NISTIR 5540

# Multi-Agency Certification and Accreditation (C&A) Process: A Worked Example

**Ellen Flahavin**
**NIST**

**Annabelle Lee**
**The MITRE Corporation**

**Dawn Wolcott**
**The MITRE Corporation**

**Sponsored by:**
**Drug Enforcement Administration**

U.S. DEPARTMENT OF COMMERCE
Technology Administration
National Institute of Standards
and Technology
Gaithersburg, MD 20899

NIST

NISTIR 5540

# Multi-Agency Certification and Accreditation (C&A) Process: A Worked Example

**Ellen Flahavin**
**NIST**

**Annabelle Lee**
**The MITRE Corporation**

**Dawn Wolcott**
**The MITRE Corporation**

**Sponsored by:**
**Drug Enforcement Administration**

U.S. DEPARTMENT OF COMMERCE
Technology Administration
National Institute of Standards
and Technology
Gaithersburg, MD 20899

December 1994


U.S. DEPARTMENT OF COMMERCE
Ronald H. Brown, Secretary

TECHNOLOGY ADMINISTRATION
Mary L. Good, Under Secretary for Technology

NATIONAL INSTITUTE OF STANDARDS
AND TECHNOLOGY
Arati Prabhakar, Director

## FOREWORD

This National Institute of Standards and Technology Interagency Report (NISTIR) presents a practical example on how to perform multi-agency certification and accreditation (C&A).

The National Institute of Standards and Technology (NIST) makes no claim or endorsement of this C&A method. However, as this material may be of use to other organizations, NIST participated in producing and printing the document to make the lessons learned publicly available and to provide for broad dissemination of this federally sponsored work. This publication is part of a continuing effort to assist federal agencies in accordance with NIST's mandate under the Computer Security Act of 1987.

NIST expresses its appreciation to the Drug Enforcement Administration (DEA) for their contributions to this report.

Questions regarding this publication should be addressed to the Computer Security Division, National Computer Systems Laboratory, Building 225, Room B221, National Institute of Standards and Technology, Gaithersburg, MD, 20899.

Additional copies of this publication may be purchased through the National Technical Information Service, Springfield, VA, 22161. telephone: (703) 487-4650.

1. INTRODUCTION . . . . . 1
1.1 EPIC and the Mountain Pass Project . . . . . 1
1.2 Scope of the Mountain Pass Security Effort . . . . . 3
1.3 Mountain Pass Development Methodology . . . . . 3

2. SECURITY ENGINEERING . . . . . 5
2.1 Security Engineering Life Cycle . . . . . 5
2.2 EIS Security Requirements Development . . . . . 7
2.3 FIPS PUB 102 Certification and Accreditation (C&A) Process . . . . . 9
2.4 EPIC C&A Process . . . . . 10
2.5 Functional Description of Mountain Pass Certification Tasks . . . . . 13

3. SYSTEM DEVELOPMENT ROLES AND RESPONSIBILITIES . . . . . 19
3.1 Program Management . . . . . 20
3.2 Senior Management Team (SMT) . . . . . 20
3.3 Systems Engineering . . . . . 20
3.4 Integration Contractor . . . . . 21
3.5 Risk Analysis and Vulnerability Assessment (RAVA) Contractor . . . . . 21
3.6 Security Test and Evaluation (ST&E) Contractor . . . . . 21
3.7 Working Groups . . . . . 21
3.7.1 Certification Working Group (CWG) . . . . . 21
3.7.2 Accreditation Working Group (AWG) . . . . . 22
3.7.3 Working Group Charter . . . . . 23

4. CERTIFICATION TESTING AND ACCREDITATION DOCUMENTATION . . . . 25
4.1 System Security Plan . . . . . 25
4.2 Risk Analysis and Vulnerability Assessment (RAVA) Report . . . . . 30
4.3 Security Policies and Procedures . . . . . 31
4.4 Trusted Facility Manual (TFM) . . . . . 33
4.5 Certification Test Documentation . . . . . 33
4.5.1 Security Test and Evaluation (ST&E) Plan . . . . . 33
4.5.2 Test Report . . . . . 34
4.6 Accreditation Package . . . . . 35

5. LESSONS LEARNED . . . . . 37
5.1 Management Lessons Learned . . . . . 37
5.2 Technical Lessons Learned . . . . . 38
5.3 Summary . . . . . 39

APPENDIX A: SECURITY REQUIREMENTS MATRIX . . . . . 41

APPENDIX B: CERTIFICATION AND ACCREDITATION LETTER ..... 47

APPENDIX C: CHARTER - SECURITY REVIEW COMMITTEE ..... 49

APPENDIX D: POLICIES, REGULATIONS, AND STANDARDS ..... 53

APPENDIX E: SAMPLE MEMORANDUM OF UNDERSTANDING ..... 57

APPENDIX F: EPIC C&A TASKS AND SCHEDULE ..... 71

APPENDIX G: GLOSSARY ..... 77

## LIST OF TABLES

**Table** **Page**

Table 4-1. Test Report Matrix . . . . . 34

## LIST OF FIGURES

**Figure** **Page**

Figure 2-1. Systems Engineering Life Cycle . . . . . 5
Figure 2-2. EIS Security Process and Responsibilities . . . . . 9
Figure 2-3. Mountain Pass Phase I: Certification and Accreditation Process . . . . . 11
Figure 2-4. Mountain Pass Phase II: Certification and Accreditation Process . . . . . 12
Figure 2-5. Mountain Pass OT&E and Final C&A Process . . . . . 13
Figure 3-1. Mountain Pass Roles and Responsibilities . . . . . 19
Figure 4-1. Sample Security Architecture Diagram: EIS Unclassified Region . . . . . 28
Figure 4-2. Sample Security Architecture Diagram: EIS Classified Region . . . . . 29

# 1. INTRODUCTION

This document describes a worked example of a multi-agency certification and accreditation (C&A) process. The objective of this document is to provide a practical example of how to perform multi-agency C&A. The example is based on a project implemented for the Drug Enforcement Administration (DEA), called Mountain Pass. The project was implemented to improve the El Paso Intelligence Center (EPIC) information system and related communications and to satisfy EPIC's current and anticipated system needs. EPIC is a multi-agency facility managed by DEA, located in El Paso, Texas and supported by personnel from various participating federal agencies. Mountain Pass was certified and accredited by DEA with the participating agencies defining and assisting the certification process and accepting the implemented security features.

The Mountain Pass Project was completed in November 1992 and was managed jointly by the Department of Justice (DOJ), DEA, the Department of Defense (DOD), and the Defense Information Systems Agency (DISA). DISA was the Project Manager (PM) and DEA was the Deputy PM.

This document includes sample tables, reports, outlines, and charters to assist other Federal agencies in their multi-agency C&A efforts. Although this document focuses on the Mountain Pass Project, the lessons learned and general guidelines provide practical guidance to all civil Federal agencies that perform multi-agency C&A. Also, this document focuses on the certification activities.

This document consists of five sections and seven appendices. The emphasis in the body of the document is how multi-agency C&A may be performed and the appendices provide samples and examples. Section 1 provides an overview of the Mountain Pass Project. Section 2 discusses the security engineering life cycle, the general C&A process, and the EPIC C&A process. Section 3 describes the EPIC system development roles and responsibilities. Section 4 describes the EPIC certification testing and the accreditation documentation. Finally, Section 5 summarizes the lessons learned from the EPIC project. Appendix A includes a security requirements matrix. Appendix B includes a sample letter to the external agencies requesting support on the C&A effort. Appendix C includes a charter for one of the working groups. Appendix D includes the policies, standards, and regulations that were used to develop the EPIC security requirements. Appendix E includes a generic memorandum of understanding. Appendix F lists the C&A tasks and provides a time table for their completion. Finally, appendix G includes a glossary.

## 1.1 EPIC and the Mountain Pass Project

EPIC is supported by personnel from various participating agencies (e.g., Federal Aviation Administration, United States (U.S.) Coast Guard, U.S. Customs Service). Its mission is to

provide intelligence on drug movement throughout the world by land, sea, and air that is relevant to the United States. EPIC's functions are to:

- Provide time-sensitive intelligence support to Law Enforcement Agencies (LEAs). For example, act as a *clearing house* for suspect information
- Coordinate investigations among LEAs
- Maintain an intelligence baseline on drug movement information

The EPIC Information System (EIS) Mountain Pass Project established the first increment of an objective architecture to upgrade and improve the existing system. The Mountain Pass project was itself divided into two phases. The focus of Mountain Pass was to upgrade the existing system and integrate existing database files.

Mountain Pass served the following functions:

- Replaced obsolescent systems and equipment
- Provided enhanced data processing capabilities
- Integrated stand-alone automated data processing (ADP) systems and communications links
- Consolidated existing files into a database management system (DBMS) - (EPIC Internal Database (EID))
- Defined an objective system architecture for the mid-1990's
- Provided EPIC with an improved, integrated information system by building the initial increment of the objective architecture
- Defined a strategy for getting from Mountain Pass to the objective system

The EIS provided enhanced and integrated capabilities which could be tailored to the needs of authorized EPIC users. EIS was built using open system principles that support the future integration of commercial or Government-developed products. Commercial-off-the-shelf (COTS) hardware and software products satisfied most EPIC needs for automated support.

## 1.2 Scope of the Mountain Pass Security Effort

Certification is required by OMB Circular A-130 for all computer applications processing Sensitive Unclassified (hereafter referred to as Sensitive) information. FIPS PUB 102, *Guideline to Computer Security Certification and Accreditation*, 27 September 1983, was the document used for C&A guidance on the EPIC project. FIPS PUB 102 presents, in detail, an approach to developing a program and performing a technical process for certifying and accrediting Sensitive applications.

Prior to Mountain Pass, C&A activities at EPIC were handled in an informal manner, with no formal process. For example, the majority of the EPIC documentation addressed the day-to-day operation of the facility and the agreements between the various Federal agencies that participate in EPIC. The Mountain Pass C&A process was intended to address Federal, DOJ, and DEA security standards, guidelines, and requirements. Because EPIC is sponsored and operated by multiple Federal agencies, these agencies were requested to actively participate in the Mountain Pass security engineering and C&A activities. This document describes the security activities, C&A program, tasks, and roles that were developed and implemented for the Mountain Pass Project.

## 1.3 Mountain Pass Development Methodology

The system development methodology that was followed at EPIC was a tailored analyze-design-plan-implement approach. First, a detailed functional analysis of the EPIC environment was conducted. The current EPIC environment was analyzed to determine how, why, when, where, and what tasks were being performed, who performed the tasks, and what products were prepared. Specifically, the analysis included a review of all system-related documents, interviews with current and proposed users and system specialists, and observation of the current system operation. The result of the functional analysis was a recommended Functional Architecture which addressed EPIC's functional requirements and alternative design concepts.

Using the Functional Architecture, the Mountain Pass Project team used a COTS integration approach that allowed the system architects and engineers to quickly define and implement a low risk development strategy. This was necessary because of the extremely tight schedule for completing the project. Additional principles applied to the Mountain Pass Project were to:

- Build on existing capabilities where feasible

- Implement the *obvious* (high value, low risk)
  - Use proven solutions
  - Use standard protocols and interfaces

- Emphasize COTS integration versus research and development solutions
- Implement a configuration management program
- Design to accommodate projected growth in database size, external system access, and user population
- Implement a training program

The key Mountain Pass Project architectural decisions were to:

- Utilize a client-server processing model with:
  - Centralized, specialized servers
  - Distributed workstations
- Install separate Secret and Sensitive local area networks (LANs) with a low-to-high security guard separating the two regions
- Require software that met the C2 functionality as defined in DOD 5200.28-STD, *The Trusted Computer System Evaluation Criteria (TCSEC)*. Specifically, Mountain Pass required:
  - Implementation of a C2-compliant relational DBMS
  - Installation of a C2-compliant multi-tasking operating system for workstations and servers

In addition, the security architecture was limited by the following two constraints: (1) existing policies for the safeguarding of Sensitive and Classified information and (2) the availability of technology to segregate data at different classification levels.

The Mountain Pass security architecture was implemented in two phases. In Phase I, the basic capabilities were provided to two pilot workgroups at EPIC. In Phase II, these capabilities were incrementally expanded and tailored to other workgroups. Also, in Phase II, four major upgrades were added: automated login, multi-database query, DBMS, and the EPIC Guard. Both phases were completed in approximately eighteen months.

# 2. SECURITY ENGINEERING

Security engineering (including C&A) for Mountain Pass was included as part of the system engineering life cycle. Due to the extremely tight schedule for implementing Mountain Pass, the security engineering tasks were developed and executed concurrently with the system design and development activities. In addition, the security engineering tasks were performed in parallel, specifically, development of a security architecture, definition of security requirements, and preparation of a System Security Plan (SSP).

## 2.1 Security Engineering Life Cycle

Figure 2-1 illustrates the system engineering life cycle stages. Following the figure is a summary of the security tasks that are performed at each system engineering life cycle stage with Mountain Pass security engineering tasks also included. Mountain Pass tasks are listed in italics. The purpose of the summary is to identify and sequence the Mountain Pass security tasks as part of the system engineering process. The specific Mountain Pass tasks are discussed in detail in later sections of this document.

