	8
2.3 ACCREDITATION MILESTONES	8
2.4 INTERIM APPROVAL TO OPERATE (IATO) PACKAGES	8
2.5 TYPE ACCREDITATION PACKAGES	9
2.6 COMMAND AND CONTROL (C2) PROTECT TOOLS	9
2.7 CONTROLLED CRYPTOGRAPHIC ITEM (CCI)	9
2.8 MAINTAINING ACCREDITATION	9
2.9 TESTING	10
2.10 RESIDUAL RISK ASSESSMENT RESULTS (RRAR)	11
2.11 SECURITY CLASSIFICATION GUIDE (SCG) AND CLASSIFICATION OF DOCUMENTS	13
2.12 REACCREDITATION	13
2.13 INFORMATION ASSURANCE VULNERABILITY ASSESSMENT (IAVA) ALERT COMPLIANCE	13
2.14 PROPRIETARY INFORMATION	13
2.15 COMPETITION SENSITIVE INFORMATION	13
2.16 SENSITIVE INFORMATION	14
2.17 INCIDENT REPORTS	14
 SECTION 3 ORGANIZATION AND RESPONSIBILITIES	 15
3.1 DESIGNATED APPROVING AUTHORITY (DAA)	15
3.2 CERTIFICATION AGENT	15
3.3 COORDINATION WITH MAJOR ARMY COMMANDS (MACOMS)	16
3.4 INFORMATION ASSURANCE MANAGER (IAM) FOR DEVELOPMENTAL SYSTEMS ...	16
3.5 PROGRAM/PROJECT MANAGER (PM)	17
3.6 PRE-DEPLOYMENT INFORMATION ASSURANCE SECURITY OFFICER (IASO)	17
3.7 POST-DEPLOYMENT IASO	17
3.9 PEO AMMO SECURITY FORUMS	19
3.9.1 INFORMATION ASSURANCE (IA) INTEGRATED PRODUCT TEAM (IPT)	19
3.9.2 ACCREDITATION WORKING GROUPS (AWG)	19
 SECTION 4 CERTIFICATION AND ACCREDITATION	 20
4.1 CERTIFICATION TESTER INDEPENDENCE	20
4.2 SECURITY WAIVER PROCEDURE	20
4.2.1 SECURITY WAIVER NEED	20
4.2.2 SECURITY WAIVER REQUEST	21
4.3 STAFFING PROCESS	21
4.3.1 STAFF SUMMARY SHEET	21
4.3.2 RISK STATEMENTS ON THE SUMMARY SHEET	21

SECTION 5 RISK MANAGEMENT	22
5.1 RISK MANAGEMENT PROGRAM NEED	22
5.2 RISK ASSESSMENT PROCESS.....	22
5.3 MINIMUM REQUIREMENTS FOR A RISK ASSESSMENT.....	22
5.4 RISK MANAGEMENT THROUGH THE LIFECYCLE PHASES	22
5.5 DEVELOPING VALID COUNTERMEASURES	22
5.6 DEFINING AND ANALYZING THE THREAT	23
5.7 PRE-DEPLOYMENT IASO INVOLVEMENT	24
5.8 EFFECTIVENESS REVIEWS	24
SECTION 6 TEMPEST	25
SECTION 7 INFORMATION ASSURANCE VULNERABILITY MANAGEMENT	27
APPENDIX A ACRONYMS	27
APPENDIX B DEFINITIONS	30
APPENDIX C SSAA OUTLINE	32
APPENDIX D REACCREDITATION ASSESSMENT ADDENDUM AND IATO PROCESSES	39

SECTION 1 INTRODUCTION

1.1 SCOPE AND PURPOSE

The Office of the Assistant Secretary of Defense has established the Department of Defense (DoD) Directive 5200.40, DoD Information Technology Security Certification and Accreditation Process (DITSCAP), as the standard security Certification and Accreditation (C&A) process for all DoD components. The purpose of the Program Executive Office for Ammunition (PEO AMMO) Security / Accreditation Management Plan (SAMP) is to provide guidance for conducting security accreditations in accordance with the DITSCAP for all developmental/tactical Automated Information Systems (AISs) under the jurisdiction of PEO AMMO. This SAMP applies to all Program / Project Managers (PMs) and Product Managers (PdMs) developing, acquiring, and fielding systems, under PEO AMMO.

This SAMP provides general instructions for implementing the DITSCAP for collateral PEO AMMO systems.

1.2 DOCUMENT ORGANIZATION

This document is organized as follows:

Section 1 identifies the scope and purpose, organization of this document, and applicable references.

Section 2 provides an overview of the accreditation process.

Section 3 provides an overview of organizations and their associated responsibilities.

Section 4 documents the need for certifier independence and the procedure for security waivers.

Section 5 discusses risk management.

Section 6 describes the current procedure for addressing TEMPEST requirements.

1.3 REFERENCES AND RELATED DOCUMENTS

AR 380-5	Department of the Army Information Security Program, 29 September 2000
AR 380-19	Information Systems Security, 27 February 1998
AR-381-14	Technical Counterintelligence (TCI) (U)
AR 25-1	Army Information Management, 31 May 2002
AR 25-XX	Information Assurance(will supercede AR 380-19 when signed)
CAPP	Controlled Access Protection Profile, Version 1.d, 8 October 1999
Common Criteria	Common Criteria for Information Technology Security Evaluation, August 1999, Version 2.1, CCIMB-99-031;032;033, ISO/IEC 15408:1999
DA PAM 73-7	Software Test and Evaluation Guidelines, 25 July 1997
DoD 5000.2-R	Mandatory Procedures for Major Defense Acquisition Programs (MDAPS) and Major Automated Information Systems (MAIS) Acquisition Programs, 5 April 2002
DoDD 8500.1	Department of Defense Directive Information Assurance, October 24, 2002

DoD 8510.1-M	Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP), Application Manual, July 31 2000
DoDI 5200.40	Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP), Instruction, December 30 1997
(no number)	Digitization Security Classification Guide (Army Digitization Initiative Security Classification Guide), 16 July 1996
LSPP	Labeled Security Protection Profile, Version 1.b, 8 October 1999
NSTISSAM TEMPEST 2-95	National Security Telecommunications and Information Systems Security Advisory Memorandum - Red/Black Installation Guidance, 12 December 1995
NSTISSI No. 4009	National Security Telecommunications and Information Systems Security Instruction - National Information Systems Security (INFOSEC) Glossary, September 2000
NSTISSI No. 7000	National Security Telecommunications and Information Systems Security Instruction - TEMPEST Countermeasures for Facilities (U), 29 November 1993
NSTISSP No. 11	National Information Assurance Acquisition Policy
NSTISSP No. 200	National Security Telecommunications and Information Systems Security - National Policy on Controlled Access Protection, 15 July 1987
(no number)	Deputy Secretary of Defense Memorandum, Defense Acquisition, October 30, 2002
(no number)	PEO AMMO Information Assurance Policy for Developmental Systems, 30 September 2003.
www.us.army.mil/portal/portal_home.jhtml	Army Knowledge Online (AKO) Information Assurance
lase.disa.mil	Information Assurance Support Environment (IASE)

1.4 Supercession Notice

Not applicable. This is the initial version.

SECTION 2 THE ACCREDITATION PROCESS

2.1 OVERVIEW

Accreditation is a formal declaration by a designated approving authority that an Army Information System (AIS) is approved to operate in a particular security mode using a prescribed set of safeguards. Accreditation is based on an evaluation of the security risks associated with operating the system. The requirement for accreditation applies to all Army AISs, and is required for interoperability testing, exercises, demonstrations, and fielding.

An accreditation can be granted for a maximum of three years. An interim approval to operate (IATO) may be granted for a maximum of 180 days when an AIS does not meet all the applicable security requirements but the mission of the system is so critical that the risk must be accepted for a limited time.

In order to facilitate accreditation management, the accreditation process for an AIS begins with registering the AIS with the PEO AMMO in accordance with DITSCAP Phase 1 requirements. Registration is the process in Phase 1 that initiates the dialog among the Project/Product Manager (PM), the Designated Approving Authority (DAA), the Certification Authority (CA), and the System User Representative. Registration begins with a review of the mission need and concludes with preparation of an initial draft of the System Security Authorization Agreement (SSAA).

Registration tasks guide the collection of necessary information to address the process in a repeatable, understandable, and effective manner. These tasks identify the information necessary for determining security requirements and the level of effort to accomplish the Certification and Accreditation (C&A) that is influenced by the degree of assurance needed in the areas of confidentiality, integrity, availability, and accountability. During registration, information is collected and evaluated, security requirements are determined, risk management and vulnerability assessment actions begin, and the level of effort required for C&A is determined and planned.

For Phase 1 (Definition), PEO AMMO requires a completed SSAA with Appendices A through F. Phase 1 SSAAs must also document how Command and Control (C2) Protect Tools will be integrated into the system. Implementation of C2 Protect Tools must be in accordance with Army Policy and agreements made in Phase 1 with the PEO AMMO Information Assurance Manager (IAM) for developmental systems. The PM and/or the CA organizations prepare the Phase 1 SSAA package. The Pre-Deployment Information Assurance Security Officer (IASO) is responsible to the PM and DAA for the preparation of package and for management of the process for their system. The pre-deployment IASO is responsible for continual coordination with the User Representative, CA, and DAA throughout the DITSCAP Process. It is then updated in each phase as the system development progresses and new information becomes available. During DITSCAP Phase 2 (Verification), the SSAA and applicable appendices should be updated as changes dictate, such as documenting solutions coming out of system Accreditation Working Groups (AWGs) or updates of test procedures. The changed documents will not be required to be submitted to the PEO until Phase 3 (Validation) unless the changes are quite significant.

For Phase 3, the complete accreditation package, to include the SSAA, Appendices A through R, and a staff summary sheet is required. For both Phase 1 and Phase 3 submittals, a review period of 45 working days is required. Careful planning will be required to minimize delays in fielding.

For both Phase 1 and Phase 3, it is expected that the complete SSAA submission for review will include one hard copy and one soft copy. Whenever the review of an SSAA results in the PEO providing comments to the PM and Information Assurance Security Officer (IASO), it is expected that the follow-on submission of the updated SSAA to the PEO will include answers/responses to all comments in a separate document. The answers can be integrated into the same soft copy document that the PEO

provided as comments. This will be done in order to greatly decrease the amount of re-review time and will result in a shorter overall time for systems to receive the desired accreditations.

Phase 4 (Post Accreditation) involves monitoring the system management and operation to ensure that an acceptable level of residual risk is preserved. The activities that are conducted to accomplish this include security management, change management, and periodic compliance validation reviews.

All the information relevant to the C&A of a system is collected into the one document, the SSAA. The SSAA is a formal agreement among the DAA, CA, PM, and System User Representative. It is used throughout the entire DITSCAP process to guide actions, document decisions, specify Information Assurance (IA) requirements, document certification tailoring and level of effort, identify possible solutions, and maintain operational systems security. The use of Common Criteria profiles is required.

The main body of the SSAA should describe the AIS from a system-security perspective so items affecting the accreditation boundary and certification level can be evaluated. Generally, few changes are expected between the Phase 1 and Phase 3 SSAA main bodies. It is important that the accreditation boundary be accurately defined. The boundary must encompass everything that is being accredited and this will include all components that are under the control of the DAA of the system that is being accredited. A formal definition of the term accreditation boundary can be found in the DITSCAP documents DoD 5200.40 and DoD 8510.1-M. AR 380-19 also defines accreditation boundary, but somewhat differently than DITSCAP. Therefore, the SSAA must state in paragraph 3.4 which definition is being used.

