Mandatory Reference: 545, 552
File Name: 545mae_062701_cd24
Last Revised: 06/27/2001

INFORMATION SYSTEM CERTIFICATION AND **ACCREDITATION PROCESS,** APPROVAL TO OPERATE

*Consistent with ADS 545 and 552, with **Government Information Security Reform (GISR) legislation,** and with Office of Management and Budget **(OMB) guidance in memoranda and in OMB Circular A-130**, USAID information systems that process or store **sensitive information**, **or classified national security information** are required to be certified prior to processing or storing such information. In response to these requirements, the Information Systems Security Officer (ISSO) for USAID provides the following mandatory guidance for USAID's information system certification and accreditation **(C&A)** process and approval to operate procedures for all systems used to process sensitive and classified national security information.

***Completion of the C&A process for major applications and general support systems (followed by formal approval to operate a major application or support system) is a key component in executing USAID's Agency-wide security program and in implementing security plan(s).**

*Since the C&A process provides the necessary framework for the information management activities needed to develop, build, test, and implement USAID's Enterprise Architecture (EA), C&A actions must be part of the acquisition/life cycle for information systems (IS). The four phases of the C&A process – ***Definition*****,** ***Verification*****,** ***Validation*****,** and ***Post Accreditation*** **-** are shown in Figure 1, C&A and the IS ACQUISITION/LIFE CYCLE, at the end of this internal mandatory reference.

Overview of the C&A Process

1.** To begin the C&A process, program and systems managers must ***define their business needs and requirements. Responsibilities will have to be assigned to the appropriate individual(s), and organizations will need to negotiate methods for implementing security requirements among identified stakeholders.

> ***a**. Primary references for **Phase I, *Definition***, can include a major application or system Concept of Operations (CONOPS), identified security requirements, a test/evaluation plan, and a contingency plan. A security plan is always required. Major application or system security plan templates and formats can be found online on the USAID information systems security intranet web site {at http://inside.usaid.gov/M/IRM/ipa/iss/index.htm }. Templates and formats are available from M/IRM/IPA as well.

***b.** Organizations must prepare appropriate materials and identify essential activities in order to get a major application or system **ready for certification.** Based on the research conducted in **Phase I**, a System Security Authorization Agreement (SSAA) containing the essential initial documentation is prepared. The SSAA is a living document (kept in a binder) that records all security requirements and the stakeholders' agreement(s) on the planned performance of the C&A process. In some cases, separate technical documents will be produced; in other, less complex applications or systems, technical requirements can be covered in sections of an over-arching security plan document. In all cases, the SSAA will evolve and change as the C&A process continues.

***2.** The initial step in **Phase II, *Verification*,** is a review of the initial documentation (ideally completed and assembled into the SSAA binder during Phase I). These materials in the SSAA binder often will include

- *An **SSAA memorandum**, signed by the stakeholders, documenting Phase I agreements (this memorandum may need to be revised in succeeding Phases);
- *****A **security plan**, which will usually include
  - **Security requirements documentation** (if not broken out separately);
  - **Contingency planning** information for the system being assessed (if not broken out separately); and
  - An overview of the **concept of operations (CONOPS)** to be followed during the process (if not broken out separately).
- *****A **C&A plan;**
- *****A **system security test and evaluation plan (ST&EP), with security certification test procedures;**
- ***A security test report (STR),** which combines the findings of **the risk assessment (or analysis) vulnerability testing,** and **ST&EP testing;**
- ***Risk/vulnerability assessment documentation;** and
- *****(If needed) **security certification and accreditation statements,** addressing **internal and external connections** affecting the application or system**.**

*Organizations must update Phase I materials, and perform tailored assessment activities, as part of their **Phase II *certification analysis*,** in order to get their major application or system **ready for certification.**

*3. **Phase III, *Validation*,** is the culmination of the C&A process. At this point

- *The findings of the vulnerability testing and the certification testing are analyzed and **a certification statement is issued by the certification authority (CA)**; and

- *The completed SSAA binder (or certification package) **is forwarded to the designated security accreditation authority (DSAA**). If the DSAA agrees, **he or she issues a written accreditation statement**.