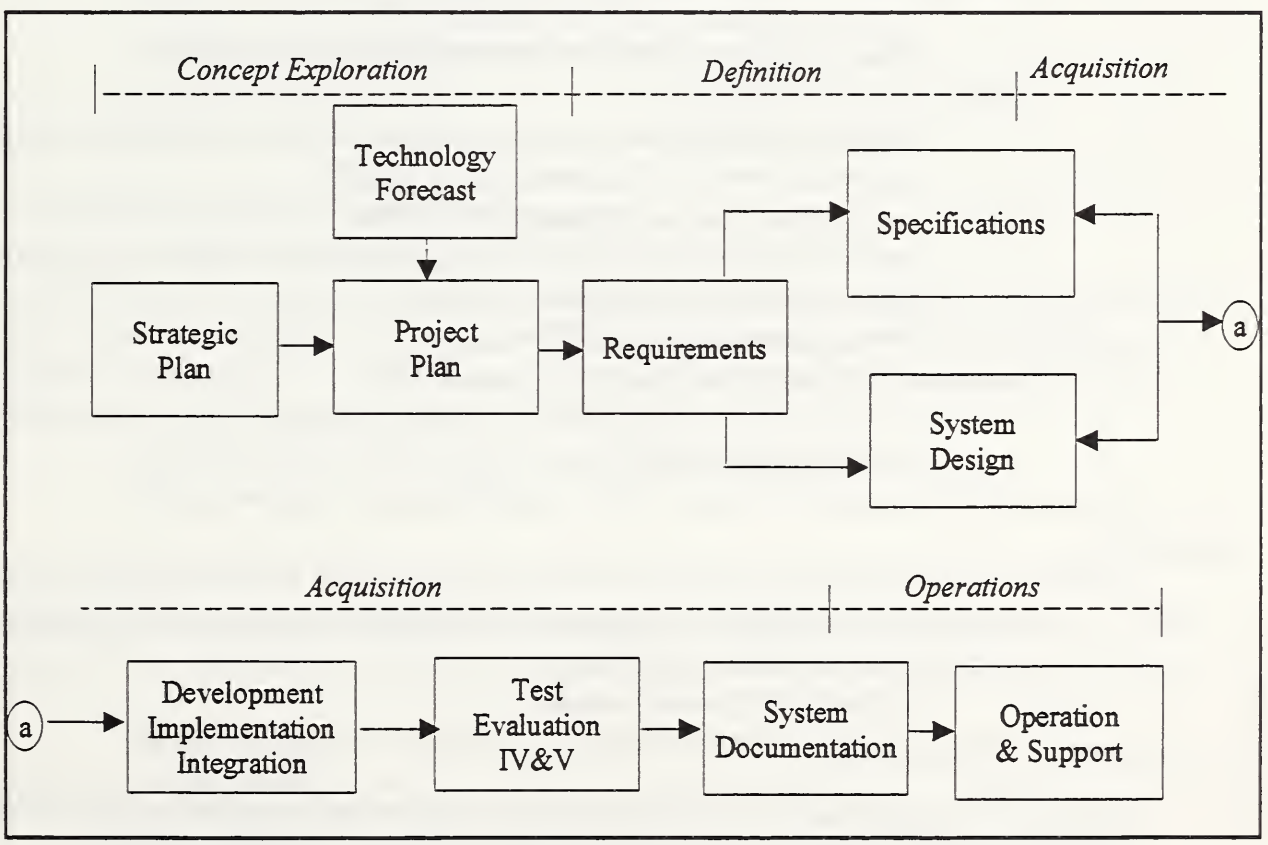


**Figure 2-1. Systems Engineering Life Cycle**

Concept Exploration:

- Conduct initial risk/threat assessment
  - *Specify clearance levels of users and sensitivity levels of data*
- Analyze security capabilities and priorities
  - *Review the DEA Headquarters security requirements*
- Identify/consult the Designated Approving Authority (DAA)
  - *Identify the DAA for EPIC*
- Identify applicable security standards
  - *Identify applicable security standards*
  - *Review Federal, DOJ, and DEA security documents and standards*

Definition:

- Evaluate system risk
  - *Review existing DEA Headquarters risk analyses*
- Analyze security capabilities and constraints
  - *Review the DEA Headquarters security functionality*
- Develop security requirements[1]
  - *Prepare a glossary of terms and definitions*
  - *Identify, validate, and document security requirements*
- Define security architecture
  - *Prepare a system security architecture (including identification of the systems/networks to be connected to the EIS)*
- Develop acquisition plan and high level C&A Plan
  - *Prepare the RFP and a C&A Plan (including the tasks to be performed in support of the accreditation decision)*
  - *Develop a schedule of C&A tasks*
- Include security in the acquisition documentation
  - *Provide status briefings to the working groups, EPIC personnel, DAA, and the Management Team*

Acquisition:

- Revise security requirements and security architecture based on comments received and prepare security design
  - *Revise security requirements*

---

[1] (EIS security requirements are based on the C2 requirements specified in DOD 5200.28-STD. The major extensions to C2 are in auditing, security administration, and configuration management. These variations are derived from DOJ and DEA requirements.)

  - *Revise system security architecture*
  - *Identify security roles and responsibilities*
  - *Prepare a Memorandum of Understanding (MOU) between EPIC and the external agencies*
  - *Prepare a System Security Plan (EIS SSP)*
- Evaluate system risk
  - *Conduct a risk analysis and vulnerability assessment (RAVA)*
- Perform certification tests
  - *Perform security test and evaluation (ST&E)*
  - *Provide status briefings to the working groups, EPIC personnel, DAA, and the SMT*
- Perform security training
  - *Train the EPIC users and security officer*
- Accredit the system
  - *Prepare an interim and a final Accreditation Statement*

Operations:

- Recertify and reaccredit the system
- Analyze residual risk
- Identify security enhancements/revisions
- Perform security audits

## 2.2 EIS Security Requirements Development

The set of EIS security requirements was primarily based on security features implemented for systems at DEA Headquarters. Initially, the EIS Security Requirements team, consisting of representatives from DOJ, DEA, EPIC, and the Mountain Pass project team, met at EPIC to:

- Identify/validate the baseline security requirements
- Assign security responsibilities to EPIC and DEA Headquarters personnel

The Security Requirements Team agreed on a set of security requirements and identified implementation issues, for example, the resources required and schedule implications. At the completion of the requirements definition process, the proposed security requirements were:

- Reviewed with EPIC and DEA Headquarters personnel for accuracy and completeness

- Validated and accepted by the project Senior Management Team (SMT)

- Briefed to the Mountain Pass security working groups (e.g., Accreditation Working Group (AWG) and Certification Working Group (CWG)) for concurrence

- Provided to the representatives of the participating Federal agencies. Additional security requirements were defined by the external Federal agencies that provided data to EPIC via electronic connections.

To ensure concurrence on the security requirements by all participants, a security requirements review process was implemented and a security matrix was developed to document and track the security requirements. This matrix listed for each security requirement:

- Applicable federal, DOJ, and DEA security policies, standards, and/or regulations. This reference was the source for the security requirement.

- Device(s) and component(s) where the security requirement was implemented

- Organization responsible for implementing the security requirement, for example, integration contractor

- Test method (inspection, demonstration, test)

A sample security requirements matrix is included in appendix A, table A-1. Although the table is not intended to be a comprehensive list of all the Mountain Pass security requirements, it does include many examples. For Mountain Pass, the security requirements matrix was modified several times to include new requirements and the refinement/modification of existing requirements. The final security requirements matrix was used in the Mountain Pass Project to provide continuity and traceability of the requirements from source document to implementation. In addition, these security requirements were used by the ST&E and RAVA contractors in performing their security tasks. The ST&E contractor developed security tests based on the requirements and the RAVA contractor evaluated the security countermeasures against the security requirements.

Figure 2-2 assigns responsibilities to organizations involved in the EPIC project. For example, the system developer was responsible for designing and implementing the system. The life cycle stages identified in figure 2-1 are listed in italics in figure 2-2.

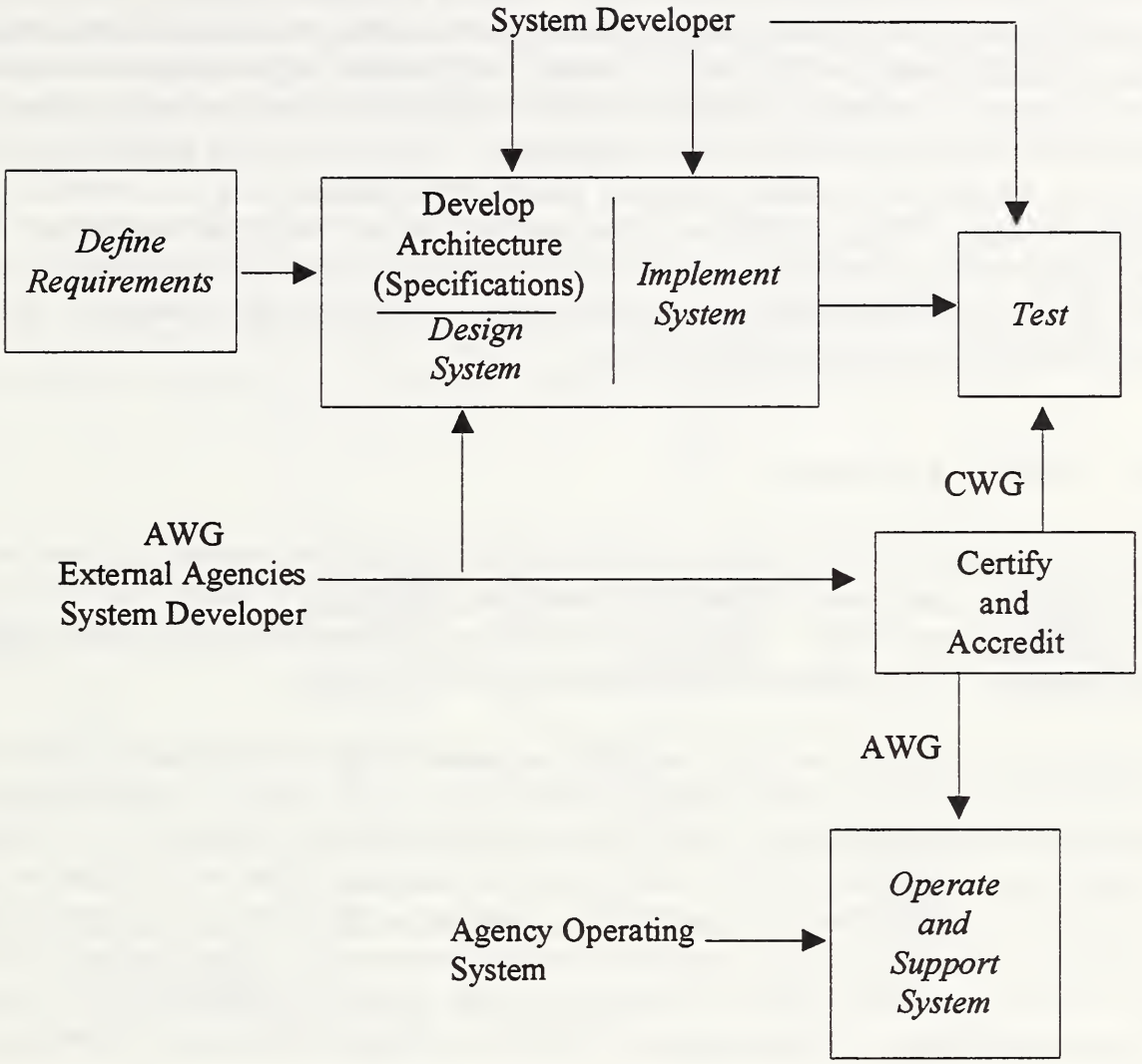


**Figure 2-2. EIS Security Process and Responsibilities**

## 2.3 FIPS PUB 102 Certification and Accreditation (C&A) Process

The EIS certification process was based on the process defined in FIPS PUB 102, *Guideline for Computer Security Certification and Accreditation*. This standard was used because EPIC is primarily authorized and staffed by Federal civil agencies and the National Institute of Standards and Technology (NIST) is responsible for providing guidance for civil agencies that process Sensitive information.

As defined in FIPS PUB 102, the certification effort is divided into basic evaluation and detailed evaluation. The general distinction between basic and detailed evaluations is that basic evaluation focuses on the *overall* security functionality. Detailed evaluation focuses on whether specific security features work correctly, satisfy performance criteria, and acceptably resist penetration. The certification process is an iterative process, with previous stages being reentered and the work repeated. For example, during basic evaluation/RAVA, a new security function may be identified that had not been previously documented. Development of a new security function may require a revision to the security boundary defined in the planning stage and repetition of the data collection stages. At the completion of the certification tests, the formal acceptance of system security by the DAA is based on the Security Evaluation Report/Certification Report of Findings and the documentation developed during the system engineering life cycle stages. The DAA for EIS was the Deputy Administrator of DEA.

## 2.4 EPIC C&A Process

Due to the nature of DEA's mission and the sensitivity of its data, evaluating system security, implementing appropriate safeguards, and certifying systems are a vital part of DEA's system life cycle development process. Due to EPIC's mission and the sensitivity of its data, security was also important to the agencies that participate at EPIC.

Certification of the EIS involved a technical assessment of the security features/functionality to determine the extent that these features met the EIS and DEA security requirements and applicable security policies (e.g., DOJ, Executive Orders (E.O.s), Privacy Act). Certification also included executing security tests to demonstrate the adequacy of the security features and requirements. Accreditation of the EIS was a management decision by the Deputy Administrator of DEA to operate the EIS in a specific operational environment. The objective of the C&A effort was to accredit the EIS as a partitioned system, physically separated into two regions: a Sensitive region and a Classified region, with a low-to-high security guard connecting the two regions.

For Mountain Pass, RAVA was selected as the basic evaluation methodology. ST&E was selected as the detailed evaluation methodology. Both methodologies assess the adequacy of the security features, but from different perspectives. RAVA focused on the appropriateness of the safeguards to minimize risk and ST&E focused on the functionality and effectiveness of the safeguards.

EIS C&A addressed the iteration process in two ways:

- The certification process was repeated twice after Phase I - in Phase II at the completion of the four major upgrades, and at the completion of Phase II - (Operational Test and Evaluation (OT&E))

- The Phase I C&A process was intended to serve as a *pilot* for the later phases, with revisions to the process based on lessons learned during Phase I

The basic and detailed evaluation tasks were not performed sequentially; rather, the tasks were implemented concurrently. This is typical of most C&A efforts. Also, an interim accreditation was requested at the completion of Phase I and final accreditation requested at the completion of Phase II.

The following diagrams illustrate the C&A process for EIS. Figures 2-3 and 2-4 illustrate the C&A process applicable for Phases I and II of Mountain Pass, respectively. The number of tasks that were completed during each phase (e.g., data review, RAVA) varied by phase. For example, in Phase I, the ST&E included a minimal number of tasks based on the technical capabilities that were implemented. The major changes at each phase are in italics.