Appendices A through F should identify only those items that apply to the AIS being accredited. These items generally will not change from Phase 1 to Phase 3. Appendix F is to be a thorough list of all security requirements that apply to the AIS to be accredited. A complete and accurate Appendix F during Phase 1 will minimize the cost and schedule impact of PEO directed changes to security requirements. A tool for developing Appendix F is available on the PEO AMMO Information Assurance section of the Army Knowledge Online (AKO). This tool is a Microsoft Excel spreadsheet. All PMs and IASOs are strongly urged to make use of the tool, as it will be utilized during PEO review of all SSAAs. This tool is named "Security Requirements Traceability Matrix (SRTM) Verification Tool." It identifies generic security requirements that generally apply to PEO AMMO systems. It should be tailored to show as Not Applicable (N/A) all requirements that do not pertain to the given system, and to include system-specific requirements that are not already addressed by it. This will ensure a complete and accurate Appendix F to the SSAA, and therefore will provide good basis for Appendices G and H, which must be traceable back to Appendix F.

PEO AMMO requires User Security Manual / Standing Operating Procedures (USM/SOP) to be submitted with every Phase 3 accreditation package. The USM/SOP is to provide specific guidance for securely operating the AIS. It provides physical and administrative measures that mitigate security risks, thereby improving the security posture of the AIS without incurring undue cost or operational impacts. Additionally, if the users of the system have an option to conduct training at an unclassified level, the SOP must cover the step by step procedures for securely setting up and configuring the system for operation at an unclassified level and then returning it to the normal classified mode of operations. The USM/SOP generally satisfies the requirements for Appendix M of the SSAA.

Appendix N is required only when the AIS to be accredited will be connected to systems operating under an authority other than the PEO AMMO. This appendix must contain any existing System Interconnect Agreements, where the system will connect to other networks or other systems. Paragraph 2-22 of AR 380-19 describes circumstances when Memorandums Of Understanding (MOUs) /Memorandums Of Agreement (MOAs) are required. Sample MOAs are provided in the policy of some networks/systems (see AR 380-19). The content and formats for the memorandums in Appendix N and the staff summary sheet can be found on the PEO AMMO IA area of the AKO. The content and formats are critical and should be carefully followed. The PEO AMMO IA area of the AKO should be checked for updates of the memorandums just before they are finalized.

There is an extensive amount of accreditation information on the PEO AMMO IA area of the AKO that includes most of the references cited in this document, identification of DITSCAP tasks for each phase of the DITSCAP process, various checklists, etc. It is strongly recommended that the following be read and understood before beginning the accreditation process: DoD Instruction 5200.40 Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP), December 30, 1997, DoD 8510.1-M Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual, July 31, 2000, Common Criteria for Information Technology Security Evaluation August 1999 Version 2.1 CCIMB-99-031;032;033 ISO/IEC 15408:1999, Controlled Access Protection Profile Version 1.d 8 October 1999, Labeled Security Protection Profile Version 1.b, 8 October 1999, AR 380-19 Information Systems Security 27 February 1998, AR 25-XX Information Systems Security (will supercede AR 380-19 when signed), and AR 380-5 Department of the Army Information Security Program, 29 September 2000.

2.2 SECURITY PROFILES

As of 31 December 2001, DoD 5200.28-STD, Trusted Computer Security Evaluation Criteria, is obsolete. The PEO AMMO will not accept evaluations based on it. The DoD 5200.28-STD has been replaced by the Common Criteria for Information Technology Security Evaluation. The Common Criteria requires a protection profile for each AIS to be accredited. PMs/PdMs can develop a protection profile tailored to the security requirements of their AIS or choose from a number of protection profiles that have been developed, evaluated, and approved. If the PM develops their own protection profiles, they must go through the National Information Assurance Partnership process to have them validated. Protection profiles are available on the PEO AMMO IA area of the AKO and at http://www.iatf.net/protection_profiles/profiles.cfm. The Information Systems Security Organization of the National Security Agency has developed the Controlled Access Protection Profile (CAPP) which is generally suitable for AIS running in the system high security mode of operation and the Labeled Security Protection Profile (LSPP) which adds trusted labeling to the CAPP. The use of the appropriate protection profile will be in accordance with the agreement in Phase 1 by the DAA, CA, PM, and System User Representative.

2.3 ACCREDITATION MILESTONES

The PEO will require a minimum of 45 working days to review the Phase 1 SSAA package and the Phase 3 SSAA package. The Phase 3 (Type Accreditation or IATO) package necessarily includes the results of the security test and evaluation (certification) performed to determine the effectiveness of the AIS's automated security mechanisms and an assessment of the residual risk after all mitigating factors have been considered. The security test and evaluation performed on the system must be consistent with the security requirements that have been identified and agreed to as documented by the Phase 1 SSAA. The security tests must be conducted on the AIS as it will be fielded; i.e., the final hardware and software configurations.

Phase 2 activities can be begun after Phase 1 is complete. During Phase 2, the SSAA is refined and the initial certification analysis is performed. Phase 2 activities are internal to the developing PM. Changes to the SSAA during Phase 2 serve as a draft of the Phase 3 package. The Phase 2 package is not submitted to the DAA unless significant changes from the Phase 1 package have been made. Changes to test procedures or development of test procedures are not significant for the purposes of submitting a Phase 2 package.

2.4 INTERIM APPROVAL TO OPERATE (IATO) PACKAGES

An Interim Approval To Operate (IATO) may be granted when an AIS does not meet security requirements but the mission is so critical that the risk must be accepted for a limited time. An IATO is often granted when the urgency of approval does not permit the development of a full SSAA package. See Appendix D of this document for a flowchart of the IATO Process.

A DAA may grant an IATO provided that, as a minimum, the following exist and accompany the request for the IATO: a Phase 1 SSAA, a USM/SOP, the results of security (certification) testing, an assessment of residual risk, a recommendation from the certifier, and a staff summary sheet. A complete Phase 3 package is preferred for IATOs, however, allowances for unforeseen circumstances may be made as needed. The certification and risk assessment efforts leading to an IATO need to address the basic residual risk assessment requirements identified in Section 2.10. C2 Protect Tools and Information Assurance Vulnerability Assessments (IAVAs) must be integrated in accordance with guidance provided by the PEO AMMO IAM for Developmental Systems.

2.5 TYPE ACCREDITATION PACKAGES

PMs must ensure that systems are accredited prior to fielding. Consistent with applicable Army regulations, when the risk level as described in the accreditation package is within the bounds of acceptable risk, the PEO AMMO may approve operation, and therefore grant a type accreditation, of an AIS for up to three years.

The type accreditation effort must include a complete Phase 3 SSAA, including all appendices and a Staff Summary Sheet. The SSAA must address all IATO requirements and the following additional material: full verification and testing of SSAA Appendix F Security Requirements, documentation of the results, and assessment of the residual risk for failed Appendix F security requirements and any other detected security vulnerabilities.

2.6 COMMAND AND CONTROL (C2) PROTECT TOOLS

All PEO AMMO systems will incorporate C2 Protect Tools in accordance with Army and PEO AMMO policy. The Army has established a list of available tools that may be found on the ACERT website. This list will be updated, as more tools become available. IASOs shall obtain the agreement of the PEO AMMO IAM for Developmental Systems, as the Designated Approving Authority (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. C2 Protect Tools and Antivirus Software will be configured and maintained in accordance with Army and PEO AMMO policy. Other Information Assurance (IA) Tools that will be incorporated into the systems shall comply with Army policy and be approved by the system's DAA representative before the tools are integrated into the system's baseline. The approach taken to implement C2 Protect Tools, the configuration of C2 Protect Tools, the coordination made with the developer of the C2 Protect Tools, and all associated agreements shall be documented in the system's Phase 1 SSAA. The Test and Evaluation Report must provide evidence that this requirement has been met and the Security Concept of Operations (CONOPS) portion of the SSAA must address how the implementation of C2 Protect Tools has met the guidance outlined by the PEO AMMO IAM for Developmental Systems.

2.7 CONTROLLED CRYPTOGRAPHIC ITEM (CCI)

All Communications Security (COMSEC) products used in AIS to protect Secret and Top Secret must be National Security Agency (NSA) approved. Controlled Cryptographic Items (CCIs) will be protected in accordance with NSA Department of Defense (DoD) and Army directives.

2.8 MAINTAINING ACCREDITATION

When software and hardware upgrades are necessary and to be fielded for systems that have already received type accreditation, the CA must assess the upgrade against the following criteria for a Certification Memorandum:

- The upgrade continues to satisfy the security requirements in the SSAA

- The upgrade does not adversely affect the security posture of the system
- The upgrade does not meet requirements for reaccreditation as documented in the SSAA. If a system requires reaccreditation refer to Section 2.12.

When the upgrade satisfies these criteria, the CA can document this information and complete a Certification Memorandum to include this upgrade in the current type accreditation. The Certification Memorandum is reviewed and approved by the Certification Authority. This assessment documentation will be provided as the following enclosures to the Certification Memorandum:

- An attachment to Appendix Q that addresses the changes to the residual risk assessment, Information Assurance Vulnerability Assessment (IAVA) alert compliance, and impact of changes.
- An attachment to Appendix M for any changes to the USM/SOP (if required).

See Appendix D for the flowchart, "Reaccreditation Assessment (Addendum Process)," that defines when a certification memorandum is required.

2.9 TESTING

This section addresses testing and priority definitions for problem reports and enhancements to be applied on PEO AMMO systems, consistent with guidance in DA PAM 73-7 and other applicable Army and DoD testing and IA regulations. The objective of testing is to deliver an error free system to the users. Despite the extensive testing efforts made, some system errors will undoubtedly occur. These errors must be properly addressed and categorized so they may be investigated and corrected. This SAMP requires PMs/PdMs and the pre-deployment IASOs to apply the security priority definitions for security-related problem reports and enhancements. All security-relevant problem reports and enhancements are either priority one or two unless the pre-deployment IASO, with concurrence of the PEO AMMO IAM for Developmental Systems, specifically approves a documented residual risk assessment that supports the other priorities. These required residual risk assessments are incremental reviews intended to provide management with the necessary information for developing and maintaining systems capable of being accredited, within budget, resource, and schedule constraints. No problem report or enhancement is required for Information Assurance Vulnerability Assessment (IAVA) alerts that clearly do not apply to the system. However, a problem report is required when a system is in non-compliance for a specific applicable IAVA alert. All problem reports and enhancements associated with an IAVA alert are priority one or two unless the DAA specifically authorizes a different priority for the AIS. If an IAVA alert is not applicable, this must be identified in the IAVA portion of the Residual Risk Assessment Report (RRAR) of the SSAA (Appendix Q) along with the impact of non-compliance to IAVA alerts that are applicable.

The security-related priority definitions and non-security context are as follows:

- **PRIORITY 1:** A software problem or enhancement for an omitted capability that:
 - a. Prevents the accomplishment of an operational or mission essential capability specified by baselined requirements.
 - b. Prevents the operator's accomplishment of an operational or mission essential capability. Causes a loss of user confidence in operational capability of the AIS due to lost, erroneous, inconsistent, or incomplete data.
 - c. Jeopardizes personnel safety.