*The **SSAA binder** then **becomes the "accreditation package"** and the **accreditation statement is placed inside the SSAA binder.** These materials justify the **"authorization to operate**." The SSAA materials provide the data and documentation needed to **validate the system or major application**, and **to support the security certification statement,** which will be **executed by the certifying authority (CA).** Certification Authorities, which include Mission Directors at USAID Missions**, certify IS that support operations conducted in their organizations.**

*Organizations develop materials to support the accreditation statement,** which will be **executed by the Designated Security Accreditation Authority (DSAA) in the C&A process.** The CIO serves as the Designated Security Accreditation Authority (DSAA) for most of USAID's Information Systems (IS), including IS at USAID Missions. The Director, Office of Financial Management (M/FM), USAID's Chief Financial Officer (CFO), serves as the DSAA for financial IS in USAID/Washington.

*4. In **Phase IV, *Post Accreditation*,** once a major application or system is formally accredited, further operations must be monitored to ensure that all SSAA documents and certification standards are maintained.

> *a. **Major changes** in software and/or hardware (to include additional connections to other networks or systems) **will require** program **managers to begin the C&A process again, to re-certify and re-accredit** their major application or system.
>
> *b. More specific C&A procedures will be contained in a **USAID Certification and Accreditation Procedures (USAIDCAP) Handbook**, to be prepared by the USAID ISSO. See also the National Information Assurance Certification and Accreditation Process (**NIACAP**, National Security Telecommunications and Information Systems Security Instruction {NSTISSI} No. 1000). Additional information on some of the processes outlined above follow.

5. Certification is **an evaluation process assessing** non-technical and technical **security management, operations, and technical controls, policy, and requirements. Together with** a **risk analysis** and a **vulnerability assessment, certification produces documents** that **support** management **decisions** (with respect to particular IT asset(s), design(s) or implementation) **that meet** a pre-specified set of

security requirements. Certification is based on both Federal law and regulatory guidance, and USAID security policy promulgated in USAID ADS chapters 561, 545, and 552. Certification has two component elements:

- A security requirements and vulnerability analysis; and

- A facility security plan.

Both elements must be completed by cleared U.S. citizen personnel, within the requesting Bureau, Office, or Mission, working under the supervision of a senior supervisory authority. Upon completion, the requirements analysis and facility security plan are to be forwarded to the ISSO for USAID for action within M/IRM.

a. Requirements Analysis

A requirements analysis identifies the need to process Sensitive But Unclassified (SBU) or classified national security information. The format of the requirements analysis is at the discretion of the requesting entity; however, it must

1. Justify the need for processing SBU or classified information;

2. Identify the types of information or data that require processing (e.g., cables, reports, spreadsheets, etc.);

3. Identify the highest classification level of information that needs to be processed (i.e., SBU, CONFIDENTIAL, or SECRET);

4. Locate, on a facility blueprint-type drawing, the location of all system components, workstations, printers, and other peripheral devices. If certification to process national security information is being requested, measure all distances between each IT system component (e.g., workstations, printers, and peripherals) and all communication devices (e.g., facsimile machines, modems, telephones, etc.), public access areas, and non-U.S. Government-controlled space;

5. Provide the name, office symbol, business address, and office telephone number of the individual formally designated as the site Information Systems Security Officer (ISSO) responsible for the system;

6. Identify the location of the nearest U.S. Government facility that processes classified national security information (e.g., U.S. Embassy, U.S. Consulate, Department of Defense installation, or neighboring USAID entity); and

*7. **Provide a diagram/topology of the system.**

b. Facility Security Plan

A facility security plan contains specific security procedures for safeguarding a system and the data it processes. The format of the facility security plan is at the discretion of the requesting entity. However, it must include

1. A configuration drawing of **the system,** all system components, workstations, printers, modems, and other peripheral devices;

2. A description of the door locks used to control physical access to the system and its components, workstations, printers, modems, and other peripheral devices;

3. An identification, by type and location, of the security containers used to safeguard classified material and media produced as a result of classified processing operations;

4. A location-specific procedure for destroying classified material and media;

5. A plan for application software and data backup as well as emergency actions;

6. A memorandum designating specific individuals' responsibility for overall system management, system security (site ISSO and alternate), and local/regional U.S. security personnel. If certification to process national security information is being requested, all designees must have current security clearances and be U.S. citizens; and

7. In cases where certification to process national security information is being requested, a memorandum from the Regional Security Officer (RSO) or Office of Security (SEC) acknowledging that the system and all of its components, workstations, cables, printers, modems, and other peripheral devices are compliant with the prevailing red/black installation requirements (available from the ISSO for USAID and/or RSO).