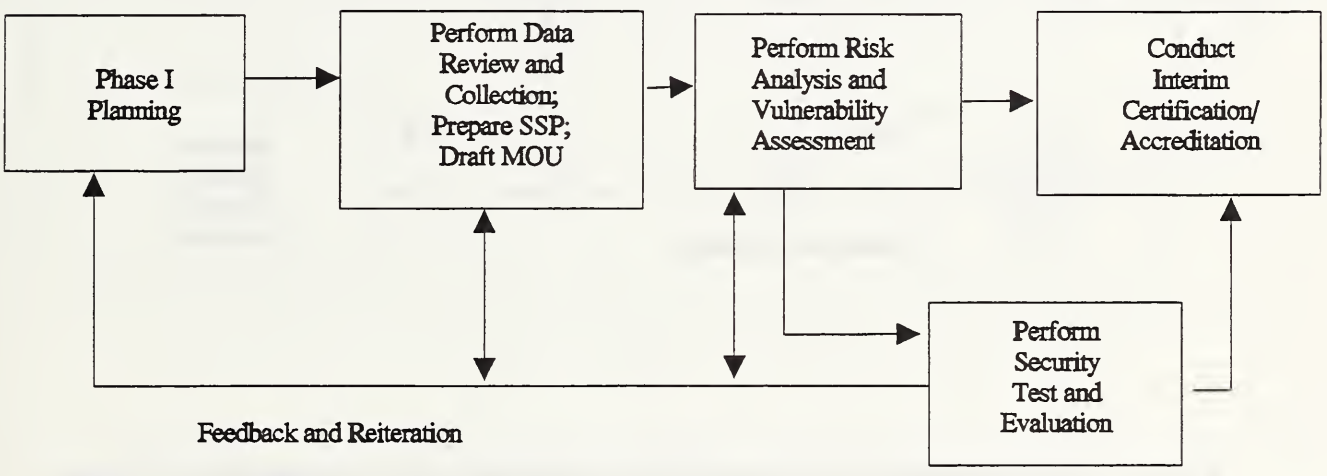


**Figure 2-3. Mountain Pass Phase I: Certification and Accreditation Process**

Phase I certification focused on the existing physical and administrative/personnel security functionality because the number of technical security features that were implemented was limited. In general, the Phase I security features were provided by COTS products. At the completion of Phase I, an interim accreditation from the DAA was requested. This accreditation did not include the MOUs for the external systems because the existing technical data exchange arrangements did not change until Phase II. Goals of the Phase I certification effort were to test the certification process and make refinements, if required. This effort was critical because of the limited time frame for Mountain Pass and the number of C&A tasks

that overlapped throughout the project.

Phase II certification focused on the following areas: implementation of the security features in other EPIC workgroups, installation of the four major upgrades, and review of the physical and administrative security features to ensure they have not been modified. At the completion of Phase II, the DAA and the AWG were briefed on the status of the certification tasks. Interim accreditation was not requested at the completion of Phase II.

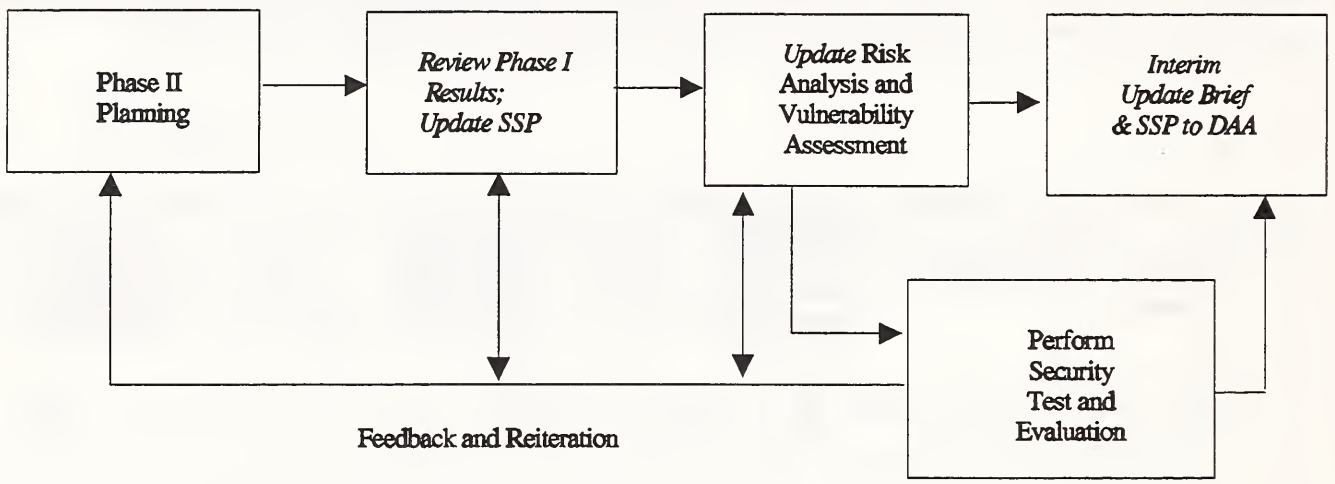


**Figure 2-4. Mountain Pass Phase II: Certification and Accreditation Process**

At the completion of Phase II (OT&E), a final system certification test was performed, as illustrated in figure 2-5. This final certification included the certification tasks performed for Phases I and II and additional security tests for the integrated system. The objectives were to verify that the security functionality implemented in Phases I and II had not been compromised, particularly the physical and personnel security safeguards, and to test the new technical and procedural security features for the entire system.

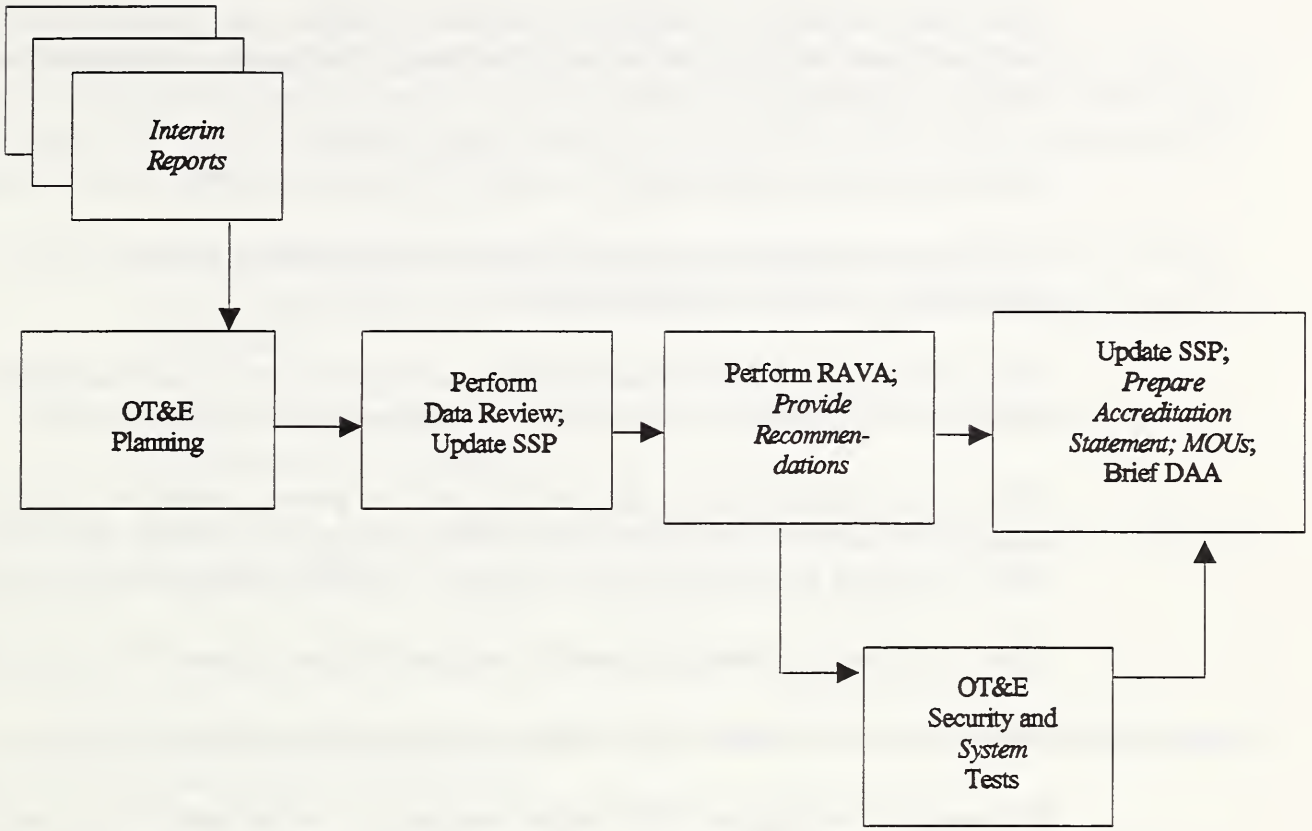


**Figure 2-5. Mountain Pass OT&E and Final C&A Process**

## 2.5 Functional Description of Mountain Pass Certification Tasks

The certification process described below is a *functional* description based on the Mountain Pass Project, specifying what must be done and a general description of how the tasks are to be accomplished. It does not present a detailed, step-by-step procedure for performing the certification tasks. Although the tasks are specific to Mountain Pass, the general approach is applicable to other system efforts.

**Planning Stage**: In the planning stage, the focus was on understanding the specific application and the certification process. The following questions provided the focus for defining the planning stage tasks. These questions were derived from FIPS PUB 102.

- What are the goals of the Mountain Pass project and EIS? Where are the major anticipated problem areas and areas of emphasis?

- What other resources are needed to complete the effort, for example, technical tools, independent contractor to perform testing (verification and validation), RAVA contractor?

- Is documentation available that describes EIS and its controls?

- What are the applicable external policies and requirements, including laws, regulations, standards, and guidelines?

- What are the applicable internal policies and requirements, quality assurance standards, test procedures, documentation standards, and audit standards?

- What are the boundaries for this certification? A general guideline is that the certification boundary includes all the relevant components of the application (EIS), including the administrative, physical, procedural, and technical features.

- What is the level of detail required in the Certification Report of Findings/SSP?

In response to the questions listed above, the following tasks addressed the C&A effort:

- Reviewed the background information necessary to understand the proposed EIS. This activity included a high-level review of the current and proposed EIS to understand the system and the issues.

- Reviewed the applicable Federal, DOJ, and DEA security policies, procedures, and regulations. DEA documents focused on implementing the DOJ and Federal regulations.

- Defined the scope of the C&A effort and developed the C&A Plan.

- Assigned C&A responsibilities and developed a schedule for completing the C&A tasks. The C&A tasks were divided among several organizations: integration contractor, RAVA contractor, ST&E contractor, systems engineer, C&A working groups, and sponsor.

- Proposed a methodology to be used for completing the certification and accreditation. FIPS PUB 102 was the primary reference document.

- Ensured that the Mountain Pass SSP followed the format specified in Office of

Management and Budget (OMB) Bulletin 90-08, *Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information.*

**Data Collection**: In data collection, the focus was on building on the base of knowledge acquired during the planning stage, for example, documenting additional security requirements identified by the users. The following questions, based on FIPS PUB 102, focused the EIS data collection effort:

- What is the functionality provided at each implementation phase of Mountain Pass. Specifically, what are the security technical capabilities implemented in each phase?

- What are the security requirements for the EIS and what is the planned implementation by phase?

- What is the system architecture for EIS and the flow of information within and external to EIS?

- What is the EIS Mountain Pass security architecture?

The goal was to provide sufficient information to guide the C&A activities. The following tasks addressed the questions listed above:

- Documented the functionality provided in each phase of the Mountain Pass effort.

- Performed the most critical tasks in the data collection stage (specified the EIS security requirements and developed the EIS security architecture).[2]

- Allowed additional security requirements to be identified by the external agency representatives in developing the MOU.

- Ensured that the security requirements were allocated to devices, as defined in the security architecture. For example, audit may be allocated to the operating system, the DBMS, and the EPIC Guard. The audit data to be collected was specified in the architecture document as were the reports that summarized the data.

---

[2] It was assumed that the security requirements would not change for Phase II and OT&E. However, they needed to be reviewed and validated at each additional phase.

- Identified the external systems that are electronically linked to EPIC. This information was required for inclusion in the MOU between EPIC and the external agency.

**Basic Evaluation.** The EIS risk analysis determined if the physical, personnel, administrative, and technical security safeguards adequately protected the Sensitive information processed on the EIS. This risk analysis considered the safeguards currently in use at the EPIC facility and those planned for the EIS. The risk analysis must include the following tasks:

The following tasks were defined for the EIS RAVA:

- Reviewed the current EPIC administrative/personnel and physical security safeguards
- Reviewed the proposed EIS security requirements
- Evaluated the security features implemented in Phase I (Do the security features satisfy the requirements and are they allocated to devices/components in the security architecture?)
- Evaluated the security features implemented in Phase II and at OT&E
- Reviewed the methodology for implementing the security features
- Determined the residual risk based on the identified threats and implemented safeguards
- Recommended changes to the RAVA process for subsequent phases
- Prepared applicable reports (e.g., Phase I interim accreditation and OT&E final accreditation)

**Detailed Evaluation**. A detailed evaluation was performed to determine whether the security features were correctly implemented and reasonably resistant to penetration. The major tasks of the EIS ST&E were the following:

- Evaluated the functionality of the security features to ensure they performed as specified in the COTS documentation. (These are commonly called *unit tests*)
- Evaluated the overall security functionality. (This task was performed during OT&E.)

- Determined the impact of the security features on the performance requirements and established a baseline set of security parameters

- Performed penetration tests to ensure the security controls were not readily circumvented or subverted. (The amount of penetration testing performed in Phase I was minimal.)

- Reviewed the proposed security administration reports (e.g., audit reports, user profile analysis) for usability

- Evaluated the security administration procedures for completeness and usefulness

## 3. SYSTEM DEVELOPMENT ROLES AND RESPONSIBILITIES

DOJ, DEA, DOD, and DISA shared the responsibility for the conduct of the Mountain Pass Project. The management approach followed was a collaborative Senior Management Team, made up of members of the four participating organizations, to provide overall direction and oversight of project activities. A PM, assisted by a Deputy and a project staff, directed the day-to-day activities of the project.

The following sections discuss the responsibilities for the roles depicted in figure 3-1. A Program Management Plan[1] was developed that fully describes the system development roles and responsibilities. This document provided the guiding principles for the project and there was little deviation from it.