- d. Is a significant security finding that must be fixed immediately. It must be fixed and validated during appropriate regression testing before the AIS can become operational at any site or be granted either interim approval to operate or a type accreditation. Only the pre-deployment IASO can close it.
- **PRIORITY 2:** A software problem or enhancement for an omitted capability that:
 - a. Adversely affects the accomplishment of an operational or mission essential capability specified by baselined requirements so as to degrade performance and for which no alternative work-around solution is known.
 - b. Adversely affects the operator's accomplishment of an operational or mission essential capability specified by baselined requirements so as to degrade performance and for which no alternative work-around solution is known.
 - c. Is a security relevant finding that must be fixed within the time frame the DAA specifically authorizes as documented in the staff summary sheet. It must be fixed and validated during appropriate regression testing by the completion date. Only the pre-deployment IASO can close it. A type accreditation will not be granted until it is closed. An IATO may be granted, but is contingent on it being closed or DAA authorization of a later completion date being received. All problem reports and enhancements associated with IAVA alerts are priority one or two unless the DAA specifically authorizes a different priority for the AIS.
 - **PRIORITY 3:** A software problem or enhancement for an omitted capability that:
 - a. Adversely affects the accomplishment of an operational or mission essential capability specified by baselined requirements so as to degrade performance and for which an alternative work-around solution is known.
 - b. Adversely affects the operator's accomplishment of an operational or mission essential capability specified by baselined requirements so as to degrade performance and for which an alternative work-around solution is known.
 - c. Will not prevent AIS security accreditation but will be an issue to be corrected or implemented as soon as resources and schedule permit. It is not associated with an IAVA alert unless specifically authorized by the DAA. The work around solution that provides the countermeasure mitigating the risk must be fully documented in the RRAR and USM/SOP.
 - **PRIORITY 4:** A software problem or enhancement for an omitted capability that:
 - a. Is an operator inconvenience or annoyance but does not affect a required operational or mission essential capability.
 - b. Does not affect AIS security accreditation but should be corrected or implemented during a normal maintenance upgrade. It is not associated with an IAVA alert unless specifically authorized by the DAA. These types of problems will be noted in the RRAR and USM/SOP
 - **PRIORITY 5:** All other software problems or enhancements for an omitted capability.

2.10 RESIDUAL RISK ASSESSMENT RESULTS (RRAR)

The residual risk assessment will address the threats against the AIS and the associated risks for the full life cycle of the AIS, to include: development and production, fielding (delivery), operation (garrison, exercises, physical combat, deployed), and Post Production Software Support (PPSS) and maintenance.

The residual risk associated with any AIS that will be used in both peace and war times must be addressed in both garrison and deployed modes. The RARR must also address any certification test failures. The Chief Information Officer (CIO)/G-6 (formerly known as the Director of Information Systems for Command, Control, Communications, and Computers (DISC4)) and PEO AMMO provide guidance for preparing risk assessments. This guidance is available on the PEO AMMO IA area of the AKO. Appendix C of this document provides a RRAR template.

For all PEO AMMO systems, the following residual risk assessment format is required for addressing each area of risk and certification test failures:

- Header (title of the issue)
- Statement of issue (the problem)
- Impact on the system (vulnerability before any countermeasures are applied to the generic or specific vulnerability, as applicable)
- Countermeasure (must be valid and operationally feasible if the procedure is performed manually, identify)
- Residual risk (low, medium, or high).

The certification effort to obtain a type accreditation involves an additional certification effort beyond the basic requirements for all PEO AMMO approvals to operate. The additional effort involves verifying that Appendix F security requirements have been addressed in the system's design and development, documenting the verification results, and assessing the residual risk for failed Appendix F security requirements as well as any other detected security vulnerabilities. The basic residual risk assessment requirements for all PEO AMMO approvals to operate include the following analyses as well as an evaluation of open security-related problem reports and enhancements for all operating systems resident on AIS components:

- Results from an approved Army vulnerability scanner run against the AIS
- Implementation status as of a specific date for all applicable vendor security-relevant patches and product upgrades for all commercial products that are incorporated in the AIS, addressing the vulnerabilities for all applicable vendor security-relevant patches and product upgrades as of the specific date that are not implemented in the AIS, associating each risk assessment with the unimplemented patches or unimplemented product upgrades
- Network ports and services in use
- Audit events
- C2 Protect Tools being used
- Known vulnerabilities associated with all commercial products incorporated in the AIS for which there are no available vendor patches and product upgrades
- Known vulnerabilities associated with GOTS
- The system shall comply with all IAVA alerts released within 7 working days of the SSAA submission to PEO AMMO for ALL reviews, identifying all non-applicable alerts, including problem reports and risk assessments where a system is not in compliance with a specific applicable alert. This compliance includes all alerts dated from January 2000 to the 7 working days.
- All open security-related problem report and enhancement items for the specific AIS via a table containing the problem report or enhancement identifier used for tracking, the assigned priority, origination dates, applicable references to specific paragraphs in Appendix Q for selected table items, references for all priority one and two items, and the scheduled completion date for all priority one and two items.

- Discretionary review of the separate supporting documentation established, incrementally approved, and maintained by the pre-deployment IASO that supports tracking and managing of all open security-related problems and enhancements of each AIS that the pre-deployment IASO oversees.

Additional information on Risk can be found in section 5 Risk Management.

2.11 SECURITY CLASSIFICATION GUIDE (SCG) AND CLASSIFICATION OF DOCUMENTS

All PEO AMMO systems are required to have a Security Classification Guide (SCG) that is consistent with the requirements outlined in AR 380-5, Department of the Army Information Security Program. The SCG is the authority for classifying accreditation-related documentation.

Details of any system capability or security deficiency that would aid an adversary in exploiting or disabling the AIS is classified SECRET under the authority of the Army's Digitization Security Classification Guide (DSCG). Where an AIS has an associated SCG, that system SCG takes precedence over the DSCG as long as the system SCG is more restrictive. The system SCG will not lower the classification levels set by the DSCG. For example, vulnerabilities will be classified SECRET by the DSCG. IASOs will carefully review Appendix P Security Test and Evaluation Results, Appendix Q, Residual Risk Assessment, and the staff summary sheet to ensure that they have been properly classified and utilize the proper wording as per templates provided on the PEO AMMO IA area of the AKO.

2.12 REACCREDITATION

The requirements for reaccreditation are delineated in AR 380-19 and AR 25-XX (when published). In accordance with the DITSCAP, the reaccreditation requirements must be identified in the SSAA.

AR 380-19 requires a reaccreditation after three years following the effective date of the existing accreditation. During the three-year period, if changes are made to the system that do not impact system security, then only a certification memorandum is required (see Section 2.8) and the system can continue to operate under the existing accreditation. If the changes do impact system security, then a reaccreditation must be performed. The reaccreditation must include consideration of current IAVAs and C2 Protect Tools, recertification (Appendix P) and reassessment of risk (Appendix Q). Any risk mitigations that require procedural changes must be addressed in the USM/SOP. See Appendix D for a flowchart, "Reaccreditation Assessment (Addendum Process)," that defines when a certification memorandum is required.

2.13 INFORMATION ASSURANCE VULNERABILITY ALERT (IAVA) COMPLIANCE

IAVA compliance must be addressed as part of Appendix P, Test and Evaluation Reports, and/or Appendix Q, Residual Risk Assessment Results. A template outlining the content required for an analysis and discussion of IAVA compliance for a system is posed on the PEO AMMO IA area of the AKO.

2.14 PROPRIETARY INFORMATION

Proprietary information must be properly marked and properly handled to include the use of Non-Disclosure Agreements where necessary.

2.15 COMPETITION SENSITIVE INFORMATION

Competition Sensitive information must be properly marked and properly handled to include the use of Non-Disclosure Agreements and Non-Conflict Agreements where necessary.

2.16 SENSITIVE INFORMATION

Unclassified Sensitive Information is the term to be applied to information that is sensitive in its nature and unclassified. This is the preferred term for the commonly and inappropriately used term Sensitive But Unclassified (SBU) within the Department of Defense.

2.17 INCIDENT REPORTS

Incident reports shall be reported to the IASO and the office of PEO AMMO as appropriate. All incident reports shall be categorized in accordance with the ratings included in the following categories.

- Category 1 – Root Level compromise
- Category 2 – User Level Compromise
- Category 3 – Attempted Access
- Category 4 – Denial of service
- Category 5 – Poor Security Practice
- Category 6 – Probe or Scan
- Category 7 – Malicious Code
- Category 8 – Not yet classified

SECTION 3 ORGANIZATION AND RESPONSIBILITIES

3.1 DESIGNATED APPROVING AUTHORITY (DAA)

The DAA will establish an Information Assurance (IA) Integrated Process Team (IPT) working group and appoint a representative. Each PEO AMMO Project and Product Manager will appoint representatives to attend and participate in the IA IPT meetings. The PEO AMMO representative will act as a point of contact for resolution of issues requiring a DAA decision.

The DAA for PEO AMMO systems processing information up to and including the Secret sensitivity level is PEO AMMO. The responsibilities of the DAA for security accreditation include:

- Ensuring the requirements of AR 380-19 or AR 25-XX (when published) and other applicable procedures dealing with IA are followed
- Reviewing and approving the system security safeguards and signing the accreditation statement, including an interim approval to operate
- Ensuring the safeguards approved are implemented and maintained
- Establishing a program of review for reaccrediting the system when significant changes to system hardware or software occur, when a breach of existing security mechanism or violation of system integrity is found, or when three years have elapsed since the effective date of the existing accreditation
- Ensuring systems they accredit do not process data with a sensitivity level beyond the scope of the accreditation
- Establishing a security education and awareness program in accordance with AR 380-19 and/or AR 25-XX (when published)
- Appointing an IAM for developmental systems to establish and manage the PEO AMMO security program in accordance with the PEO AMMO Security Policy. The IAM for developmental systems will chair the IA IPT.
- Ensuring PMs/PdMs assign a pre-deployment IASO for each system
- Incorporating security into the PEO AMMO systems architecture and implementing specifications and plans.

3.2 CERTIFICATION AUTHORITY (CA) AND CERTIFICATION AGENT

The Certification Agent is responsible for performing the comprehensive evaluation of the security features of an IT system and any associated safeguards to determine the extent to which a given system meets a set of specified security requirements.

The Certification Agent supports the Certification Authority (CA) in developing a C&A strategy to get the given system accredited. The responsibilities of the CA for security accreditation include:

- Following the requirements of AR 380-19 or AR 25-XX (when published) and other applicable procedures dealing with IA when proceeding through the C&A process and tailor DITSCAP where necessary
- Performing vulnerability and risk assessments
- Determining level of certification effort

- Preparing the draft SSAA
- Conducting certification activities, assessing vulnerabilities, and reporting results to the PM, DAA, and User representative
- Determining whether the system is ready for certification and update SSAA
- Evaluating security requirements compliance and determining residual risk
- Recommending risk mitigation measures and accreditation type, and generating final SSAA.
- Reviewing the certification evidence, test results, and analysis results supporting an IATO, certifying that short term operations of the system is within the bounds of acceptable risk, and therefore recommending that the system be issued an IATO
- Reviewing the certification evidence, test results, and analysis results supporting a type accreditation, certifying that the system and its operation comply with the SSAA security requirements, and therefore recommending that the system be generically accredited
- Reviewing the certification evidence, test results, and analysis results for software and hardware upgrades of generically accredited systems, determining whether the upgrade satisfies the criteria for a Certification Memorandum to include the upgrade in the current type accreditation, and when appropriate, signing the memorandum and providing the assessment documentation as enclosures

3.3 COORDINATION WITH MAJOR ARMY COMMANDS (MACOMS)

After the DAA approves and signs the accreditation document, the Pre-Deployment IASO will forward it to the Information Assurance Program Manager (IAPM) of each Major Army Command (MACOM) and major activity receiving the system. The MACOM IAPM, together with the command information manager and the command functional user representative either accepts the type accreditation as is or, based on their operating environment, prescribes additional measures or procedures to operate the system in their MACOM. Such additional measures are appended to the SSAA and constitute the system accreditation in that MACOM. Pre-deployment IASOs are required to closely and continually coordinate with MACOMS and major activities using this system

3.4 INFORMATION ASSURANCE MANAGER (IAM) FOR DEVELOPMENTAL SYSTEMS

PEO AMMO appoints an IAM to establish and manage the PEO AMMO security program for developmental systems in accordance with the PEO AMMO Security Policy. The IAM for developmental systems chairs the IA IPT.