***More details on Agency IS security responsibilities are contained in the Internal Mandatory Reference, "Information Technology Security Roles and Responsibilities." (See Mandatory Reference, "Information Technology Security Roles and Responsibilities")**

6. Approval to Operate

Approval is the formal authorization for a system or major application to process information at a specified level of sensitivity in an operational environment. It is based upon validation that a system or major application is installed and operated in compliance with **Federal law and regulatory guidance, and** specified USAID security requirements (identified in USAID ADS Security Guidance and Chapters 545 and 552-- **completion of a USAIDCAP effort provides documentation needed to validate that a system or major application has been properly assessed and documented in order to receive approval to operate**. All IS approvals to operate will be granted by the Director of M/IRM based on the recommendations of the ISSO for USAID.

The **designated** ISSO is tasked with processing and evaluating any site or organizational requests for major application or system certification and accreditation, and approval(s) to operate.

The approval process includes the following procedures:

a. The requesting Bureau, Office, or Mission must forward to the ISSO for USAID a requirements analysis and facility security plan (assistance in completing these documents is available upon request from M/IRM/IPA);

b. The ISSO for USAID will conduct, or will direct the **designated** ISSO to conduct an evaluation of the requirements analysis and facility security plan;

c. The **designated** ISSO must ask SEC to verify that all required physical security controls are in place and operating as designed;

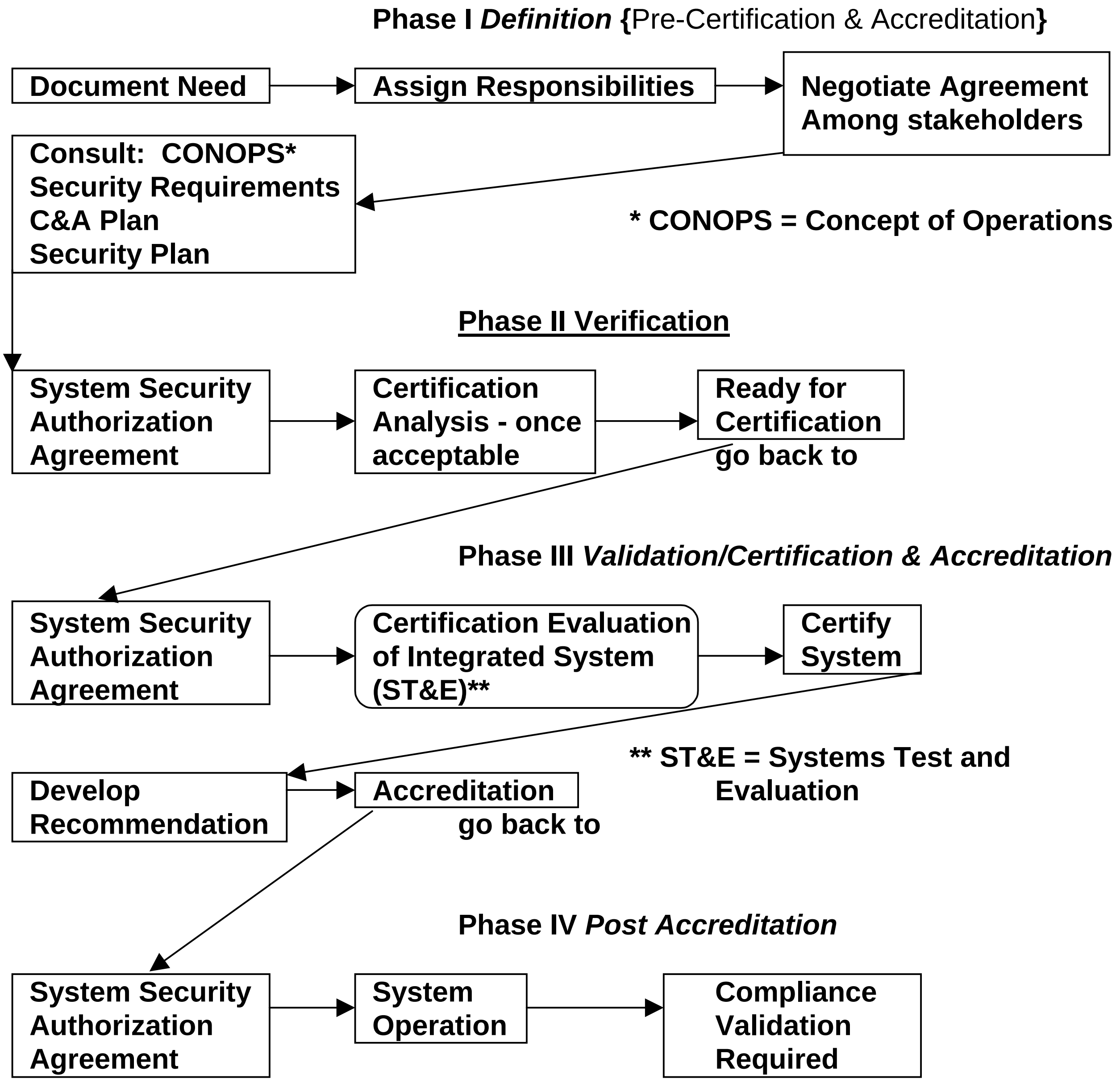
d. The ISSO for USAID will provide security awareness briefings for all personnel authorized to process classified national security information. If briefings are not feasible, the ISSO for USAID will provide the site ISSO with training and awareness materials;