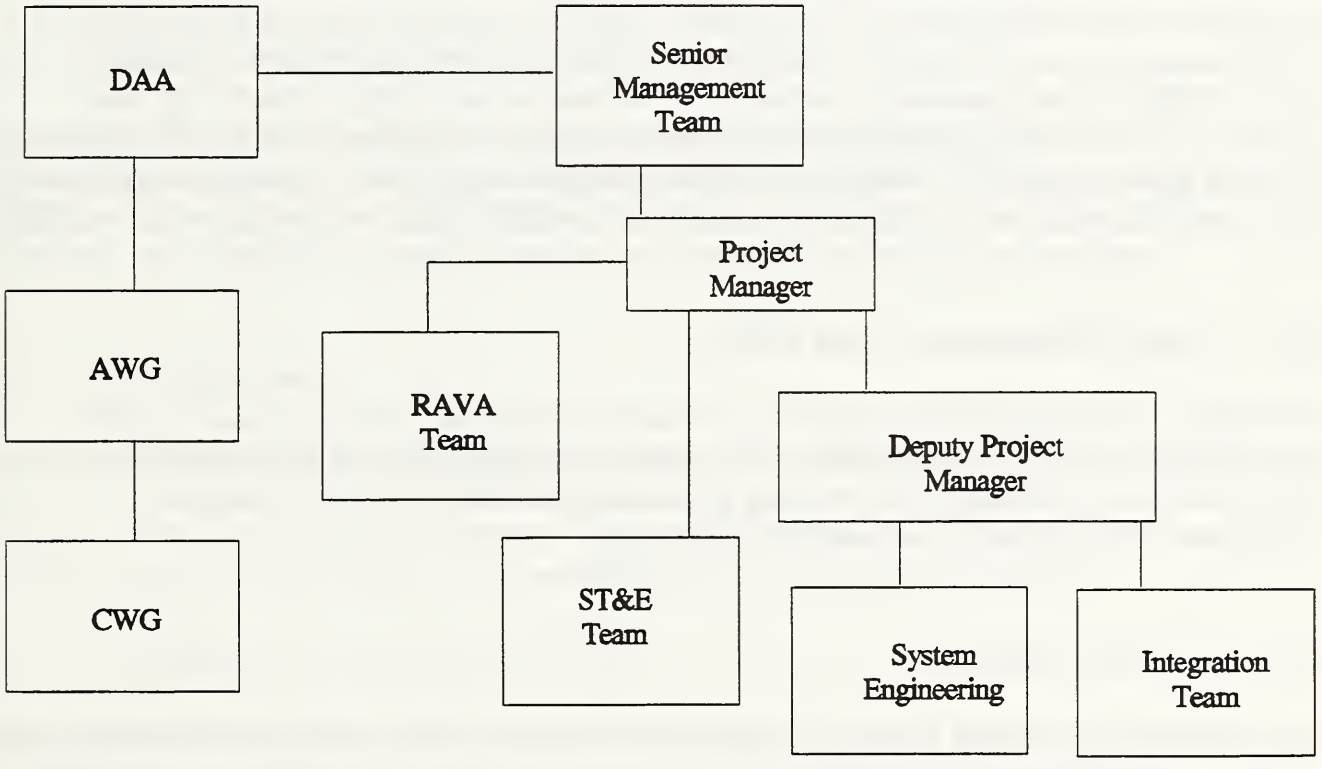


**Figure 3-1. Mountain Pass Roles and Responsibilities**

---

1 *The El Paso Intelligence Center Improvement Project Project Management Plan*, 12 February 1991.

### 3.1 Program Management

The Senior Management Team met periodically and provided oversight and both general and specific guidance to the Program Management Office (PMO). PMO personnel were provided by DISA and EPIC. The day-to-day activities of the project were directed by a PMO team consisting of a PM, his Deputy, and advisory and administrative staffs. At the working level, the project was composed of a System Engineering Team and an Integration Team. Each team was led by a government Team Chief. Finally, a Transition Team composed of EPIC personnel assisted in the transition of system management and support from the project team to EPIC at the completion of the project.

Approximately 80% of the project activity was planned to take place at EPIC. Ideally, both the PM and the Deputy and most of the project team were to reside at EPIC. Most of the technical work was expected to be performed at EPIC, with some work to be performed in the Washington area. In reality, a significant portion of the project work was completed in the Washington area because of better access to vendors and technical knowledge and expertise. The PM was originally intended to be an on-site position, but since the 80% rule was not enforced, the PM worked primarily out of Washington, D.C. to direct the efforts of the integration team and to maintain contact with the SMT. The Deputy PM resided at EPIC.

### 3.2 Senior Management Team (SMT)

The SMT was responsible for approving the improvements that would be made to EPIC, periodically reviewing the progress of the project, resolving issues raised by the PM or individual team members, and providing guidance to the PM. The SMT was the configuration management authority for the project.

### 3.3 Systems Engineering

The Systems Engineering Team was responsible for both Mountain Pass and objective system designs and their supporting analyses. The team developed and maintained an overall plan for achieving the Mountain Pass system configuration as well as the implementation plan for the objective system, performed quick-reaction engineering analyses, implemented prototypes to evaluate candidate solutions, and provided technical oversight of the integration effort.

### 3.4 Integration Contractor

The Integration Team was responsible for implementing the improvements approved by the SMT. A single integration contractor was assigned overall responsibility for the implementation effort. Specific tasks included equipment and software installation, integration, test and evaluation as well as system administration, operations and maintenance, and training. Where feasible, the integration team used prototyping to help define solutions.

### 3.5 Risk Analysis and Vulnerability Assessment (RAVA) Contractor

The RAVA contractor was responsible for evaluating the implemented security features and determining system residual risk. The RAVA contractor evaluated the selected security countermeasures to ensure they addressed the security requirements.

### 3.6 Security Test and Evaluation (ST&E) Contractor

An independent contractor, not the system integrator, performed the ST&E to ensure objectivity in executing the tests and analyzing the test results. The ST&E contractor worked closely with the system developer/integrator to understand the EIS and with the RAVA contractor to determine the security features that needed to be tested in each phase.

### 3.7 Working Groups

Because Mountain Pass was a multi-agency project, it was important to have a representative from each non-DEA agency that could participate throughout the Mountain Pass certification process. Thus, a Certification Working Group and an Accreditation Working Group were formed that provided a vehicle for representation by each participating agency.

#### 3.7.1 Certification Working Group (CWG)

The CWG was the technical advisory organization and consisted of representatives from the program management agencies and the integration and development contractors. Its responsibilities were to:

- Assist in defining the security requirements
- Assist in preparing the C&A Plan
- Provide technical recommendations and guidance

- Provide DEA technical perspective
- Coordinate activities with the AWG
- Provide the details for the SSP
- Review the reports from the RAVA and ST&E contractors
- Review the interim and final Accreditation Statement and accreditation briefings to the AWG and DAA

### 3.7.2 Accreditation Working Group (AWG)

The AWG was chaired by DEA and consisted of DEA security and AIS representatives, EPIC personnel, program management personnel, developers, and representatives from participating agencies. Some of the AWG representatives also participated in the CWG. Participation by federal agencies in the AWG was considered critical to the success of the Mountain Pass Project.

A two-step process was used to establish the AWG. First, an initial meeting was hosted by DEA and attended by representatives of all organizations who could possibly be concerned with the accreditation of the EIS. To ensure participation by these agencies, a letter was sent from the Administrator of DEA requesting agency support and a representative on the AWG. This was important because involvement by the federal agencies was not funded by DEA. (The complete letter is included as appendix B of this document.) Second, those agencies/organizations who decided to remain in the working group were expected to designate a working group member for follow-on meetings.

The AWG addressed the specifics of EIS C&A from a management perspective. Initially, this group was responsible for defining C&A requirements for Mountain Pass. Once this was accomplished, the AWG served as the review and approval authority for the certification process. The AWG met monthly and performed the following C&A activities:

- Represented the respective Federal agency in decision-making, for example, recommendation to accredit EPIC
- Provided the management perspective
- Participated in the systems engineering and C&A processes
- Provided feedback to the developers

- Made recommendations to the parent agency
- Assisted in formulating the MOU that documented the exchange of data between the external agencies and EPIC
- Reviewed the SSP and the Accreditation documentation
- Assisted in drafting the Accreditation Statement

Prior to each AWG meeting, an agenda was distributed to all representatives. If necessary, documentation was distributed to ensure the members would have time to review to material prior to the meeting. At the completion of each meeting, minutes were drafted and distributed.

### 3.7.3 Working Group Charter

A charter was used to establish the AWG and a more permanent multi-agency Security Review Committee organization at the completion of the Mountain Pass Project. The charter described the role of the organization and highlighted the responsibilities of the members. The charter included the following sections.

- Basis for Establishment
- Purpose
- Authority
- Membership
- Activities and Responsibilities
- Meetings
- Staff Support
- Sunset Provisions

A complete copy of the charter is included in appendix C of this document.

# 4. CERTIFICATION TESTING AND ACCREDITATION DOCUMENTATION

This section describes the documentation that was produced to support the accreditation decision and the Federal, agency, and DEA policies and regulations that guided the development of the security requirements and the security documentation.

## 4.1 System Security Plan

The *Computer Security Act of 1987* (Public Law 100-235) requires that all Federal computer systems that contain Sensitive information implement a plan for the security and privacy of these systems. OMB Bulletin 90-08 provides guidance for the preparation of computer security plans. The objectives of the security planning process, as described in OMB Bulletin 90-08, are to identify and assess:

- The nature and extent of Sensitive information systems and the security requirements of such systems
- The adequacy of the administrative, management, and technical approaches used in protecting Sensitive systems
- Responsibilities and accountability for the security of Sensitive systems
- Requirements for additional guidance, standards, assistance, training, and new technology to improve the protection of Sensitive information resources.

Appendix A of OMB Bulletin 90-08 was used as the fundamental outline for documenting the EIS SSP.

The EIS SSP described the security requirements essential to protecting the information processed in the EIS and outlined the C&A activities used to determine if these requirements were adequately satisfied.

The EIS SSP was developed incrementally and modified as the program progressed. It documented the security requirements, architectural decisions, technical controls implementation, and the C&A plans and schedules. The final EIS SSP was submitted as part of the accreditation package and included the following major sections.

**Specifications/Requirements**: Security requirements impacted the COTS product selection, the system architecture, and system administration. The security requirements were derived from:

- Applicable Federal, DOJ, and DEA statutes, policies, regulations, and guidelines
- Current system implementation and available technology
- User requirements
- Planned system evolution

The primary security statutes and regulations in order of precedence are: federal laws and statutes, national directives and orders, OMB circulars and bulletins, and DOJ guidelines. The complete EIS SSP reference list is included as appendix D of this document.

EIS security requirements have been described as C2+ because the minimum of C2 functionality was required for the EIS with additional functions found at higher assurance levels in the TCSEC (e.g., audit, configuration management, and security administration). Security requirements were applied to both EIS regions with administrative and operational activities performed on each region because of the separation of the two regions. Both regions operated in system high mode with all users cleared to the highest level of information on the Classified region.

The EIS security requirements were grouped under the following headings:

- EIS Security Program
- Discretionary Access Control (DAC)
- Object Reuse
- Advisory Labels
- Mandatory Access Control (MAC)
- Identification and Authentication
- Audit
- System Architecture
- System Integrity
- Trusted Facility Management
- Backup and Recovery
- Contingency Planning
- Security Testing
- Configuration Management
- Trusted Distribution
- System Security Plan
- Security Features User's Guide
- Trusted Facility Manual
- Test Documentation
- Design Documentation

- Communications Security
- Physical Security
- TEMPEST
- Personnel Security
- Certification and Accreditation
- Protection Software
- Dial-Up Lines
- Administrative Security
- System Requirements

**Security Architecture**: The EIS security architecture was partitioned, logically and physically, into two separate regions. The first region contained Sensitive information and the second contained Classified information up to the Secret level. The two regions were connected by a one-way Guard (the EPIC Guard) that permitted the one-way flow of information from the Unclassified region to the Classified region. Security architecture diagrams were used to graphically display the configuration that was to be accredited. The architecture diagrams were extremely useful for clearly identifying the external databases and message systems and illustrating the proposed configuration at EPIC. Many versions of the architecture diagrams were developed prior to system accreditation. A generalized version of the EIS Unclassified region is illustrated in figure 4-1 and a generalized version of the Classified region in figure 4-2[1].

[1] The diagrams have been generalized.