PEO AMMO systems must meet applicable government security requirements from design through implementation and test phases. PEO AMMO will enforce the security policies and procedures, and may employ the following concepts, methods, or techniques to ensure the integrity of security:

- Reviewing and validating all hardware and software security requirements for compliance
- Reviewing and validating all PEO AMMO systems security related documents originated by the system's PM/PdM, CA, or the developing contractor(s)
- Reviewing all PEO AMMO systems test plans and procedures
- Reviewing all plans for addressing security issues to include all "get well" plans documented in the staff summary sheets submitted with packages for DAA approval.
- Reviewing documentation established and maintained by the pre-deployment IASO that supports tracking and managing all open security-related problem reports and enhancements of each AIS that the pre-deployment IASO oversees

- Verifying that all problem reports and enhancements associated with an IAVA alert are priority one or two unless the IASO, with concurrence of the PEO AMMO IAM for Developmental Systems, specifically authorized a different priority for the problem report
- Attending security-related Preliminary Design Reviews (PDRs), Critical Design Reviews (CDRs), Failure Review Boards (FRBs), Test Readiness Reviews (TRRs), working group meetings, and AWGs as necessary to ensure security-related issues are monitored and evaluated.
- Establishing and managing the IA program for developmental systems
- Developing program-unique guidance
- Establishing a procedure in which the status of all AIS accreditations, their sensitivity levels, and requirements for operation are documented and available
- Chairing the IA IPT
- Other duties as identified in AR 380-19 and/or AR 25-XX (when published).

3.5 PROGRAM/PROJECT MANAGER (PM)

The responsibilities for PMs include but are not limited to:

- Appointing a pre-deployment IASO to establish and implement their respective system's security program.
- Ensuring that the pre-deployment IASOs are trained and certified
- Ensuring continuous pre-deployment IASO and designated IASO support staff participation in all programmatic activities that establish priorities and the detailed implementation schedule for system functionality, problem reports, and enhancements
- Effecting continuous coordination with the system's Training and Doctrine Command (TRADOC) System Manager (TSM) as the designated User Representative
- Effecting continuous coordination with the MACOM IAPM in which the systems being developed are to be demonstrated, tested, and/or fielded
- Ensuring the IATO accreditation documentation is delivered to the MACOM IAPMs prior to the system's Limited User Test (LUT) or Initial Operational Test and Evaluation (IOT&E)
- Ensuring that approved type accreditation documentation is delivered to the MACOM IAPM prior to delivery of the system to the receiving unit
- Ensuring that dry run security testing for the type accreditation occurs prior to the system's Operational Test Readiness Review (OTRR) conducted by government testing organizations, reporting the dry run results as indicative of the system's security posture and suitability for recommending a type accreditation after formal security testing is completed
- Ensuring that formal security testing for the type accreditation is conducted using essentially the same software as the government test community uses for interoperability test events and the IOT&E or LUT leading to the system fielding decision
- Ensuring that type reaccreditation documentation reflecting system changes is provided to the MACOM IAPMs and using activities.

3.6 PRE-DEPLOYMENT INFORMATION ASSURANCE SECURITY OFFICER (IASO)

A pre-deployment IASO is appointed by the system PM to establish the system's security program and oversee all accreditation efforts. The IASO chairs the system AWG and represents the PM at the IA IPT. The responsibilities of the pre-deployment IASO are as follows:

- Establishing an AKO account, registering for access to the Army IA site, https://www.us.army.mil/portal/portal_home.ihtml, and routinely checking for updates to policy
- Establishing a PEO AMMO IA section account on the AKO to routinely check the IA area for updates, updating their C&A schedules and using the products provided to ensure their accreditations meet the standard
- Registering to receive Army Computer Emergency Response Team (ACERT) alerts from, or periodically visiting the web site <https://www.acert.belvoir.army.mil/ACERTmain.html> in order to acquire the IAVA Alerts
- Addressing the IAVA Alerts
- Ensuring the training and certification requirements mandated by Department of the Army and PEO AMMO policy are met in accordance with the Army policies found at the PEO AMMO IA area of the AKO and Information Assurance Support Environment (IASO) web sites. This includes proactively completing all required IASO training in a timely manner
- Identify the need for an AWG to address security issues or to support security events, and chair the AWG, to include requesting that PMs/PdMs appoint an appropriate panel of subject matter experts to the AWG
- Participating in all programmatic activities that establish priorities and the detailed implementation schedule for system functionality, problem reports, and enhancements
- Establishing and maintaining current documentation that supports tracking and managing all open security-related problem reports and enhancements of each AIS that the pre-deployment IASO oversees, ensuring that the prioritization is consistently based on the security-relevant priority definitions in this SAMP
- Approving and documenting in the system residual risk assessments all security-relevant problems prioritized other than one or two, ensuring that the documentation for each specific system is available for easy review by the system's CA and/or PEO AMMO within 7 working days of request, and ensuring that this documentation contains sufficient information for reviewers to fully evaluate the prioritization of all security-relevant items without requesting additional detailed information from the Project/Product Manager and/or implementing organization.
- Closing security-related priority one and two software problems or enhancements after evaluating the problem resolution and assessing the regression testing performed to validate that resolution before submitting for PEO approval and signature
- Ensuring that the system meets requirements and that all risks have been mitigated to an acceptable level
- Ensuring that the system's concept of operations addresses user needs and the USM/SOP provides viable security solutions
- Ensuring that the SSAA package meets the content and presentation of evidence requirements outlined in PEO, Army, and DoD policy
- Ensuring that documentation is delivered to PEO AMMO in a timely manner permitting a 45-day review cycle
- Ensuring that regular AWGs are conducted so that issues and risks to their systems are continually resolved throughout the systems' life cycles.
- Proactively coordinating with all MACOMs and major activities that will receive the system so that pre-deployment IAMs and IASOs have the information and support needed to carry out their responsibilities when the system is transitioned to them.
- Ensuring that users comply with the USM/SOP supplied with the system.

3.9 PEO AMMO SECURITY FORUMS

3.9.1 INFORMATION ASSURANCE (IA) INTEGRATED PRODUCT TEAM (IPT)

The IA IPT focuses on security C&A-related issues. A PEO AMMO representative chairs the IA IPT. The IA IPT reviews and resolves PEO AMMO-wide security issues. The IA IPT approves the PEO AMMO security architecture, reviews reports of accreditation, and notes such progress. When necessary, the IA IPT provides consolidated recommendations to the PEO. The IA IPT meets quarterly or on an as-needed basis.

3.9.2 ACCREDITATION WORKING GROUPS (AWG)

PMs will establish an AWG for the system undergoing accreditation as requested by the pre-deployment IASO to address a security issue or to support a security event. The purpose of the AWG is to provide assistance to the PM in resolving security and accreditation issues that are likely to develop during the type accreditation process. The AWG will serve as a panel of subject matter experts in security disciplines, user requirements, system operations, and the system development and fielding process, and will include in membership, as a minimum: representatives for the DAA, CA, System PM, and System User.

The AWG will be chaired by the pre-deployment IASO, who will report directly to the PM. The AWG will meet on an as-needed basis to review the progress in the accreditation process and address system issues. Issues involving other systems under PEO AMMO will be brought to the attention of the IA IPT by the PM.

SECTION 4 CERTIFICATION AND ACCREDITATION

4.1 CERTIFICATION TESTER INDEPENDENCE

Pre-deployment IASOs must ensure that an independent organization or team performs the certification functions. This is a long-standing requirement. AR 380-19, Paragraph 2-7.d that states "Upon completion of maintenance or modification of software, independent testing and verification will be required before returning software to operation", makes this requirement for independent testing clear. Paragraph 3-4.e, states "Where practical, individuals who complete the certification should be independent from the developer's staff." If the IASO cannot demonstrate a thorough knowledge of Information Assurance, the IASO shall select a Government representative knowledgeable in IA for assistance.

DoD policy states that the DAA will appoint a Certification Authority (CA) who will plan, conduct and approve the certification test. PEO AMMO has appointed the Communications & Electronics Research Development and Engineering Center, Space and Terrestrial Communications Directorate (CERDEC, S&TCD) Information Assurance Product Director (IA PD) as the CA. Furthermore, CERDEC, S&TCD IAPD shall provide the certification agent (the technical person or persons who actually perform the certification testing and analysis) for all PEO AMMO programs. This will assure independence as well as competence for the team members performing the certification as required by the DITSCAP and PEO AMMO policy.

The DITSCAP and PEO AMMO policy explicitly requires independence as well as competence for the team members performing the certification. Competence is defined as having the required training and experience to perform certification and accreditation work.

In accordance with paragraph C3.4.7.2.2 of the DITSCAP Application Manual: "If a contractor is involved or individuals from other Government organizations are temporarily detailed to assist in the C&A process, funding requirements must be defined and included in the SSAA. The composition and size of the team will depend on the size and complexity of the system. The team must have members with composite expertise in the whole span of activities requirement and who are independent of the system developer or project manager."

IAW paragraph C8.5 of the DITSCAP Application Manual: "The Certifier should be independent from the organization responsible for the system development or operation. Organizational independence of the Certifier ensures the most objective information for the DAA to make accreditation decisions."

In summary the certification agent must be both competent and independent from the developer's staff.

4.2 SECURITY WAIVER PROCEDURE

4.2.1 SECURITY WAIVER NEED

If a PEO AMMO system will be unable to meet the security requirements specified in the SSAA, the respective PM is required to submit a Request for Deviation/Waiver. An approved Request for Deviation is a temporary authorization to operate when the mandatory configuration baseline requirements are not met, whereas an approved Request for Waiver is a permanent authorization to operate when the requirements are not met. Waivers for security requirements affect the system's ability to achieve the accreditation milestones, and therefore require DAA approval prior to submission of the SSAA for signature. A security waiver should be identified and obtained as soon as possible in the system life cycle to ensure that the associated risks are acceptable, and necessary countermeasures are identified

and incorporated in the system design. Two additional security milestones should be added by the PM to the Program Master Schedule (PMS) for each expected waiver, they areas follows:

- Submission of security waiver
- Approval of security waiver.

4.2.2 SECURITY WAIVER REQUEST

The request for a security waiver from the DAA will be handled via the submission of a memorandum request for deviation/waiver from the PM to the IA IPT for review if the requirement is at the PEO AMMO level. If the requirement is a DA or DoD requirement, DA or DoD procedures will be followed. The request for deviation/waiver must be accompanied by a risk assessment, the DAA memorandum in draft, and staff summary sheet. The IAM is responsible for coordinating the review responses and recommending approval/disapproval of the Request for Deviation/Waiver. Concurrent with the recommendation to approve/disapprove the waiver, the PEO support staff will recommend DAA signature and approval/disapproval of the security waiver or request for waiver to DA. The security waiver will be forwarded to the appropriate DAA for concurrence. If the DAA does not concur, the Request for Deviation/Waiver and the Security Waiver will be returned to the PM for resolution. Upon DAA approval, the security waiver will be forwarded to the PM and included in the SSAA that has yet to receive DAA approval.