e. **When the previous actions have been completed**, the **ISSO for USAID will recommend** to the Director of M/IRM **approval or disapproval** of an organization's request to authorize an IS to process SBU or classified national security information; and

f. The **Director** of **M/IRM will provide** the senior official of the requesting Bureau, Office, or Mission **a memorandum that formally grants** a system **approval to process SBU or** national security **classified information**. If a system is refused approval to process a specific level of information, the reason for refusal will be provided the requesting Bureau, Office, or Mission.

*Figure 1 - C&A and the IS ACQUISITION/LIFE CYCLE

The four phases of the Certification and Accreditation (C&A) process -
Definition {Pre-C&A}, Verification, Validation/C&A, and Post Accreditation - are below:


Phase I Definition {Pre-Certification & Accreditation}
Document Need
Assign Responsibilities
Negotiate Agreement Among stakeholders
Consult: CONOPS* Security Requirements C&A Plan Security Plan
* CONOPS = Concept of Operations
Phase II Verification
System Security Authorization Agreement
Certification Analysis - once acceptable
Ready for Certification
go back to
Phase III Validation/Certification & Accreditation
System Security Authorization Agreement
Certification Evaluation of Integrated System (ST&E)**
Certify System
** ST&E = Systems Test and Evaluation
Develop Recommendation
Accreditation
go back to
Phase IV Post Accreditation
System Security Authorization Agreement
System Operation
Compliance Validation Required

{Any changes to the accredited system begin the process again, starting with Phase I}

Text description of previous chart follows:

Figure 1, titled "C&A and the IS ACQUISITION/LIFE CYCLE" is a graphic depiction of the four phases of the certification and accreditation process, in the form of a flow chart. It begins with a statement: "The four phases of the Certification and Accreditation (C&A) process - Definition {Pre-C&A}, Verification, Validation/C&A,

and Post Accreditation - are below," then demonstrates the steps in the C&A Process.

Phase I, *Definition* {or Pre-Certification and Accreditation} goes from documenting security needs, to assigning responsibilities, to negotiating agreement among stakeholders. Phase one then shifts to consulting additional documentation, including the concept of operations (CONOPS), the system security requirements, the initial C&A plan and the security plan.

Phase II, Verification starts with preparation of the system security authorization agreement, and continues with the certification analysis. Once the certification analysis is acceptable, the system is ready for certification.

Phase III, Validation/Certification & Accreditation begins with a return to the system security authorization agreement, continues with the certification evaluation of the integrated system, applying system test and evaluation (ST&E) methods, to certify the system. Once the system is certified, develop a recommendation for accreditation.

Phase IV, Post Accreditation mandates reviews of the system security authorization agreement to track system operations that are required to validate compliance. Any changes to the accredited system begin the process again, starting with Phase I.