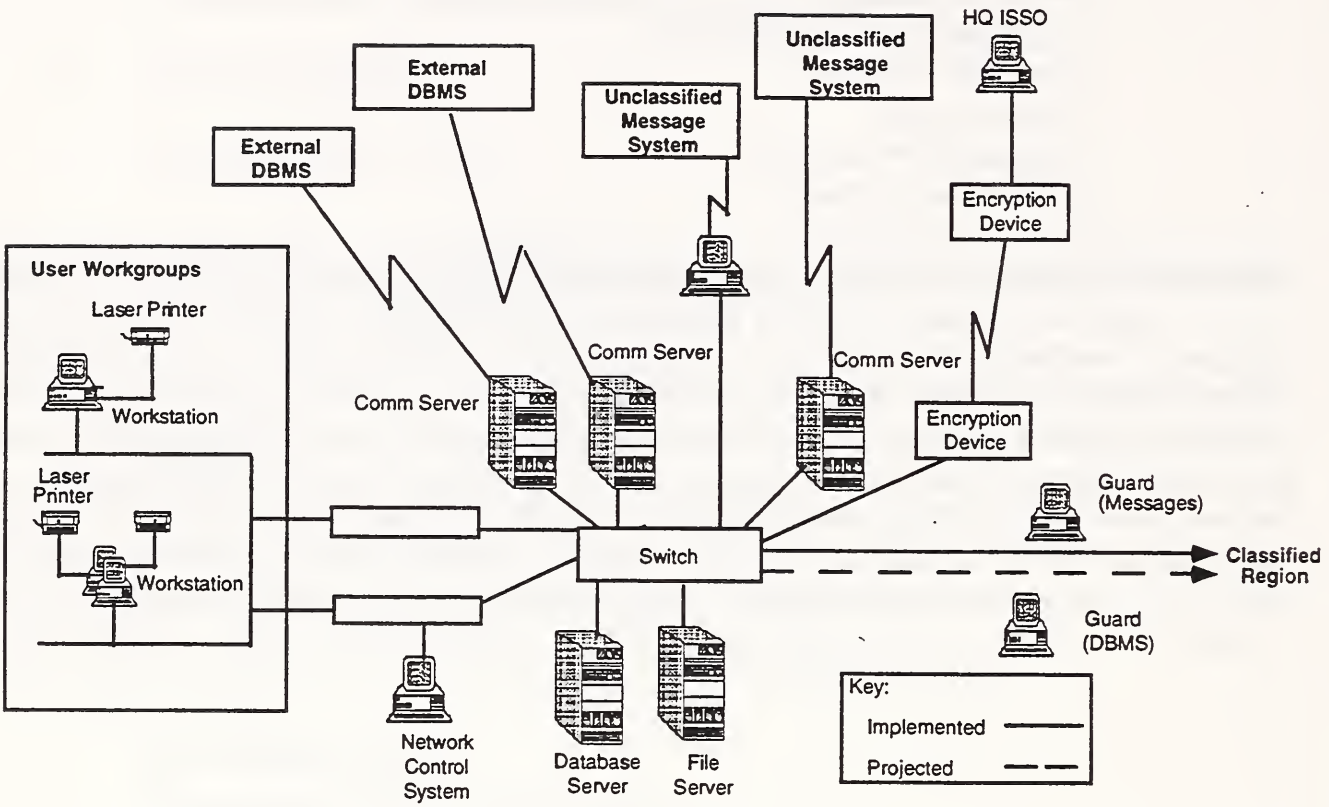


**Figure 4-1. Sample Security Architecture Diagram: EIS Unclassified Region**

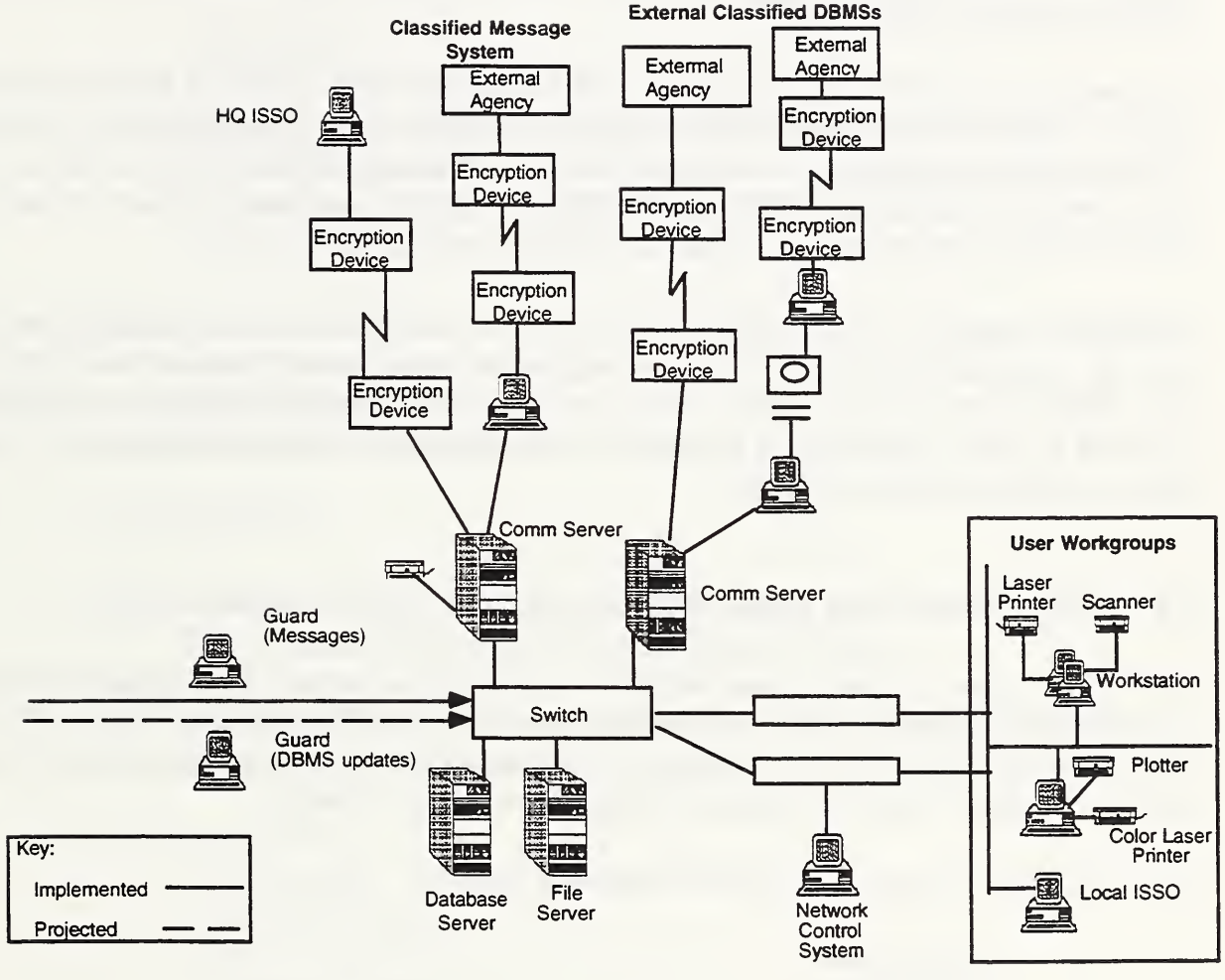


**Figure 4-2. Sample Security Architecture Diagram: EIS Classified Region**

**C&A Plan**: The EIS C&A Plan described the C&A methodology, the certification tasks, system security plan, and accreditation documentation. The C&A Plan included a detailed list of all the C&A tasks and the organization with primary responsibility for that task (e.g., RAVA contractor, CWG, AWG, ST&E contractor). A sample C&A task schedule, based on the Mountain Pass effort, is included in appendix F of this document. The C&A Plan also described the roles and responsibilities of the CWG, AWG, Integration Contractor, RAVA, ST&E contractor, and the ISSO.

Included in the C&A Plan was a generic MOU between EPIC and each linked external agency. The MOU documented the security functionality, security procedures, and disclosure of information requirements necessary to allow the exchange of data between EIS and each external system. A generic MOU is included in appendix E of this document. It was the responsibility of each external agency to tailor the generic MOU.

**Technical Controls**: The technical controls section contained a matrix that allocated the EIS security requirements to the EIS system component where the requirement was implemented (e.g., EPIC Guard, site/procedural). This section also discussed the security capabilities provided by each component as it applied to the major requirements headings (e.g., DAC, audit, system state, data integrity).

## 4.2 Risk Analysis and Vulnerability Assessment (RAVA) Report

The RAVA report for each phase included a listing of the security requirements evaluated in that phase, the evaluated risk, and the reevaluated risk (for Phase II and OT&E). The RAVA Report also described the risk analysis methodology, including the automated tools that were used, an outline of the risk analysis findings report, and a schedule.

The final RAVA report included the following sections:

- Introduction
- Methodology
  - Data Collection
  - Questionnaire Development [Identify vulnerabilities and generate scenarios]
  - Threat Assessment
  - Documentation Review
  - Questionnaire Survey
  - Code Review
  - Analysis

  - Return-on-Investment with Calculation
  - Recommendations for Management
  - Deviations from the stated methodology

- Source Documents
  - SOW
  - References
  - Policy (additional sources that were not documented or used in the EPIC SSP were DOJ Order 2600.2B *Security Programs and Inspection Response* and DOJ Order 2830.1D *Automated Information Systems Policies*)

- System Architecture
  - Components
  - Risk Index Calculation
  - Requirements Analysis

- Flaw Hypothesis

- Analysis
  - Flow Diagrams (Data, Procedures, Triggers, Fields)
  - Detailed Countermeasures (technical and non-technical), detailed test scripts, functions and process

- Recommendations
  - Administration
  - Operational Security
  - Technical Security
  - Transmission Security
  - Communications Security
  - Physical Security
  - Computer Security

## 4.3 Security Policies and Procedures

The EIS Security Policy and Procedures document (EIS SP&P) outlined the security controls implemented by EPIC to safeguard all Sensitive and Classified information assets and materials. The EIS SP&P document also established guidelines and responsibilities for the

protection of EPIC information assets. The purpose of the EIS SP&P document was to describe the security-related policies, procedures, and responsibilities for protecting Classified and Sensitive information stored, processed, or handled by the EIS.

Following is an outline of the content of the EIS SP&P:

- INTRODUCTION
  - Purpose
  - Requirements
  - Responsibilities

- SYSTEM DESCRIPTION
  - Hardware
  - System Configuration
  - Information Systems (Internal and External) Databases
  - Software
  - Operating Mode

- ENVIRONMENT
  - Facility
  - Information Security and Access
  - Authorized Personnel
  - Security Training and Awareness
  - Physical

- USER SECURITY POLICIES AND PROCEDURES
  - System Security Overview
  - User Identification and Authentication
  - Discretionary Access Control
  - Mandatory Access Control
  - Workstation Peripheral Access Control
  - Classified EIS Network Operations
  - Configuration Management
  - Backup and Recovery

- CONFIGURATION MANAGEMENT
  - CM Tasks
  - CM Plan
  - Responsibilities

- BACKUP AND RECOVERY
  - EIS Contingency of Operations Plan
  - Responsibilities

- AUDIT
  - Security Goals of the EIS Audit Mechanism
  - EIS Audit Functions
  - Administration of Audit Trail Processing
  - Audit Data Capture and Retention

## 4.4 Trusted Facility Manual (TFM)

The EPIC TFM was a companion to the existing COTS documentation, hardware documentation, and EIS documentation (primarily, the *EIS SSP* and the *EIS Users Guide*). The TFM was developed for the EIS ISSO who was responsible for administering and maintaining the security of the EIS. The TFM served as a *roadmap* for maintaining the security of the EIS.

Following is an outline of the content of the EIS TFM:

- Introduction
  - Roles and Responsibilities
  - Security Databases
- Security Considerations
  - Threats and Countermeasures
- EIS Security Features
  - ISSO Interface

## 4.5 Certification Test Documentation

System testing was performed at the completion of Phases I and II and at OT&E. Security testing was included as part of the system testing effort. Because EPIC was required to be accredited, separate security test documentation was produced at the completion of each test cycle. Following is a description of the security test plans and test reports that were produced.

### 4.5.1 Security Test and Evaluation (ST&E) Plan

The ST&E Plan described the test events and test procedures used to verify that the security safeguards implemented at EPIC were adequate to protect the Sensitive and Classified

information processed by the EIS. The ST&E Plan also described the responsibilities of the test participants. The results of the ST&E were used to support EIS accreditation.

The objectives of the test plan were to:

(1) Establish procedures for examining the utility and correctness of the EIS security controls and features

(2) Determine if the security controls and features functioned properly

(3) Ensure that the security controls were not readily circumvented or subverted

### 4.5.2 Test Report

At the completion of each security test phase, a test report was generated that documented the results of the ST&E. Following is a sample report identifying the requirements that were tested and, for security requirements not tested, the reason why. For example, a requirement may not have been tested because the implementation at the time was not complete.

**Table 4-1. Test Report Matrix**

| Test Event | Test Completed | Test Incomplete | Not Tested |
|---|---|---|---|
| 1- EIS Management Controls | | | |
| Requirement 1 | X | | |
| Requirement 2 | | X | |
| 2 - Discretionary Access Controls | | | |
| Requirement 3 | | X | |
| Requirement 4 | | | X |
| 5- Identification and Authentication | | | |
| Requirement 8 | | X | |
| Requirement 9 | | | X |

## 4.6 Accreditation Package

At the completion of Phase I, the DAA, SMT, and AWG were briefed on the status of the Mountain Pass Project. Both the SMT and the AWG assisted in developing the brief that was presented to the DAA. Included in the interim accreditation briefing were the following:

- Project Overview and Status
- What is Mountain Pass
- Project Approach
- EIS Midterm Capabilities
- Project Status
- Certification and Accreditation Process
- Review of Governing Policies/Procedures
- Documentation of the Risks
- Identification of the Countermeasures to off-set Risks
- Implemented Countermeasures
- Testing of the Countermeasures
- Identification of Residual Risks
- Roles and Responsibilities
- Management and Task Administration
- Risk Analysis and Vulnerability Assessment
- Operational and Security Test and Evaluation
- System Acceptance Testing and Documentation
- Results of Phase 1 Vulnerability Assessment
- Results of Phase 1 Testing & Evaluation
    - Items Tested
    - Test Results
- What the Results Mean
- Security Challenges
- Status and Recommendations
    - Recommendation: Interim Approval to Continue to Operate

The EIS interim Accreditation Statement included the following:

- Functionality provided to the pilot workgroups

- Certification that the security safeguards have not been degraded or compromised

- Verification that the links to the external systems had not been modified and that the data received has not been changed

- DAA acceptance of the EIS C&A process

At the completion of the Mountain Pass Project, an Accreditation Recommendation and an Accreditation Package were prepared. The final Accreditation Recommendation summarized the results of the certification process and included an accreditation recommendation. The Recommendation letter included the following:

- Introduction and Summary
- Background
- Major Findings
- Recommended Corrective Actions
- Attachment A. Proposed Accreditation (or Interim Accreditation) Statement
- Attachment B. Proposed MOU(s)

The final accreditation package included all of the security accreditation documentation produced during the Mountain Pass Project. This information provides the details and back-up to support the accreditation recommendation. The package included the following:

- System Security Plan (including the C&A Plan, security requirements, security architecture, and technical controls)

- Phases I and II RAVA and ST&E results

- RAVA report for the integrated system

- Results of the OT&E tests (including security tests)

- Final accreditation recommendation to the DAA (this is a separate section, included as a summary of all of the SSP documentation)

- MOU between EPIC and the external agencies

## 5. LESSONS LEARNED

Individuals representing all agencies participating in the EPIC project were interviewed to identify the primary lessons learned during the development and acquisition process. These lessons learned are divided into two areas: management and technical and are summarized in sections 5.1 and 5.2. Activities/processes that worked well and those that did not are included.

### 5.1 Management Lessons Learned

**Senior Management Team:** The SMT functioned as the planning and decision-making group responsible for ensuring adherence to the Mountain Pass activities. The SMT provided the appropriate level of management authority and *political clout* to make decisions and ensure that the project progressed on schedule and within budget. The SMT was an effective organization because it provided significant management oversight and made decisions when requested. For example, the SMT was very responsive to the PM's needs and requests for formal direction.

**Program Management:** The PMO was an effective manager of a multitude of simultaneous contracts and contractors, and government personnel. The PMO enthusiastically participated in and encouraged the exchange of information among the various Mountain Pass participants, worked effectively with the SMT in resolving issues and recommending solutions, and clearly communicated the delivery dates and products needed. This kept the project on schedule and within budget. Having an on-site coordinator (the Deputy PM) was extremely important because it facilitated the early identification of problems and their rapid resolution. It also provided the on-site teams with the appropriate level of authority and guidance necessary to ensure decisions were made and implemented correctly.

**Accreditation Working Group (AWG):** The AWG facilitated communications between participants and helped to raise security issues early. A great deal of informal communications between AWG members helped to get issues raised and solved in an open environment. All meetings were well documented and information was always readily available and distributed to all participants. The AWG was a key success factor because all members actively participated, were energetic and positive, and caused necessary actions to happen quickly. AWG members also provided significant technical expertise when requested, resulting in well-informed discussions and decisions at the meetings. Another critical success factor was continuity of the membership - the majority of the AWG members participated from the beginning to the end of the Mountain Pass Project and members who were replaced were provided with all the documentation to bring them up to speed.