With regard to content, a request for security waiver must include a plan to achieve the requirement and security accreditation milestone. It must indicate the expected version of the system that will comply with the requirements. If the waiver is a recurring waiver, the request must reflect why the previous activities planned to meet the requirement were not accomplished. The waiver must meet all PEO AMMO, HQDA, and DoD content and presentation of evidence requirements.

4.3 STAFFING PROCESS

4.3.1 STAFF SUMMARY SHEET

Every accreditation package submitted for PEO approval must be accompanied a staff summary sheet that is approved and signed by the PM. The content and format of the staff summary sheet must comply with the template posted on the PEO AMMO IA area of the AKO.

4.3.2 RISK STATEMENTS ON THE SUMMARY SHEET

All risks identified for the system must be summarized along with an identification of the overall level of risk as being Low, Low to Medium, Medium, Medium to High, or High. All countermeasures must be clearly documented, implemented, and realistic, that is procedural or technical countermeasures shall not place an undue burden on unit personnel or degrade performance of the system in a manner that significantly affects mission accomplishment.

SECTION 5 RISK MANAGEMENT

5.1 RISK MANAGEMENT PROGRAM NEED

PMs shall manage and engineer information systems using the best processes and practices known to reduce security risks, including the risks to timely accreditation. PMs are required to conduct a system risk assessment based on system criticality, threat, and vulnerabilities, and to incorporate appropriate countermeasures. In order to meet this mandate, PMs must manage the risks to their systems throughout those systems' lifecycles. The Deputy Secretary's memorandum, *Defense Acquisition*, dated October 30, 2002, and Attachment 2 to that memorandum, Interim Acquisition Guidebook, clearly require PMs to address Information Assurance and risk management for their systems using "best procedures."

5.2 RISK ASSESSMENT PROCESS

The risk assessment process involves the analysis of the threats, threat agents, associated risks, impacts, countermeasures or safeguards, and residual risk. It must evaluate the potential impact that the loss or compromise of information, denial or degradation of service, unauthorized manipulation of information, unauthorized use, loss of mission critical functionality, and lack of integrity within the system or network will have on national security. In accordance with Memorandum, HQDA, SAIS-IAS, 1 March 2000, subject: Guidelines for preparing Risk Assessments as Part of System Security Accreditations, the risk assessment process must address the adequacy of the physical, administrative, procedural, and automated security mechanisms that are relied on to ensure secure system operation.

5.3 MINIMUM REQUIREMENTS FOR A RISK ASSESSMENT

The RRAR that shall be part of every IATO and Type Accreditation package will document the system's risk assessment and risk management program. The RRAR shall address the system's generic threats and shortfalls uncovered during certification testing, such as instances where a system fails to meet the security requirements agreed to and documented in the system's Security Requirements Traceability Matrix (SRTM) and risks associated with IAVA compliance. The risk assessments must provide valid countermeasures and clearly identify residual risks after the countermeasures have been applied.

5.4 RISK MANAGEMENT THROUGH THE LIFECYCLE PHASES

Recognizing that threats to a system can change as the environment changes, the RRAR will address the risks for each system lifecycle phase to include development and production, fielding/delivery, operation to include garrison, exercise, combat and other deployments, and Post Production Software Support (PPSS). In order to make the RRAR easily understood by the target audience and to significantly reduce the level of effort required to develop and review the RRAR, all PEO AMMO risk assessments shall address each risk area as follows: develop a header (title of the issue) such as "unauthorized user deliberate attack." The risk assessment shall state the issue (problem statement) such as unauthorized manipulation of critical system files, impact on the system such as denial of service, compromise of system integrity and information, that is the impact of the vulnerability before the countermeasure is applied, the countermeasure statement that identifies the specific safeguard(s), and the residual risk stated as either high, medium, or low after the countermeasure is applied. The use of terms such as "medium-high" or "low-medium" shall be minimized to avoid ambiguity.

5.5 DEVELOPING VALID COUNTERMEASURES

Countermeasures must be clearly understood, operationally feasible, and must not place an undue burden on the unit receiving and maintaining the system or users operating the system. Technical safeguards, such as implementation of a patch or disabling of a vulnerable service, must be fully

implemented and procedural countermeasures must be clearly documented in the USM/SOP as required actions that the unit leaders must enforce and the system's users must carry out, in order to be considered valid countermeasures.

Examples of countermeasures include integration and use of C2 Protect Tools using configurations approved by the PEO AMMO IAM to provide defense in depth, elimination of command line access to the operating system, establishing a Physical Control Zone (PCZ) around the system to exclude individuals that pose the greatest risk to the system, and implementation of contingency plans that will put the system quickly back into operation after an attack or natural disaster.

Generic statements that fail to identify specific countermeasures or that fail to convey exactly what must be done or what was fixed to mitigate risk are unacceptable. Broad statements that fail to address specific issues will not be considered valid. For example, statements like "implementing the procedures in the USM/SOP" or "enforcement of the unit's physical security program" are not valid countermeasure statements because they fail to identify the specific procedure that will mitigate a specific risk.

5.6 DEFINING AND ANALYZING THE THREAT

A threat is an event or method that can potentially compromise the integrity, availability, or confidentiality of an information system. The threats to information systems include deliberate or unintentional acts caused by authorized or unauthorized users, natural or man-made disasters, as well as direct physical attacks by individuals or groups. Threats identified in relevant system documents, such as the System Threat Assessment Report (STAR), Operational Requirements Documents (ORDs) and Capstone Requirements Documents (CRDs), and by authoritative agencies must be considered along with the generic threats outlined in Figure 5-1. This figure represents a threat model showing the relationship of threats and threat agents of concern to a PEO AMMO system. Although this threat model is simple and effective, it cannot be considered all-inclusive. It should be used as a starting point in the analysis of the threats to the system.

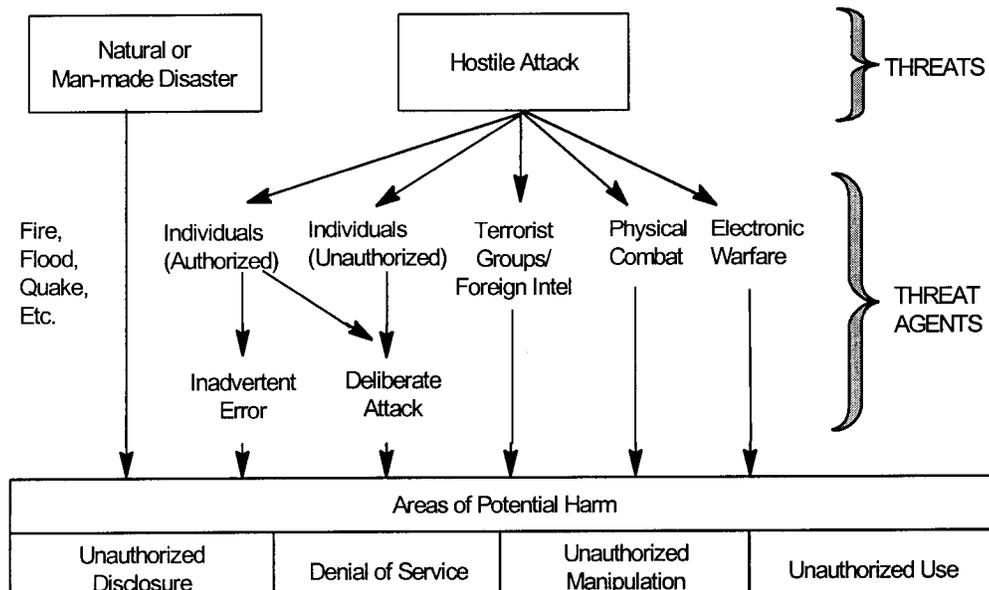


Figure 5-1 PEO AMMO Threat Model

The most difficult threat to protect against will be deliberate hostile acts by authorized individuals. This threat must be mitigated by the application of a secure system security design, sound security procedures such as the separation of duties, and the vigilance on the part of superiors, those charged with maintaining the unit's overall security programs and implementing the USM/SOP that will outline the countermeasures developed as part of the risk management process. Deliberate attack includes a new generation threat, Computer Network Attack (CNA). CNA is one of the significant threats identified in the Global Information Grid (GIG) and ABCS 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 Internet hacking techniques to deny, modify, or disclose information in an unauthorized manner.

Countering this threat requires rigorous risk management to include the application of sound countermeasures and software development best practices, such as implementation of secure configuration policies and Common Operating Environment (COE) specifications, to reduce a system's risk exposure to this major threat. In certain instances, implementation of a certain aspect of a secure configuration policy, integration specification, or a mandated fix may adversely impact mission critical functionality. If a required implementation, fix or configuration is not integrated for this reason, then the resultant vulnerability must be addressed and countermeasures identified in the system's RRAR.

5.7 PRE-DEPLOYMENT IASO INVOLVEMENT

PEO AMMO Pre-deployment IASOs shall be fully involved in the management of their system's risks, to include development of their system's RRARs. IASOs must use collaboration vehicles such as the PEO AMMO IA site on the AKO, the PEO AMMO IA IPT meetings, and system AWGs to raise issues, develop viable solutions, accomplish coordination with stakeholders such as the user representative, CA, and DAA, and then implement solutions that will improve their system's security posture and reduce the risks to their system to include risks to timely accreditation. IASOs shall keep the DAA staff fully informed of all C&A Schedules to minimize the risk of not obtaining a timely accreditation or approval to operate for their system. Appendix C contains a table of contents for a RRAR. Although the outline may be tailored, the content of the RRAR must address all the areas identified in the outline and it must reflect the considerations outlined in the proceeding discussion. The Pre-deployment IASO's responsibilities do not end with accreditation of the system. The Pre-deployment IASO must ensure that MACOM IAPMs and Major Activity IAMs that will use their system obtain a copy of the approved system SSAA to include the RRAR and must effect continual coordination with MACOMs and major activities that will use their system.

5.8 EFFECTIVENESS REVIEWS

The pre-deployment IASO must address issues identified from the field as part of the process of on-going effectiveness review of the system's risk management program. The effectiveness review process determines whether the countermeasures are providing the desired results. This process ensures that the documented security techniques have not created a more serious vulnerability, risk or operational impact. The effectiveness review of applied countermeasures will form the basis for future security actions or risk areas that must be addressed.

SECTION 6 TEMPEST

PEO AMMO Pre-deployment IASOs are required to contact Mr. Donald Bell, 902nd MI, the Army Certified TEMPEST Technical Authority (CTTA), at DSN 622-4440, commercial (301) 677-4440, Nonsecure Internet Protocol Router Network (NIPRNET) e-mail Donald.Bell@meade-inscom.army.mil, Secure Internet Protocol Router Network (SIPRNET) secure mail: Bell2@mail.north-inscom.army.smil.mil, to determine the need for a CTTA review for their system and to have a TEMPEST review performed on their systems as required.

SSAAs will cite NSTISSI 7000 (U), National Security Telecommunications and Information Systems Security Advisory Memorandum (NSTISSAM) TEMPEST/2-95, and AR 381-14 (U) Technical Counterintelligence (TCI) (U), and will document the coordination made with the Army CTTA in their packages. The CTTA will determine what, if any, countermeasure review and tests are required for TEMPEST certification in accordance with AR 381-14. The CTTA's determination will be based on the evaluation of the equipment make and model, level and percentage of classified processing, where the system will be fielded, and the TEMPEST threat, by country, against the system. Include in paragraph 2.1.6 of the SSAA the following wording:

"The [system name] will comply with National Security Telecommunications and Information Systems Security Instruction 7000 (NSTISSI-7000), 29 November 93, National Security Telecommunications and Information Systems Security Advisory Memorandum (NSTISSAM) TEMPEST/2-95, RED/BLACK Installation Guidance, 12 December 95, and Army Regulation 381-14, Technical Counterintelligence (TCI) (U), 30 September 2002, as appropriate."