A critical lesson learned was that it was important to keep the personnel from all the participating agencies actively involved. This active involvement helped with the agency buy-in to the selected security policies, requirements, and features.

**Certification Working Group (CWG):** This group was established to provide technical guidance and recommendations to the AWG and the contractors. However, because most of the CWG members also participated in the AWG, this group met only a couple of times. At times, the AWG meetings were lengthy because a detailed analysis of an issue with recommended alternatives was not provided. These analyses should have been developed by the CWG.

**Systems Engineering Team:** The Systems Engineering team facilitated and coordinated meetings and communications between the developers, users, and the SMT and they provided the integration contractor with valuable technical direction.

**Integration Contractor:** The integration contractor was provided a detailed system design and, therefore, was able to develop a relatively rapid COTS solution. They were responsive to the sponsor and the users in modifying the implementation to provide an acceptable user interface. One of the major lessons learned was that the implementation of the security features should have occurred much earlier in the implementation effort. This resulted in a crunch in the schedule and less time to complete the RAVA and ST&E tasks.

## 5.2 Technical Lessons Learned

**Memorandums of Understanding (MOUs):** The MOU process was the most difficult problem for the AWG members to finish. Even with extensive information sharing, it appeared that there were many distinct differences in the way law enforcement agencies protect information. There were no consistent information processing standards for law enforcement agencies. The MOUs should have been started sooner (at the beginning of the project) when all the AWG representatives were initially selected. Also, the MOU process was impacted by the requirement to have the agreements signed by the agency legal representatives. This extended the time to completion.

**Software Engineering:** The DBMS and user interface software were primarily developed at the integration contractor facility in the Washington, D.C. area. Because there was minimal interaction and communication with users at EPIC, significant changes had to be made when the implementation was demonstrated to the users. Also, it was more difficult to accommodate complex (and sometimes varying) user requirements from a distance.

**Basic and Detailed Evaluation:** ST&E was extremely effective as the detailed evaluation methodology. The ST&E team used the security requirements and the results of the RAVA tasks as the basis for developing the security and certification tests. This provided continuity and traceability. The RAVA methodology was most effective in identifying the primary security vulnerabilities and risks.

**Security-Related Issues:** It is important to define security requirements early, with a special focus on audit requirements because of storage and performance implications. The specification of security requirements will assist in the selection of COTS products. Divide security requirements into categories and assign individual responsibility for identifying and validating security requirements by category. Identify those security requirements which are mandatory (non-negotiable) versus those which can be delayed. This information may be used in the selection of the integration contractor and COTS products.

Identify roles and responsibilities of security management personnel (e.g., ISSO) to ensure that the roles are properly defined and the individuals are involved in developing the security procedures.

**Training:** Educate the users in the required security features to ensure they understand the role of security and their role in maintaining the security of the system.

## 5.3 Summary

The accreditation of a multi-agency Federal system requires the extensive involvement and coordination of many organizations, for example, agency representatives, program management staff, contractors, and users. This is critical to the success of the program. The following list summarizes what was effective for the Mountain Pass Project:

- Security was examined early in the project, prior to the selection of COTS hardware and software. Therefore, products were selected with security functionality used as one criteria of acceptability.

- The security requirements were defined at the beginning of the system life cycle and the proposed security features selected early to ensure their correct implementation. A delay in the integration of security features can result in a lengthened schedule with increased cost.

- All federal agency personnel (including DEA) were actively involved from the beginning and this helped with the agency *buy in* on the EPIC security features and technical controls.

- The representatives from the federal agencies had voting authority for their agency and, consequently, were committed to the project.

- The DAA received the accreditation recommendation *after* the AWG formal vote. The DAA was then assured that the participating federal agencies approved the EPIC security implementation.

- Security engineering (and C&A) were included as an integral part of the system development life cycle. This was critical to the timely completion of the project.

- The DAA was involved from the beginning and was frequently briefed throughout the system development cycle. This provided the DAA with many opportunities to provide input, if necessary, and to ensure that the final accreditation decision could be made in a timely manner.

As a result of the Mountain Pass effort, the development of the C&A Plan and the definition of the C&A process were viewed as a *model* for future DEA C&A efforts.

There were two areas that were not as effective and should have been done differently: the C&A planning process should have been started earlier and the inter-agency MOUs should have been developed earlier. The MOUs require extensive legal involvement and this takes significant time.

# APPENDIX A

## Table A-1. EXAMPLE: SECURITY REQUIREMENTS MATRIX

| Reqmt Number | Security Requirement | Source | System Allocation | Responsible Organization | Test Method |
|---|---|---|---|---|---|
| | Security Program | | | | |
| 1 | An AIS security program shall be implemented and maintained | Privacy Act, OMB[2] Circular A-130 | EIS | EPIC management | Inspection (I) |
| 2 | Security measures shall be implemented that are commensurate with the highest classification or sensitivity of data processed or stored by the EIS | OMB Circular A-130, DOJ Order 2640.2C | EIS | EPIC management | I |
| | Discretionary Access Control (DAC) | | | | |
| 3 | The EIS access control mechanisms shall ensure that objects are protected from unauthorized access | DOJ Order 2640.2C | Operating System, DBMS, Message Handling System, EPIC Guard | Integration Contractor, ST&E | Demonstration (D) |
| 4 | Access control shall be specified to the granularity of individual users | COMPUSEC 1/85[3], DOJ Order 2640.2C | Operating System, DBMS, Message Handling System, EPIC Guard | Integration Contractor, ST&E | D |

[2] Office of Management and Budget

[3] COMPUSEC 1/85 is the National Telecommunications and Information Systems Security (NTISS) name for DOD 5200.28-STD.

| Reqmt Number | Security Requirement | Source | System Allocation | Responsible Organization | Test Method |
|---|---|---|---|---|---|
| 5 | Access permissions shall be assigned by the EPIC ISSO | DOJ Order 2640.2C | Site | EPIC ISSO | I |
| | Object Reuse | | | | |
| 6 | User A shall not have access to information within a temporary storage object (memory object or file object) released back to EIS by user B | COMPUSEC 1/85 | Operating System, EPIC Guard, Message Handling System | Integration Contractor | Test (T) |
| | Mandatory Access Control (MAC) | | | | |
| 7 | Mandatory access controls shall be provided by the low-to-high security guard | COMPUSEC 1/85 | EPIC Guard | Integration Contractor | T |
| | Identification and Authentication (I&A) | | | | |
| 8 | The EIS shall provide for the unique I&A of all users | DOJ Order 2640.2C | Operating System, DBMS, EPIC Guard, Message Handling System | Integration Contractor | D |
| 9 | EIS user identifiers shall be assigned by EPIC | Operational Requirement | Site | EPIC ISSO | D |
| 10 | Authentication information shall be protected from unauthorized access | COMPUSEC 1/85 | Operating System | Integration Contractor | D |
| | Audit | | | | |

| Reqmt Number | Security Requirement | Source | System Allocation | Responsible Organization | Test Method |
|---|---|---|---|---|---|
| 11 | The EIS shall create and maintain an audit trail of all audited events | DOJ Order 2640.2C | Operating System, DBMS, EPIC Guard, Message Handling System | Integration Contractor | D |
| 12 | Audit data shall be permanently maintained and archived | Operational Requirement | Site | EPIC ISSO | I |
| | System Architecture | | | | |
| 13 | The security-relevant software shall execute in its own domain that protects it from external interference or tampering | COMPUSEC 1/85 | Operating System, DBMS, Message Handling System, EPIC Guard, Site | Integration Contractor | D |
| 14 | The ISSO interface to the security-relevant software shall be clearly defined (as specified in the design documentation) | Operational Requirement | Site | Integration Contractor | D |
| | Trusted Facility Management | | | | |
| 15 | The ISSO shall supervise the implementation of security procedures | Operational Requirement | Site | ST&E | I |
| 16 | The EIS shall consolidate,generate reports, and archive the audit data | Operational Requirement | DBMS, GOTS, Site | ST&E | D |
| | Security Testing | | | | |

| Reqmt Number | Security Requirement | Source | System Allocation | Responsible Organization | Test Method |
|---|---|---|---|---|---|
| 17 | Functional tests shall be performed on the EIS security mechanisms to ensure the EIS implementation maps to the EIS security requirements | COMPUSEC 1/85 | Operating System, DBMS, Message Handling System, EPIC Guard, Site | ST&E | T |
| 18 | All discovered security flaws shall be corrected and security tests re-executed (regression testing). | Operational Requirement | Site | ST&E | D, T |
| | Configuration Management (CM) | | | | |
| 19 | A CM program shall be implemented and maintained for all security-relevant software, hardware, firmware, tests, and documentation | Operational Requirement | Site | ST&E | I |
| 20 | All proposed EIS changes shall be evaluated and controlled in accordance with the EIS CM Plan | Operational Requirement | Site | ST&E | I |
| | Security Features Users Guide (SFUG) | | | | |
| 21 | The EIS SFUG shall be updated and maintained according to the EIS CM Plan | Operational Requirement | Site | ST&E | I |
| 22 | All system users shall receive training on the EIS security features and security procedures | Computer Security Act of 1987 | Site | ST&E | I |
| | Test Documentation | | | | |

| Reqmt Number | Security Requirement | Source | System Allocation | Responsible Organization | Test Method |
|---|---|---|---|---|---|
| 23 | The EIS security tests, procedures, scenarios, test results, and documentation shall be completed | Operational Requirement | Site | ST&E | I |
| | Communications Security | | | | |
| 24 | The Unclassified region's communications link between EPIC and DEA Headquarters (HQ) shall be secured for transmission of DEA-sensitive data | DOJ Order 2640.2C | KG-84, Site | RAVA, ST&E | D |
| | Physical Security | | | | |
| 25 | Access to the computer facility shall be limited to personnel assigned to the computer facility who possess Secret and DEA-sensitive clearances | DOJ Order 2640.2C | Site | RAVA,ST&E | I |
| | Personnel Security | | | | |
| 26 | All personnel with access to EPIC shall have appropriate clearances and background investigations | DOJ Order 2640.2C | Site | RAVA, ST&E | I |
| | Certification and Accreditation | | | | |
| 27 | A C&A Plan, included in the SSP, shall document the C&A process for the EIS | DOJ Order 2640.2C | Site | RAVA, ST&E | I |
| 28 | Final accreditation shall be received at the completion of OT&E | Operational Requirement | Site | DAA | I |
| | Administrative Security | | | | |

| Reqmt Number | Security Requirement | Source | System Allocation | Responsible Organization | Test Method |
|---|---|---|---|---|---|
| 29 | Device Labels: workstations and storage media (including diskettes, tapes, etc.) shall contain appropriate security classification markings/external security labels | DOJ Order 2640.2C | Site | RAVA, ST&E | I |

As illustrated in table A-1, the source for a security requirement may be a Federal law/standard or based on an operational requirement. Also, the requirement may be allocated to the complete system, to a specific component, or to the Site (for non-automated requirements).

## APPENDIX B

## CERTIFICATION AND ACCREDITATION LETTER

The purpose of this letter is to inform you of the activities I have initiated that will require your personal support.

The Drug Enforcement Administration (DEA) embarked on a project to modernize and improve the El Paso Intelligence Center's (EPIC) information processing capability. This project is called the Mountain Pass Project and involves your agency. The objective of the project is to provide the DEA/EPIC with an improved, integrated, and automated information system in 1992. The EPIC Information System (EIS) is intended to meet or exceed current information processing needs of DEA/EPIC and participating agencies, as well as provide the infrastructure from which information system requirements may be met.

It is not the intention of this project to alter or disrupt the information sharing relationships that had been established between the DEA/EPIC and the participating agencies. These relationships have served the counternarcotics efforts well and were deemed to be mutually beneficial to all DEA/EPIC participating agencies. However, we will need to properly document these information sharing relationships which developed and evolved informally over the years.

An important part of this project is the information systems certification and accreditation (C&A) process that is required by OMB Circular A-130. Certification is the technical evaluation of a system (the EIS in this case) to determine how effectively it meets information security requirements. Accreditation is the acknowledgment and acceptance of residual information security risks and the decision and authorization to operate the system in the manner for which it was intended. In order to ensure that the needed information security posture is achieved, a Certification Working Group (CWG) and an Accreditation Working Group (AWG) have been established. The CWG, for the most part, consists of technical experts who will assess risks to the EIS, analyze the vulnerabilities of the EIS, and recommend balanced actions to mitigate information security weaknesses.

The purpose of the AWG is to ensure that the information security concerns of all agencies that provide information to the DEA/EPIC are adequately addressed in the EIS. To meet this objective, the AWG is briefed monthly and from an information security standpoint, monitors the progress of the Mountain Pass Project and the results of the certification process. In addition, the AWG representatives are requested to provide input and feedback from their agencies on the topics discussed at the monthly meetings. The AWG representatives are also

asked to raise any issues that may impact on the timely accreditation of the EIS.

Before the Mountain Pass Project reaches completion, you will be requested to sign a Memorandum of Understanding (MOU) with DEA, that in a formal way describes the current informal information sharing relationship between your agency and the DEA/EPIC and defines the information security protections needed for that information. Additionally, your AWG representative will be asked to certify that the information security protections adequately protect the information sharing relationship between your agency and the DEA/EPIC. The MOU is being drafted by the AWG and will be based on others already used by several agencies.

[The federal agencies that participate in EPIC are: DOJ, FAA, Bureau of Prisons, DEA, Immigration and Naturalization Service, US Coast Guard, US Custom Service.]

## APPENDIX C

## CHARTER
## SECURITY REVIEW COMMITTEE

Section 1 - Basis for Establishment

The Committee is established by the Administrator, DEA, to fulfill the need to assure that information security requirements are maintained and enhanced throughout the continued technological enhancements of counternarcotics information systems.

Section 2 - Purpose

The purpose of the Committee is to review, recommend, monitor, and advise on major security considerations due to technology changes in information systems development. This includes evaluating the extent to which these changes will be implemented and describing the security implications of these changes. The Committee is responsible for developing a strategy to assure that security methods, techniques, plans, and procedures keep pace with the changing technology and that security continues to be an integral element in the planning and implementation of all future systems.

Section 3 - Authority

This Committee will have the authority to review, recommend, and monitor the initiatives and changes that are planned or that have occurred. The Committee members will be the voting authority representing the interests of their agency on major technological changes and reaccreditation of current systems.

Section 4 - Membership

DEA will provide the permanent Chairperson of this group. The membership shall include, but is not limited to, representatives from the following departments and agencies... The Chairperson may also, from time to time, invite visitors to provide information of interest to the Committee.

Section 5 - Activities and Responsibilities

The activities and responsibilities of the Committee shall include reviewing the methodology to identify, describe, and assess major technology changes and their impact on the security of

shared counternarcotics systems and developing a strategy to assure that security methods, techniques, plans, and procedures keep pace and that security requirements continue to be an integral part of the system development.

Section 6 - Meetings

As scheduled by the Chairperson, the Committee shall meet at least semi-annually. The Committee shall convene at the call of the Chairperson or upon request to the Chairperson by a majority of the members. Each participating department or agency shall be entitled to a single vote. An alternate for each voting member shall be designated to act in the absence of the principal. Issues before the Committee for vote shall be decided by simple majority of the voters present.

Section 7 - Staff Support

The Committee shall be supported by the members of Offices which shall provide all required policy and administrative support. The duties and responsibilities of the assigned support staff include:

- Attend and facilitate meetings
- Provide direct support to the Chairperson
- Prepare, coordinate, and disseminate meeting agendas, notices of meetings, current membership rosters, minutes, and summaries of other reports
- Maintain official records of meetings
- On behalf of the Chairperson, organize, direct, manage, and record Committee activities
- Assist the Chairperson in identifying, articulating, presenting, and developing pertinent issues and recommendations

Section 8 - Sunset Provisions

This charter shall become effective upon the signature of the Chairperson and shall remain in effect for n years from the effective date or until the Committee's purpose has been accomplished, whichever occurs first. At the end of the period, this charter shall be reviewed,

revised, and reissued, if appropriate, or this charter will be automatically terminated and the Committee disbanded.

# APPENDIX D

## POLICIES, REGULATIONS, AND STANDARDS

### Federal Policies and Regulations

- Computer Fraud and Abuse Act of 1986, Public Law 97-474
- The Computer Security Act of 1987, 40 U.S. Code 759, (Public Law 100-235), 8 January 1988
- *Electronic Communications Privacy Act of 1986*, Public Law 99-508
- *Freedom of Information Act (FOIA)*, Title 5, U.S. Code, Section 552, Public Law 89-487
- *The Privacy Act of 1974*, Title 5, U.S. Code, Section 552a, (Public Law 93-579)
- *National Security Information,* E.O. 12356, 6 April 1982
- *Telecommunications and Automated Information Systems Security Education, Training, and Awareness,* NTISS Directive No. 500, National Telecommunications and Information Systems Security, 8 June 1987
- *Management of Federal Information Resources,* OMB Circular No. A-130, OMB, 25 June 1993
- *Internal Control Systems,* OMB Circular No. A-123, OMB, 4 August 1986
- *Information Resources Management (IRM) Plans Bulletin*, OMB Bulletin 93-12, OMB, 28 April 1993
- *Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information*, OMB Bulletin No. 90-08, OMB, 9 July 1990

### DOJ Regulations

- *Telecommunications and Automated Information Systems Security*, DOJ Order 2640.2C, U. S. Department of Justice, 25 June 1993

Following is a list of other documents that were reviewed and used to develop the EPIC SSP. The documents are organized in three sections for ease of reference.

**National Instructions and Directives**


- *National Policy on Controlled Access Protection,* NTISSP No. 200, National Telecommunications and Information Systems Security, 15 July 1987

- *National Information Systems Security (INFOSEC) Glossary*, National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 4009, NSTISS, 5 June 1992

- *Glossary of Computer Security Terminology,* National Institute of Standards and Technology Interagency Report (NISTIR) 4659, National Institute of Standards and Technology, September 1991


**National Institute of Standards and Technology (NIST)**


- *Computer Security Guidelines for Implementing the Privacy Act of 1974,* FIPS PUB 41, National Institute of Standards and Technology, U. S. Department of Commerce, 30 May 1975

- *Guidelines for Security of Computer Applications,* FIPS PUB 73, NIST, U.S. Department of Commerce, 30 June 1980

- *Guidelines for ADP (Automatic Data Processing) Contingency Planning*, FIPS PUB 87, NIST, U.S. Department of Commerce, 27 March 1981

- *Guideline for Computer Security Certification and Accreditation*, FIPS PUB 102, National Institute of Standards and Technology, U. S. Department of Commerce, 27 September 1983

- *Password Usage Standard,* FIPS PUB 112, National Institute of Standards and Technology, U. S. Department of Commerce, 30 May 1985

- *Computer Viruses and Related Threats: A Management Guide,* NIST Special Publication 500-166, National Institute of Standards and Technology, U.S. Department of Commerce, August 1989


**National Computer Security Center (NCSC)**


- *A Guide to Understanding Audit in Trusted Systems,* NCSC-TG-001, Version-2, National Computer Security Center, 1 June 1988

- *A Guide to Understanding Discretionary Access Control in Trusted Systems*,

NCSC-TG-003, Version 1, National Computer Security Center, 30 September 1987

- *A Guide to Understanding Configuration Management in Trusted Systems*, NCSC-TG-006, Version-1, National Computer Security Center, 28 March 1988

- *A Guide to Understanding Design Documentation in Trusted Systems,* NCSC-TG-007, Version-1, National Computer Security Center, 2 October 1988

- *A Guide to Understanding Trusted Distribution in Trusted Systems,* NCSC-TG-008, Version-1, National Computer Security Center, 15 December 1988

- *Department of Defense Trusted Computer System Evaluation Criteria* DOD 5200.28-STD, Department of Defense, December 1985

- *Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria,* NCSC-TG-005, Version 1, National Computer Security Center, 31 July 1987

# APPENDIX E

# SAMPLE MEMORANDUM OF UNDERSTANDING

# BETWEEN

# AGENCY A

# AND

# AGENCY B

[This generic memorandum of understanding (MOU) provides an example of items that may be included in an agreement for the exchange and accessing of information by two or more federal agencies. The items are self-explanatory and this MOU is an example, only. The objective of the MOU is to identify the systems that are to be connected and the security requirements imposed on all linked systems and accessing users.]

This Memorandum of Understanding (MOU), dated (*current date*), governs the exchange of information and related cooperation between *agency A* and *agency B*. The purpose of this agreement is to allow authorized *agency A* personnel to have access to *agency B information*.

## E.1 BACKGROUND

The mission of *Agency A* is listed below:

- Provide a comprehensive and accurate intelligence picture of drug movement by land, sea, and air throughout the world as it relates to the United States (U.S.).
- Provide tactical support by the exchange of time-sensitive information dealing with drug movement.
- Support other programs of interest to *Agency A*'s participating agencies.

This MOU outlines the responsibilities and obligations of *agency A* and *agency B*.

## E.2 AGENCY A ARCHITECTURE

### E.2.1 System/Network Security Architecture

The *agency A system* security architecture is included in the body of the System Security Plan.

### E.2.2 External Agencies/Systems

Following is a list of the external agencies and systems that interconnect to the *agency A system*. The information is listed in alphabetical order, by agency.

- Agency B
  - System 1

- System 2

- Agency C
  - System 1
- etc.

### E.2.3 Future External Links

Following is a list of the external systems that are currently "air-gapped" at *agency A*. Electronic links may be established in the future.

- Agency B
  - System 3

### E.2.4 *Agency A System* Security Services

- Audit:

  - Initial login to a device/database. Records successful and failed attempts.

  - Logout from the workstation.

  - Attempts to access objects (e.g., DBMS tables, system files) based on a need-to-know basis.

The following data will be recorded for each audited event: user identifier, date/time, workstation ID, external database queried (if applicable), and type of query.

- Discretionary access control (DAC):

  - Access into the *agency A database* determined by: security clearance, need-to-know, work assignment (role), agency.

  - *Agency A system* roles are: database administrator, and ISSOs, and user.

- Security administration:
    - Security incident reporting procedures and list of actions that constitute a security incident/violation.
    - Configuration management program for controlling changes and tracking system elements (e.g., hardware devices, software, documentation, firmware).
    - System contingency plan.
- Identification and authentication (I&A):
    - Unique identifier and password combination for each user and user role (database administrator, operator, security administrator, inquiring user).
    - User account lockout after a preset number of unsuccessful access attempts.
    - Workstation time-out after a specified time period with no activity.
    - Maintenance procedures.
- Physical security:
    - Physical protection against natural disasters, internal, and external attacks.
- Personnel security:
    - Required user clearances.

## E.3 GENERAL PROVISIONS

### E.3.1 Limitations on Use and Disclosure of Information

No information which is transferred by either party to the other pursuant to the terms of this MOU may be used or disclosed by the party to whom such information is transferred except

in accordance with applicable provisions set out in this MOU and in the attached addendum(s).

No information which is transferred by either party to the other pursuant to the terms of this MOU may be used or disclosed by the party to whom such information is transferred except in accordance with applicable provisions of the *Privacy Act of 1974*, Title 5, U.S. Code, Section 552a (the "Privacy Act"), and other Federal laws, regulations, or policies applicable to the sources, use, disclosure, or dissemination of such information (collectively, to encompass both the Privacy Act and such other laws, regulations, or policies, "Privacy Law"), as in effect from time to time, including, without limitation, any applicable rules relating to information provided by either agency to the other that contains identifiable records from a third agency of the Federal Government.

### E.3.2 Retention of Records

*Agency A* and *Agency B* recognize the need to maintain a strict system of control with respect to access of shared information. *Agency A* and *Agency B* also agree to cooperate as necessary to verify that the restrictions imposed on use or disclosure by *Agency A* or *Agency B* of information obtained under this MOU have been observed by the relevant agency and its employees.

#### E.3.2.1 AGENCY A SYSTEM

##### E.3.2.1.1 Access by *Agency B Personnel* to the *Agency A System*

Authorized *Agency B* personnel, as defined in the Addendum to this Memorandum, and other personnel employed by or assigned to the *Agency A facility*, shall have access to the *Agency A system*, and related information for official purposes, in the manner, to the extent, and subject to the terms and limitations, provided in such Addendum.

##### E.3.2.1.2 Provision of Information and Assistance by *Agency B* to *Agency A*

*Agency B* will provide information for authorized law enforcement and related purposes to duly authorized employees, and will assist such employees in the investigation and analysis of narcotics-related information. The manner, extent, and the terms and limitations of *Agency B* assistance to *Agency A* will be agreed upon between *Agency B* and *Agency A* by Memorandum, an addendum to this Memorandum, or otherwise.

#### E.3.2.1.3 Limitations on Use and Disclosure of Information

All authorized *Agency B* personnel will take any steps requested by *Agency A*, to protect Classified and Sensitive information received from *Agency A*, and will observe other *Agency A* policies and procedures, relating to the dissemination of Sensitive information, that *Agency B* is reasonably requested to observe in connection with permission to disseminate information in particular cases.

#### E.3.2.1.4 Compliance with Privacy Law

*Agency A* represents and warrants that it is permitted by Privacy Law in force on the date hereof to permit authorized *Agency B* personnel to have access to the *Agency A system* on the terms provided in this Addendum to this Memorandum, and that Privacy Law in effect on the date hereof imposes no limitations, other than those specified in the attached Addendum, on *Agency B*'s ability to use or disclose information obtained from the *Agency A system* by *Agency B* hereunder.

#### E.3.2.1.5 Retention of Records

Information in the *Agency A system* will be deemed to constitute a record of *Agency A*, and *Agency A* will be deemed to have retained control of the information in the *Agency A system* for all purposes, including, but not limited to, the application of the provisions of the *Freedom of Information Act*, Title 5, U.S. Code, Section 552, and the *Privacy Act of 1974*, to information obtained from the *Agency A system* by *Agency B*.

### E.3.2.2 External System

#### E.3.2.2.1 Access to *Agency B System*

(To be completed by the external agency.)

#### E.3.2.2.2 Provision of Information and Assistance by *Agency B* to *Agency A*

*Agency B* personnel will provide information for authorized law enforcement and related purposes to duly authorized employees, and will assist such employees in the investigation and analysis of narcotics-related information. The manner, extent, and the terms and limitations of *Agency B* assistance to *Agency A* will be agreed upon between *Agency B* and *Agency A* by Memorandum, an addendum to this Memorandum, or otherwise.

#### E.3.2.2.3 Limitations on Use and Disclosure of Information

All authorized *Agency A* personnel will take any steps requested by *Agency B*, to protect Classified and Sensitive information received from *Agency B*, and will observe other *Agency B* policies and procedures, relating to the dissemination of Sensitive information, that *Agency A* is reasonably requested to observe in connection with permission to disseminate information in particular cases.

#### E.3.2.2.4 Compliance with Privacy Law

(To be completed by the external agency.)

#### E.3.2.2.5 Agency Contact Points

The individuals responsible for the implementation of this MOU and the resolution of issues hereunder shall be:

*Agency A*:

a. General implementation:
   name/position
   agency/office
   address

b. Case specific issues or project requests:
   name/position
   agency/office
   address

c. Administrative matters:
   name/position
   agency/office
   address

*Agency B*:

a. General implementation:
   name/position
   agency/office
   address

b. Case specific issues or project requests:
name/position
agency/office
address

c. Administrative matters:
name/position
agency/office
address

Any notice required to be provided by either agency to the other shall be deemed provided when delivered (or deposited in the United States mail with first class postage, return receipt requested) to the responsible individual designated above, with copies to the following:

*Agency A*:
name/position
agency/office
address

*Agency B*:
name/position
agency/office
address

### E.3.2.3 Spirit of Cooperation

*Agency A* and *Agency B* recognize that the effective use of multi-source law enforcement systems requires cooperation between agencies of the Federal Government and agree to use their best efforts to implement the letter and spirit of this MOU.

### E.3.2.4 Amendment/Termination

This document and any addenda thereto are intended to be a memorandum of understanding and cooperation between the parties. The provisions in this memorandum may be amended by the agreement of both parties or the agreement may be rescinded in its entirely by either party. *Agency A* may revoke this agreement without advance notice if there is determined to be a breach of systems integrity or security, or failure of *Agency B* to comply with established procedures. Any amendment or recision of the agreement by either or both parties to the

agreement must be made by written notice to the other party.

This MOU shall become effective from the date it is executed by representatives of the parties and may be terminated by either party upon 60 days' written notice to the other.

### E.3.2.5 Government Law

This MOU shall be executed and governed in accordance with applicable regulations and Executive Orders, and in accordance with agency procedures consistent herewith.