The PMs will obtain TEMPEST countermeasures recommendations from the CTTA and will provide them to requesting organizations and to all MACOMs that will receive the PM's system. CTTA reviews will be included as an addendum to Appendix P and risks will be addressed in Appendix Q of all SSAAs. Procedural CTTA recommendations shall be clearly described in the system's USM/SOP as procedural requirements.

IATOs for systems deployed only within the confines of CONUS will only need to document that initial coordination with the Army CTTA has been accomplished. In this case paragraph 2.1.6 of the SSAA and the USM/SOP must clearly state the restriction to CONUS during the interim period. Organizations providing support to PEO AMMO PMs will be expected to understand the current TEMPEST requirements for tactical systems and to ensure that TEMPEST has been addressed as part of the system's C&A effort.

On 29 November 1993, a new national policy on TEMPEST was approved and succeeded AR 380-19-1 (U). National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 7000, TEMPEST Countermeasures for Facilities (U), 29 November 1993, is the national TEMPEST policy. The new AR 381-14, Technical Counterintelligence (TCI) (U) addressing TEMPEST for Army systems has been published and is available on the SIPRNet. Paragraph 2.1.6 of all SSAAs must now cite the current requirements NOT wording from AR 380-19-1 (U). For systems that are already approved, the receiving unit must request this review.

Pre-deployment IASOs are required to review the guidance in sections 7, 8, and 9 of NSTISSAM TEMPEST/2-95, RED/BLACK Separation Guidance, dated 12 Dec 95. IASOs should pay particular attention to Section 7, Transportable Systems in a Tactical Environment.

NSTISSAM TEMPEST/2-95 is posted to the PEO AMMO IA area of the AKO. Access to this area is restricted to those who have been granted access to the IA portion of the PEO AMMO AKO.

SECTION 7

INFORMATION ASSURANCE VULNERABILITY MANAGEMENT

The Information Assurance Vulnerability Management (IAVM) program supersedes the IAVA Program. IAVM compliance is the absolute minimum standard for all information systems, not the preferred end state that 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; and (4) compliance verification. The ACERT/ANOSC will issue Army IAVM messages. There are three types of DoD IAVM messages: Alerts (IAVAs), Bulletins (IAVBs), and Technical Advisories (TAs). DoD has restricted the use of these terms to the IAVM program only.

IAVA messages shall establish mandatory suspense dates for acknowledgement and compliance, corrective actions to negate vulnerabilities, and implementation of additional CND requirements.

IAVB messages shall establish mandatory suspense dates for acknowledgement yet allow Commanders and IA personnel flexibility for implementation of the corrective actions to negate vulnerabilities or implementation of CND requirements. Corrective actions are required to be completed but not reported.

IATT (Army designation) messages allow Commanders and IA personnel flexibility for acknowledgement and implementation to negate vulnerabilities or implement CND requirements. Acknowledgement and compliance is not reported. Corrective actions are required to be completed but not reported.

All personnel responsible for implementing the IAVM process shall register with the ACERT Listserve to receive messages. Use only official e-mail accounts for this distribution list.

PEO AMMO IAPM/IAM for developmental systems shall disseminate implementation guidance as required and ensure implementation of IAVM requirements; IAVM information is required to support compliance requirements.

PMs are responsible for implementing corrective actions for IAVM vulnerabilities that apply to systems under their proponentcy. Tactical systems will document compliance methodology in a classified addendum as part of the risk assessment or test report of the SSAA (as previously specified). PEO AMMO shall enforce or grant exemptions to IAVM compliance. PEO AMMO will resolve compliance issues where it may result in safety or performance issues of a combat system that are operationally unacceptable.

All PMs must report IAVM compliance in the Army's Compliance Reporting Database (CRD). To meet DoD requirements, register specific system/asset owners including applicable electronic addresses, in the CRD.

All IAVM compliance reporting of classified, tactical, or operationally sensitive information systems will be through the CRD located on the SIPRNET.

At the time of preparation of this document, DA was working on clarification for IAVM implementation and compliance reporting requirements for tactical systems. As a result, additional guidance in this area shall be posted on the PEO AMMO IA area of the AKO as it becomes available.

APPENDIX A ACRONYMS

ABCS	Army Battle Command System
ACERT	Army Computer Emergency Response Team
ADP	Automated Data Processing
AIS	Automated Information System
AISSP	Army Information Systems Security Program
AKO	Army Knowledge Online
AOC	Air Operation Center
AR	Army Regulation
ATCCS	Army Tactical Command and Control System
AWG	Accreditation Working Group
BCD	Battlefield Coordination Detachment
BCE	Battlefield Coordination Element
BIT	Built-in-Test
BITE	Built-In-Test-Equipment
C2	Command and Control
C3I	Command, Control, Communications and Intelligence
CA	Certification Authority
CAPP	Controlled Access Protection Profile
CC	Common Criteria
CCA	Circuit Card Assembly
CCI	Controlled Cryptographic Items
CDR	Critical Design Review
CECOM	Communications-Electronics Command
CINC	Commanders-in-Chief
CIO/G-6	Chief Information Officer/G-6
CM	Configuration Management
CNA	Computer Network Attack
COE	Common Operating Environment
COMPUSEC	Computer Security
COMSEC	Communications Security
CONOPS	Concept of Operations
CONUS	Continental United States
COOP	Continuity of Operations Plan
COTS	Commercial Off-The-Shelf
CRD	Capstone Requirements Document
CTIC	COMSEC Transmission Security Integrated Circuit
CTTA	Certified TEMPEST Technical Authority
C&A	Certification and Accreditation
DA	Department of the Army
DAA	Designated Approving Authority
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
DoD	Department of Defense
DS	Direct Support
DSCG	Digitization Security Classification Guide
DSP	Digital Signal Processor
DSS	Defense Security Service
DTD	Data Transfer Device
ECB	Echelons Corps and Below
ECP	Engineering Change Proposal
EDAC	Error Detection and Correction

EMI	Electro-Magnetic Interference
FM	Frequency Modulation
FOT&E	Follow-On Test and Evaluation
FRB	Failure Review Board
FTA	Facility TEMPEST Assessment
GB	Gigabyte
GCCS	Global Command and Control System
GIG	Global Information Grid
GOTS	Government Off-The-Shelf
GSA	General Services Administration
GUI	Graphical User Interface
HF	High Frequency
HMMWV	High Mobility Multi-Purpose Wheeled Vehicle
HQDA	Headquarters Department of the Army
HTI	Horizontal Technology Integration
IA	Information Assurance
IAM	Information Assurance Manager
IAPM	Information Assurance Program Manager
IASE	Information Assurance Support Environment
IASO	Information Assurance Security Officer
IATO	Interim Approval To Operate
IAVA	Information Assurance Vulnerability Assessment
IDD	Interface Design Document
ILS	Integrated Logistics Support
IMO	Information Management Officer
IMPE	Information Management Processing Equipment
INFOSEC	Information Security
IOT&E	Initial Operational Test and Evaluation
IP	Interface Processor
IPT	Integrated Product Team
ISS	Information Systems Security (IA for Army)
ISSM	Information Systems Security Manager (IAM for Army)
ISSO	Information System Security Officer (IASO for Army)
ISSPM	Information Systems Security Program Manager (IAPM for Army)
ITSEC	Information Technology Security
KC	Knowledge Center
LIWA	Land Information Warfare Activity
LOS	Line of Sight
LPU	Limited Procurement Urgent
LRU	Line Replaceable Unit
LSPP	Labeled Security Protection Profile
LUT	Limited User Test
MACOM	Major Army Command
MAIS	Major Automated Information System
MB	Megabyte
MDAPS	Mandatory Procedures for Major Defense Acquisition Programs
MHz	Megahertz
MOA	Memorandum Of Agreement
MOS	Military Occupational Specialty
MOU	Memorandum Of Understanding
MP	Mission Profile
NDI	Non-Developmental Item
NETT	New Equipment Training Team
NSA	National Security Agency
NSTISSAM	National Security Telecommunications and Information Systems Security Advisory Memorandum

NSTISSI	National Security Telecommunications and Information Systems Security Instruction
NSTISSP	National Security Telecommunications and Information Systems Security Policy
OPSEC	Operations Security
ORD	Operational Requirements Document
OS	Operating System
OTRR	Operational Test Readiness Review
PC	Personal Computer
PCZ	Physical Control Zone
PdM	Product Manager
PDR	Preliminary Design Review
PEO AMMO	Program Executive Officer for Ammunition
PM	Program/Project Manager
PMS	Program Master Schedule
POC	Point of Contact
PPSS	Post-Production Software Support
PROM	Programmable Read-Only Memory
RAM	Random Access Memory
ROM	Read Only Memory
RRAR	Residual Risk Assessment Results
SA	System Administrator
SABI	Secret and Below Interoperability
SAMP	Security/Accreditation Management Plan
SATCOM	Satellite Communications
SBU	Sensitive But Unclassified
SCCB	Software Configuration Control Board
SCG	Security Classification Guide
SCI	Sensitive Compartmented Information
SCM	Software Configuration Management
SEC	Software Engineering Center
SF	Standard Form
SOP	Standing Operating Procedure
SOS	Security Operations Suite
SQA	Software Quality Assurance
SRTM	Security Requirements Traceability Matrix
SSAA	System Security Authorization Agreement
STAR	System Threat Assessment Report
TAIS	Telecommunications and Automated Information System
TCP/IP	Transmission Control Protocol/Internet Protocol
TCSEC	Trusted Computer Security Evaluation Criteria
TFM	Trusted Facility Manual
TMDE	Test, Measurement, and Diagnostic Equipment
TRADOC	U. S. Army Training and Doctrine Command
TRANSEC	Transmission Security
TRR	Test Readiness Review
USG	User's Security Guide
USM	Users Security Manual
VHF	Very High Frequency
VDD	Version Description Document

APPENDIX B DEFINITIONS

Access Control - The process of limiting access to the resources of an automated system only to authorized programs, processes, or other systems (in a network).

Accreditation - A formal declaration by the Designated Approving Authority (DAA) that the AIS is approved to operate in a particular security mode using a prescribed set of safeguards. Accreditation is the official management authorization by a DAA for operation of an automated information system in a particular security mode, using a prescribed set of safeguards based on the certification process, as well as other management considerations. The accreditation statement affixes security responsibility with the DAA and shows that due care has been taken for security.

Automated Information Systems - Any assembly of computer hardware, software, or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information in an electronic form. AIS include stand-alone computers, small computers, word processors, multi-user computers, terminals, and networks.

Automated Information Systems Security - The measures and controls that protect an AIS against denial of service and unauthorized (accidental or intentional) disclosure, modification, or destruction of automated information systems and data.

Category - A restrictive label that has been applied to classified or unclassified data to increase the protection of the data by further restricting access to it. Individuals are granted access to special category information only after being granted formal access authorization.

Caveat - A label that has been applied to classified or unclassified sensitive information to signify that personnel are granted access to the information only if they have appropriate authorization (e.g., NOFORN - information that is not releasable to foreign nationals, WNINTEL - information revealing sensitive intelligence sources and methods). This is also referred to as a Handling Restriction.