**ADDENDUM TO MEMORANDUM OF UNDERSTANDING BETWEEN *AGENCY A* AND *AGENCY B***

This Addendum to the MOU between *Agency B* and *Agency A*, dated *(current date)*, states the terms on which employees of, or assigned to *Agency A* shall have electronic access to the *Agency A system.*

1. Definitions.

The following terms shall have the following meanings. Terms used but not defined in the Addendum shall have the meaning assigned to such term in the MOU if the term is defined in the MOU. Any term or expression not defined in the MOU shall have the meaning it traditionally possesses.

a. "Authorized *Agency A* Personnel": All *Agency A* personnel, including those detailed from other Federal agencies, who are authorized electronic access to the *Agency A* system.

b. "Authorized Third Party": A person authorized by *Agency B* and *Agency A* and by the laws relating to such person, to receive information from the *Agency A system.*

2. Description.

- General description of the system, to include the type of data processed.
- *Agency B system* is accredited to process information at the following security levels:
- Classification level of the most Sensitive data to be transmitted to *Agency A system.*
- Clearance of lowest cleared user to access the *Agency B system.*
- Security mode of operation
- Resolution DAA. (The organization that will be responsible for coordinating the opinions of multiple DAAs and will resolve differences.)

3. Access to System.

*Agency A* agrees to restrict access to the *Agency B* information to only those individuals who have a legitimate need to see or review the information for the official purpose(s) for which access has been granted.

*Agency B* understands that *Agency A* cannot assure that the *Agency A system* data is always current, accurate, or complete. *Agency A* assumes full responsibility for adequate verification and interpretation of the accuracy of the data obtained and to be used.

a. *Electronic Access.*

Authorized *Agency A* personnel shall have on-line electronic access to the information contained in the *Agency B system* by means of an electronic link between the *Agency A system* and the *Agency B system.*

*Communication Lines*: Dedicated, point-to-point[4] communications lines from *Agency A* to *Agency B* have been installed and are operational.

b. *Scope of Electronic Access.*

Authorized *Agency A* personnel shall have access to *Agency B* as described below:

*Agency B* personnel will provide information for authorized law enforcement and related purposes to duly authorized employees of *Agency A*, and will assist such employees in the investigation and analysis of narcotics-related data. The manner, extent, and the terms and limitations of *Agency B*'s assistance to *Agency A* will be agreed upon between *Agency A* and *Agency B* by Memorandum, an addendum to this Memorandum, or otherwise.

c. *Authorized Agency A personnel; security clearances.*

(To be specified by *Agency A.*)

d. *Identifiers and Passwords.*

*Agency A* will issue an identifier and password to each individual. These identifiers are

---

[4] Type of communications link specified for each external agency.

unique to that individual and may not be transferred or shared. *Agency A* reserves the right to periodically change identifiers and passwords.

*Agency B* will furnish *Agency A* with system access passwords. *Agency A* will ensure security of passwords to restrict their use only to authorized persons in accordance with established *Agency B* procedures.

e. *Training.*

*Agency A* will provide training to all authorized *Agency A* personnel.

f. *Security Administration procedures.*

(To be completed by *Agency B.*)

3. *Agency A* Use of *Agency B* Information.

(To be completed by *Agency B.*)

4. Disclosure of Information.

a. *General Limitations; Privacy Act.*

Information obtained from *Agency B* or otherwise by *Agency A* authorized personnel may be disclosed subject to the further limitations provided below, to any other Government agency permitted to receive information from *Agency A* (including any Federal, state, or local) organization involved in law enforcement or regulatory activities): (1) to whom *Agency A* could disseminate such information under the "routine use", "law enforcement", "personal health or safety", or "court order exceptions", 5 U.S.C. Sections 552a(b)(3), (b)(7), (b)(8), or (b)(11) respectively, of the Privacy Act or (ii) as not inconsistent with the Third Agency Rule, which provides that information contained in a report or record furnished to *Agency A* by another agency shall not be disclosed or distributed to a third agency without the prior consent of the originating agency.

b. *Prior Approval.*

*Agency A* must obtain the approval of *Agency B* prior to disclosing to any Authorized Third Party information derived from the *Agency B system*, including, but not limited to, the fact that a case exists, the name of an individual within *Agency A,* who may be contacted by such

party to obtain additional information about such case, or any additional information about such case.

*Agency A* and *Agency B* shall work together to establish procedures for processing *Agency A*'s requests for dissemination.

c. *Record of Inquiries, Accounting, etc.*

(To be completed by *Agency B*.)

## APPENDIX F

## EPIC C&A TASKS AND SCHEDULE

The following schedule provides a list of tasks, primary organization responsible for completing the task, and a schedule of activities. The schedule is based on the tasks being completed in approximately 12 months. One objective in developing this schedule was to sequence the tasks and determine the order for completing the tasks.

**Table F-1. C&A TASKS**

| Task | Primary Responsibility | Due Date |
|---|---|---|
| C&A planning | CWG | ongoing |
| Data review and collection | CWG | ongoing |
| Basic evaluation/risk analysis: | CWG | |
| - Select risk analysis methodology | RAVA contractor | |
| - Perform Phase I risk analysis: | RAVA contractor | month 3, days 1-8 |
| - Phase I risk analysis "outbrief" at EPIC | RAVA contractor | month 3, day 9 |
| - Phase I draft report | RAVA contractor | month 3, day 26 |
| - Comments to integration contractor on draft report | CWG | month 4, day 6 |
| - Revised risk analysis report | RAVA contractor | month 4, day 8 |
| - Briefing to CWG | RAVA contractor | month 4, day 10 |
| - Risk analysis DAA/AWG briefing working session | RAVA contractor, CWG | month 4, day 27 |

| Task | Primary Responsibility | Due Date |
|---|---|---|
| - Phase I AWG risk analysis briefing | RAVA contractor | month 4, day 30 |
| - Perform Phase I Interim Accreditation: | | |
| - Draft interim Accreditation Statement | CWG, AWG | month 4, day 27 |
| - Brief Interim Accreditation Statement | CWG, AWG, DAA | month 5, day 3 |
| - Perform Phase II risk analysis: | RAVA contractor | month 6, day 30 - month 7, day 24 |
| - Phase II risk analysis "outbrief" at EPIC | RAVA contractor | month 7, day 24 |
| - Phase II draft report | RAVA contractor, CWG | month 8, day 8 |
| - Comments to integration contractor on draft report | CWG | month 8, day 13 |
| - Revised risk analysis report | RAVA contractor | month 8, day 18 |
| - Briefing to CWG | RAVA contractor | month 8, day 21 |
| - Phase II DAA risk analysis briefing working session | RAVA contractor | month 9, day 10 |
| - Phase II DAA/AWG risk analysis interim update briefing | RAVA contractor | month 9, day 17 |
| - Perform full operational capability (FOC) risk analysis: | RAVA contractor | month 9, day 24 - month 10, day 8 |
| - FOC risk analysis "outbrief" at EPIC | RAVA contractor | month 10, day 8 |
| - FOC risk analysis draft report | RAVA contractor | month 10, day 29 |

| Task | Primary Responsibility | Due Date |
|---|---|---|
| - Briefing to CWG | RAVA contractor | month 11, day 3 |
| - Comments to integration contractor on draft report | CWG | month 11, day 5 |
| - Update FOC risk analysis per ST&E results | RAVA contractor | month 12, days 2-8 |
| - Draft FOC risk analysis results/report | RAVA contractor | month 12, day 9 |
| - Comments on draft FOC risk analysis report | CWG | month 12, day 15 |
| - FOC DAA/AWG risk analysis briefing working session | RAVA contractor | month 12, day 21 |
| - FOC AWG risk analysis briefing | RAVA contractor | month 12, day 24 |
| - Final Mountain Pass risk analysis report | RAVA contractor | month 12, day 30 |
| - FOC DAA risk analysis briefing | RAVA contractor | month 12, day 30 |
| Phase I ST&E: | | |
| - Develop test plan | ST&E contractor, CWG, EPIC | month 4, day 8 |
| - Develop test scenarios | CWG, EPIC, ST&E contractor | month 4, day 8 |
| - Develop test procedures | Integration contractor, CWG, ST&E contractor | month 4, day 8 |
| - Provide test plan comments to ST&E contractor | CWG | month 4, day 10 |
| - Execute tests | ST&E contractor, Integration contractor | month 4, days 13-19 |

| Task | Primary Responsibility | Due Date |
|---|---|---|
| - Conduct test results "outbrief" at EPIC | ST&E contractor | month 4, day 17 |
| - Conduct test results DAA briefing working session | ST&E contractor, CWG | month 4, day 27 |
| - Develop test report | ST&E contractor | month 5, day 5 |
| - Provide test report comments to ST&E contractor | CWG | month 5, day 10 |
| - Prepare Phase I final ST&E report | ST&E contractor | month 5, day 12 |
| Phase II ST&E: | | |
| - Develop test plan | ST&E contractor, CWG, EPIC | month 8, day 6 |
| - Develop test scenarios | EPIC, ST&E contractor | month 8, day 6 |
| - Develop test procedures | EPIC, ST&E contractor | month 8, day 6 |
| - Provide test plan comments to ST&E contractor | CWG | month 8, day 11 |
| - Execute tests | ST&E contractor, Integration contractor | month 8, days 18-29 |
| - Conduct test results "outbrief" at EPIC | ST&E contractor | month 8, day 29 |
| - Conduct test results interim update briefing working session | ST&E contractor, CWG | month 9, day 5 |
| - Conduct test results interim update briefing to DAA/AWG | ST&E contractor, CWG | month 9, day 17 |
| - Develop test report | ST&E contractor | month 9, day 19 |
| - Provide test report comments to ST&E contractor | CWG | month 9, day 24 |

| Task | Primary Responsibility | Due Date |
|---|---|---|
| - Prepare Phase II final ST&E report | ST&E contractor | month 9, day 29 |
| OT&E (Security and Acceptance): | | |
| - Develop OT&E test planning | ST&E contractor, CWG, EPIC | month 5, day 3 - month 7, day 2 |
| - Develop OT&E draft test plan | EPIC, ST&E contractor | month 7, day 2 |
| - Provide OT&E test plan comments to ST&E contractor | EPIC, CWG | month 7, day 8 |
| - Develop OT&E final test plan | ST&E contractor | month 9, day 18- month 10, day 3 |
| - Execute OT&E tests | ST&E contractor, Integration contractor | month 10, day 27- month 11, day 21 |
| - Conduct OT&E test results "outbrief" at EPIC | ST&E contractor | month 11, day 21 |
| - Prepare draft OT&E test results report | ST&E contractor | month 12, day 4 |
| - Provide comments to ST&E contractor on draft test results report | CWG, EPIC | month 12, day 10 |
| - Develop OT&E security test plan | ST&E contractor | month 10, days 8-29 |
| - Provide OT&E security test plan comments to ST&E contractor | CWG | month 11, day 4 |
| - Develop OT&E final security test plan | ST&E contractor | month 11, day 7 |
| - Execute OT&E security tests | ST&E contractor | month 11, days 10-21 |

| Task | Primary Responsibility | Due Date |
|---|---|---|
| - Conduct OT&E security test results "outbrief" at EPIC | ST&E contractor | month 11, day 21 |
| - Prepare draft OT&E security tests report | ST&E contractor | month 12, day 9 |
| - Provide comments to ST&E contractor on draft report | CWG, EPIC | month 12, day 14 |
| - Brief AWG on final OT&E test report | ST&E contractor | month 12, day 24 |
| - Prepare final OT&E test report (including security tests) | ST&E contractor | month 12, day 30 |
| - Brief DAA on test results | ST&E contractor | month 12, day 30 |
| Certification Report of Findings: | | |
| - Develop report outline | CWG | month 8, day 11 |
| - Prepare certification report | CWG, ST&E contractor, Integration contractor | month 12, day 30 |
| Final Accreditation: | DAA | |
| - Develop draft MOUs | AWG | month 1, day 25-month 5, day 19 |
| - Review and revise MOUs | AWG | month 5, day 26-month 8, day 13 |
| - Finalize MOUs | AWG | month 8, day 27-month 11, day 12 |
| - Coordinate MOUs between DEA and external agencies | AWG | month 11, day 19-month 12, day 24 |
| - Develop Accreditation Statement | AWG, CWG | month 12, day 28 |
| - Brief Accreditation | AWG, CWG | month 12, day 30 |

# APPENDIX G

# GLOSSARY

| | |
|---|---|
| ADP | Automated Data Processing |
| AIS | Automated Information System |
| AWG | Accreditation Working Group |
| C&A | Certification and Accreditation |
| CM | Configuration Management |
| COTS | Commercial-off-the-Shelf |
| CWG | Certification Working Group |
| D | demonstrate |
| DAA | Designated Approving Authority |
| DAC | Discretionary Access Control |
| DBMS | database management system |
| DEA | Drug Enforcement Administration |
| DISA | Defense Information Systems Agency |
| DOD | Department of Defense |
| DOJ | Department of Justice |
| EID | El Paso Intelligence Center Internal Database |
| EIS | El Paso Intelligence Center Information System |
| EIS SP&P | El Paso Intelligence Center Security Policies and Procedures |
| E.O.s | Executive Orders |
| EPIC | El Paso Intelligence Center |
| FOC | full operational capability |
| FOIA | Freedom of Information Act |
| GOTS | Government-Off-the-Shelf |
| HQ | Headquarters |
| I | inspection |
| I&A | Identification and Authentication |
| INFOSEC | Information security |

| | |
|---|---|
| IRM | Information Resources Management |
| ISSO | Information Systems Security Officer |
| LANs | Local Area Networks |
| LEAs | Law Enforcement Agencies |
| MAC | Mandatory Access Control |
| MOU | Memorandum of Understanding |
| NCSC | National Computer Security Center |
| NIST | National Institute of Standards and Technology |
| NISTIR | National Institute of Standards and Technology Interagency Report |
| NTISSP | National Telecommunications and Information System Security Policy |
| NSTISSI | National Security and Telecommunications Information System Security Instruction |
| NTISS | National Telecommunications and Information Security |
| OMB | Office of Management and Budget |
| OT&E | Operational Test and Evaluation |
| PM | Project Manager |
| PMO | Program Management Office |
| RAVA | Risk Analysis and Vulnerability Assessment |
| SMT | Senior Management Team |
| SFUG | Security Features User's Guide |
| SP&P | Security Policies and Procedures |
| SSP | System Security Plan |
| ST&E | Security Test and Evaluation |
| T | Test |
| TCSEC | Trusted Computer System Evaluation Criteria |
| TFM | Trusted Facility Manual |
| TG | Technical Guidance |
| UID | Unique Identification |
| U.S. | United States |