Certification - The 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, that establish the extent to which a particular design and implementation meet a specified set of security requirements.

Configuration Control - The systematic proposal, justification, evaluation, coordination, approval or disapproval of proposed changes, and the implementation of all approved changes in the configuration of a configuration item after formal establishment of its baseline.

Controlled Access Protection - Access control through logon procedures, audit of security-relevant events, and resource isolation. Controlled access protection is normally associated with class C2 systems.

Dedicated Security Mode - A mode of operation wherein all users of the AIS possess the required personnel security clearance or authorization, formal access approval (if required), and need-to-know for all data processed by the AIS. Processing in this mode may be full-time or for specific periods of time.

Denial of Service - Action or actions that prevent any part of a Telecommunications and Automated Information System (TAIS) from functioning according to its intended purpose.

Designated Accreditation Authority - A senior management official who has the authority and responsibility to decide to accept or reject the security safeguards prescribed for an AIS, and who may be responsible for issuing an accreditation statement or certificate that records the decision to accept those safeguards for his or her department, agency, or Service.

Emission Security - The protection resulting from all measures taken to deny unauthorized persons information of value that might be derived from intercept and analysis of compromising emanations from cryptographic equipment, automated information systems, and telecommunications systems.

Formal Access Approval - Documented approval to allow access to a particular category of information.

Generic Accreditation - An accreditation in which a single SSAA is prepared for the system with the description of the operating environment reflecting all proposed operation locations. The intent is to produce one SSAA that applies to the system throughout its entire life cycle.

Handling Restriction - A label that has been applied to classified or unclassified sensitive information to signify that personnel are granted access to the information only if they have appropriate authorization (e.g., NOFORN - information that is not releasable to foreign nationals, WNINTEL - information revealing sensitive intelligence sources and methods). Often referred to as a caveat.

Integrity - The degree of protection for data from intentional or unintentional alteration or misuse.

Multilevel Security Mode - A mode of operation wherein not all users of the AIS possess the required personnel security clearance for all data being processed by the AIS.

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

Network - A 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 string of characters used to authenticate an identity.

System High Security Mode - A mode of operation wherein all users of the AIS possess the required personnel security clearance or authorization, but not necessarily a need-to-know, for all data handled by the AIS. If the AIS processes formal categories of information, all users must have formal access approval. This terminology will eventually be replaced by levels of robustness and common criteria terminology.

TEMPEST - The study and investigation of compromising emanations along with criteria for preventing such emanations as per regulations governing electronic equipment emissions.

Type Accreditation - The DoD terminology for the official authorization by the Accreditor to employ a system in a specified environment. It may be performed when multiple platforms will be fielded in similar environments. The Army refers to this as a Generic Accreditation.

APPENDIX C SSAA OUTLINE

The DITSCAP Application Document, DoD 8510.1-M, paragraphs that pertain to each title of this outline are identified in brackets.

Notes have been added to further amplify PEO AMMO content requirements. All the information prescribed by DoD 8510.1_M must be provided in the SSAA.

1.0 MISSION DESCRIPTION AND SYSTEM IDENTIFICATION

- 1.1 System name and identification [See DoD 8510.1-M C3.4.2.2.1]
- 1.2 System description [C3.4.2.2.2]
- 1.3 Functional description [C3.4.2.2.3]
 - 1.3.1 System capabilities [C3.4.2.2.3.1]
 - 1.3.2 System criticality [C3.4.2.2.3.2]
 - 1.3.3 Classification and sensitivity of data processed [C3.4.2.2.3.3]
 - 1.3.4 System user description and clearance levels [C3.4.2.2.3.4]
 - 1.3.5 Life Cycle of the system [C3.4.2.2.3.5]
- 1.4 System CONOPS summary [C3.4.2.2.4]

2.0 ENVIRONMENT DESCRIPTION

- 2.1 Operating environment [C3.4.4.2.1]
 - 2.1.1 Facility Description [C3.4.4.2.1.1]
 - 2.1.2 Physical Security [C3.4.4.2.1.2]
 - 2.1.3 Administrative Issues [C3.4.4.2.1.3]
 - 2.1.4 Personnel [C3.4.4.2.1.4]
 - 2.1.5 COMSEC [C3.4.4.2.1.5]
 - 2.1.6 TEMPEST [C3.4.4.2.1.6]
- Note: All the considerations outlined in Section 6 of this SAMP must be addressed.
- 2.1.7 Maintenance Procedures [C3.4.4.2.1.7]
- 2.1.8 Training Plans [C3.4.4.2.1.8]
- Note: This training plan is for the units and maintainers NOT the CA Team.
- 2.2 Software development and maintenance environment [C3.4.4.2.2]
- 2.3 Threat description [C3.4.4.2.3]

3.0 SYSTEM ARCHITECTURAL DESCRIPTION

- 3.1 System Architecture Description [C3.4.6.2]
- 3.2 System interfaces and external connections [C3.4.6.2.4]
- 3.3 Data flow [C3.4.6.2.5]
- Note: Detailed data flow to include message types, protocols, communications, media types, etc must be shown.
- 3.4 Accreditation boundary [C3.4.6.2.6]

4.0 SYSTEM SECURITY REQUIREMENTS

- 4.1 National and DoD security requirements [C3.4.5.2.1]
- 4.2 Governing security requisites [C3.4.5.2.2]
- 4.3 Data security requirements [C3.4.5.2.3]
- 4.4 Security CONOPS [C3.4.5.2.4]
- 4.5 Network connection rules [C3.4.5.2.5]
- 4.6 Configuration management requirements [C3.4.5.2.6]
- 4.7 Reaccreditation requirements [C3.4.5.2.7]

5.0 ORGANIZATIONS AND RESOURCES

- 5.1 Organizations [C3.4.7.2.1]
- 5.2 Resources [C3.4.7.2.2]
- 5.3 Training [C3.4.7.2.3]

Note: Training for the CA Team not the units.

5.5 Other supporting organizations [C3.4.7.2.4]

6.0 DITSCAP PLAN

6.1 Tailoring factors [C3.4.8.2]

6.1.1 Programmatic considerations [C3.4.8.2.2.1]

Note: IASOs must identify all relevant program issues

6.1.2 Security environment [C3.4.8.2.2.2]

6.1.3 IS characteristics [C3.4.8.2.2.3]

6.1.4 Reuse of previously approved solutions [C3.4.8.2.2.3]

6.2 Tasks and milestones [C7.3.2]

6.3 Schedule summary

6.4 Level of effort [C3.4.8.2]

6.5 Roles and responsibilities

APPENDIX A ACRONYMS

This appendix should include all acronyms used in the SSAA. Additionally those acronyms should be expanded the first time they are used in the SSAA text.

APPENDIX B DEFINITIONS

This appendix should include terms that are relevant to the system for which the SSAA was generated. It is not necessary to include a generic list of terms.

APPENDIX C REFERENCES

This appendix is list of references that includes all security references that apply to the system. It should not be a list of all known security references.

APPENDIX D SYSTEM CONCEPT OF OPERATIONS [C3.4.2.2.4]

This appendix is intended to include a description of the System CONOPS. This is not a repeat of the Security CONOPS that is described in SSAA Par 4.4. Most systems should already have a User (TRADOC System Manager) developed document that can be inserted here, if not, then such a document must be developed.

APPENDIX E INFORMATION SYSTEM SECURITY POLICY

This appendix is intended to include a description of the system's Security Policy statement, which includes a definition of the security requirements of the system based on the minimum evaluation class and on a detailed risk analysis. This Policy addresses all of the projected employment options for the system.

Each system's Security Policy statement must clearly set forth that system's security objectives. The Security Policy will be stated in emphatic terms that would indicate the conditions of the policy are not optional, maximizing the use of the words "will" and "shall." Terms such as "should," "optional," and "if feasible" may imply the conditions of the policy are optional and shall be avoided. These security objectives must be in accordance with the appropriate security requirements, that is those identified in Appendix F of the SSAA, and must be consistent with the PEO AMMO Security Policy. The policy statement must cover the system's initial risk assessment that was used to determine the protection profile appropriate for the system, based on the level of robustness and corresponding to the level of concern assigned to the system.

The Security Policy will contain the following elements:

- System description
- Operating environment description
 - Tactical operations
 - Garrison operations
 - Training

- Risk analysis to determine the protection profile appropriate for the system, based on the level of robustness and corresponding to the level of concern assigned to the system
- Intended sensitivity level
- Summary of security mechanisms to include operational, procedural, and technical to achieve the security objectives, that is the security objectives outlined in the system's protection profile
- Exceptions required, if any, from the minimum requirements of outlined in DoD, Army, or PEO AMMO policy, that is those defined in the systems SRTM. Exceptions must include:
 - Justification based on the standards in paragraph 2-3.b.(4) of AR 380-19 or AR 25-XX (when published)
 - Description of the countermeasures to be employed. The countermeasures proposed will not create an undue operational burden
 - A plan and timetable for meeting the requirements

Criticality is documented in the system security policy. Use the following to identify hardware criticality:

Mission Critical: The loss of the hardware would cause immediate stoppage of direct mission support of mobilization, deployment, or national emergency.

Mission Essential: The loss of the hardware would cause an eventual stoppage of direct mission support of mobilization, deployment, or national emergency.

Mission Impaired: The loss of the hardware would have an effect on (but would not stop) direct mission support of mobilization, deployment, or national emergency.

Non-mission Essential: The loss of the hardware would have no effect on direct mission support of mobilization, deployment, or national emergency.

APPENDIX F SECURITY REQUIREMENTS AND/OR REQUIREMENTS TRACEABILITY MATRIX [C3.4.5.2.8]

This appendix must identify all of the security requirements that must be met by the given system. That information must be provided in the correct format. Example checklists/tools are available on the PEO AMMO IA area of the AKO.

APPENDIX G CERTIFICATION TEST AND EVALUATION PLAN AND PROCEDURES (TYPE ONLY)

This appendix must contain the Certification Test and Evaluation (CT&E) information that is comprised of the set of software and hardware security tests conducted during the development of the system.

APPENDIX H SECURITY TEST AND EVALUATION PLAN AND PROCEDURES

This appendix must contain the Security Test and Evaluation (ST&E) information which is comprised of the examination and analysis of the safeguards required to protect the system, as they have been applied in an operational environment, to determine the security posture of that system.

APPENDIX I APPLICABLE SYSTEM DEVELOPMENT ARTIFACTS OR SYSTEM DOCUMENTATION

This appendix must contain, at a minimum, the System Security Classification Guide (SCG), all approved waivers, National Security Agency (NSA) Endorsements (for systems using NSA products/COMSEC), and unclassified TEMPEST statements by the Army CTTA (if classified, then the CTTA reports go in Appendix P).

APPENDIX J SYSTEM RULES OF BEHAVIOR

This appendix must identify the security "Do's" and "Don'ts" of the system, providing a concise list of rules the operators must be particularly aware of implementing. The appendix will also assist commanders, managers and users in identifying the key points that must be remembered. This will aid key leaders in identifying important procedures that need to be addressed without having to study the entire SOP. This appendix should be no more than a few pages and should be easily understood by non-technical personnel. These rules would also be identified in the SOP that would provide the details that users and security personnel directly involved with the system need to study.

APPENDIX K INCIDENT RESPONSE PLAN

This appendix must identify the actions to be taken when a security incident occurs. It must also be consistent with the procedures in the USM/SOP and those required by the current Army policy, e.g. AR 380-19, and the IAVA process.

APPENDIX L CONTINGENCY PLAN [5.3.8.2]

This appendix must contain the Contingency Plan(s) that describe the emergency responses, backup procedures, backup operations, recovery, and emergency destruction of classified and unclassified sensitive information. DoD 8510.1-M states that "the contingency plan evaluation task analyzes the contingency, backup, and continuity of service plans to ensure the plans are consistent with the requirements identified in the SSAA." Periodic testing of the contingency plan is required for critical systems and is encouraged for all systems. Note that PEO AMMO IA area of the AKO contains documents that provide guidance for contingency planning but these must be tailored for tactical data systems by addressing additional considerations such as actions in the event of capture of the system by an enemy force in an overrun situation.

Appendix M PERSONNEL CONTROLS AND TECHNICAL SECURITY CONTROLS

This appendix must contain the Users Security Manual and Standing Operating Procedure (USM/SOP). The Security Features User's Guide (SFG) and Trusted Facility Manual (TFM), if the system has them, should also be found here. The procedures cited in the USM/SOP will be stated in emphatic terms that would indicate the procedures are not optional, maximizing the use of the words "will" and "shall." Terms such as "should," "optional," and "if feasible" may imply the procedures are optional and shall be avoided. Additionally, if the users of the system have an option to conduct training at an unclassified level, the SOP must cover the step by step procedures for securely setting up and configuring the system for operation at an unclassified level and then returning it to the normal classified mode of operations. The format for the USM/SOP is as follows:

1	INTRODUCTION
2	PURPOSE
3	SCOPE
4	REFERENCES
5	GENERAL
5.1	System Accreditation
5.2	System Description
5.3	Abbreviations, Acronyms, and Definitions
6	RESPONSIBILITIES
6.1	System Commander
6.2	Information Assurance Security Officer (IASO)
6.3	Battalion Commanders
6.4	Security Managers
6.5	Operators
6.6	Other
7	PROCEDURES
7.1	Operations Security (OPSEC)
7.2	Physical Security

7.2.1	Pre-deployment
7.2.2	Tactical Operations
7.2.3	Re-deployment to Garrison
7.2.4	Garrison Operations
7.3	Software Security
7.4	Document Security
7.5	Personnel Security
7.5.1	Access Control
7.5.2	Accountability
7.6	Communications Security
7.7	Emissions Security (TEMPEST)
8	COMPROMISE
8.1	Suspected or Known Loss
8.2	Authentication and Signal Operation Instructions (SOI)
9	EMERGENCY REMOVAL AND DESTRUCTION PLAN
9.1	Emergency Security
9.2	Emergency Removal
9.3	Emergency Destruction
10	TRAINING
10.1	Operators, Supervisors, and Personnel With Access
10.2	Emergency Deployment Readiness Exercises and Alerts
10.3	Exercises
Annex A.	Information System Security Briefing
Annex B.	Type Accreditation Compliance Checklist
Annex C.	System Administration Guide

APPENDIX N MEMORANDUMS OF AGREEMENT - SYSTEM INTERCONNECT AGREEMENTS

This appendix must contain any existing System Interconnect Agreements, where the system will connect to other networks or other systems (see AR 380-19). Other systems and networks may be controlled by other service DAAs such as the Air Force Air Operation Center (AOC) Local Area Networks (LANs) in the Battlefield Coordination Detachment/Element (BCD/BCE) Environment. Paragraph 2-22 of AR 380-19 describes circumstances when Memorandums Of Understanding (MOUs) /Memorandums Of Agreement (MOAs) are required. Sample MOAs are provided in the policy of some networks/systems and templates for MOAs have been posted to the PEO AMMO Knowledge Center.

APPENDIX O SECURITY EDUCATION, TRAINING, AND AWARENESS PLAN

This appendix must contain a plan for Security Education, Training, and Awareness, unless that information has already been provided in the USM/SOP.

APPENDIX P TEST AND EVALUATION REPORT(S)

This appendix must be classified in accordance with SCG guidance and AR 380-5, and it must contain all formal test and analysis results. It must address the results of the testing and evaluation of all requirements contained in the SRTM for the system. The findings of the C&A system vulnerability scans performed by the CA as part of system integration must be documented here. TEMPEST reports must be included here as well.

APPENDIX Q RESIDUAL RISK ASSESSMENT RESULTS

This appendix must be classified in accordance with SCG guidance and AR 380-5, and it must address the findings documented in Appendix P, Test and Evaluation Report(s). The risks, threats, and countermeasures identified in the risk assessment/risk management review must be coherently described. The findings of the C&A system vulnerability scans performed by the CA, as part of system integration must be addressed here. The residual risk assessment must cover all findings to include risks that were not mitigated in some way, and all PEO letters directing that technical fixes be made based on these scans.

TEMPEST countermeasures and considerations must also be addressed. IAVA compliance must be addressed for all IAVAs current up to the day the package is submitted to PEO AMMO. The format for the Residual Risk Assessment Results (RRAR) is as follows:

1	INTRODUCTION
1.1	Purpose
1.2	Scope
1.3	Document Structure
2	DESCRIPTION OF THE RISK ASSESSMENT PROCESS
2.1	Risk Management Methodology
2.2	Risk Analysis Methodology
3	SYSTEM THREAT IDENTIFICATION
3.1	Threats To The System
3.2	Life Cycle Considerations
3.3	System Assets Subject To Attack
4	SYSTEM RISK ASSESSMENT
4.1	Risk Assessment Summary
4.2	Risk Assessment For Each Life Cycle Phase
4.2.1	Life Cycle Phase - Development and Production
4.2.1.1	Issue Statement
4.2.1.2	Impact Statement
4.2.1.3	Countermeasures
4.2.1.4	Residual Risk
4.2.2	Life Cycle Phase - Fielding
4.2.2.1	Issue Statement
4.2.2.2	Impact Statement
4.2.2.3	Countermeasures
4.2.2.4	Residual Risk
4.2.3	Life Cycle Phase - Garrison Operations
4.2.3.1	Issue Statement
4.2.3.2	Impact Statement
4.2.3.3	Countermeasures
4.2.3.4	Residual Risk
4.2.4	Life Cycle Phase - Exercises
4.2.4.1	Issue Statement
4.2.4.2	Impact Statement
4.2.4.3	Countermeasures
4.2.4.4	Residual Risk
4.2.5	Life Cycle Phase - Physical Combat
4.2.5.1	Issue Statement
4.2.5.2	Impact Statement
4.2.5.3	Countermeasures
4.2.5.4	Residual Risk
4.2.6	Life Cycle Phase - Post-deployment Support and Maintenance
4.2.6.1	Issue Statement
4.2.6.2	Impact Statement
4.2.6.3	Countermeasures
4.2.6.4	Residual Risk
4.3	Assessment of Technical Vulnerabilities
5	EFFECTIVENESS REVIEW
6	SECURITY ASSESSMENT RECOMMENDATIONS
7	IAVA COMPLIANCE
7.1	General Discussion
	General Discussion of all IAVAs in this section
7.2	Table of Compliance

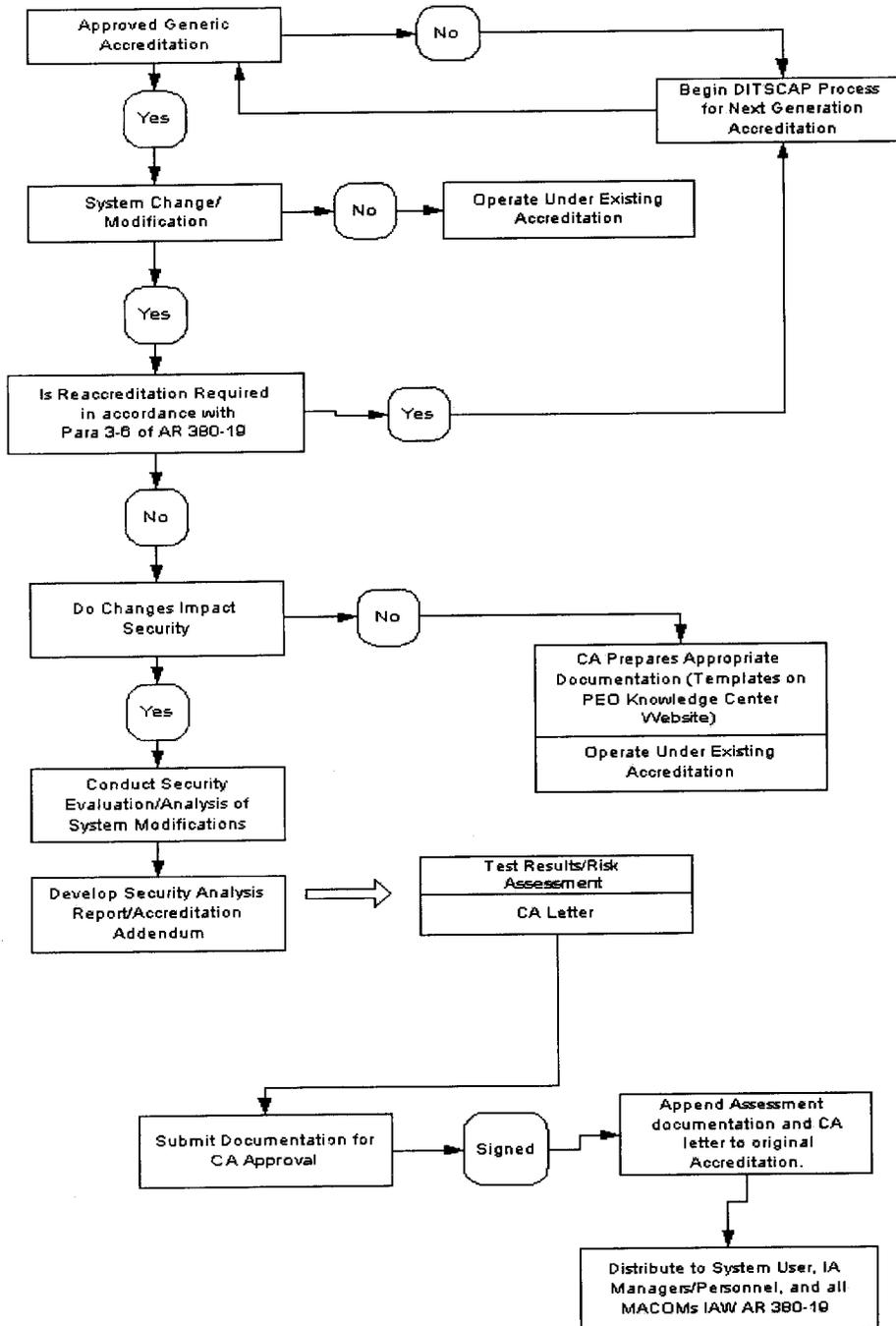
	Table includes IAVA Identification, Subject, Date, Systems Affected, Applicability to the Given System
7.3	Table of Non-Compliance
	Table includes IAVA Identification, Subject, Date, Systems Affected, Applicability to the Given System
7.3.1	Issue Statement
7.3.2	Impact Statement
7.3.3	Countermeasures
7.3.4	Residual Risk
7.4	Recommendations

APPENDIX R CERTIFICATION AND ACCREDITATION STATEMENTS

This appendix must contain the Certification Authority recommendation and the Accreditation Memorandum. Examples are available on the PEO AMMO IA area of the AKO. The format must be correct and the wording must be precise or the SSAA will not be approved. Be sure to check the PEO AMMO IA area of the AKO before developing a new Appendix R to ensure that you have the latest format.

**APPENDIX D
REACCREDITATION ASSESSMENT ADDENDUM AND IATO PROCESSES**

**Reaccreditation Assessment
(Addendum Process)**



IATO Process

