



INFORMATION ASSURANCE

CERTIFICATION AND ACCREDITATION

(C&A)

PUBLICATION

VOLUME II

**Site, Installed Program of Record, and
Locally Acquired Systems**

DEPARTMENT OF THE NAVY (DoN)
INFORMATION ASSURANCE (IA)
PUBLICATION

MODULE 5239-13 VOL II

Department of the Navy

For Official Use Only

IA Pub-5239-13 Vol. II

December 2000

Distribution:

Electronic versions of this document may be downloaded via anonymous ftp from infosec.navy.mil or via the DoN INFOSEC/IA Web Site on the NIPRNET at <https://infosec.navy.mil> and on the SIPRNET at <https://infosec.navy.smil.mil>.

For further assistance, the INFOSEC Technical Assistance Center (ITAC) may be reached at:

Commercial 1-800-304-4636

DSN 588-5428 / 4286

Local reproduction is authorized.

FOREWORD

Naval Information Assurance Program Publications (IA Pub) are issued by the Chief of Naval Operations (CNO) N643. The IA Pub series provides modules that guide the implementation of the policy direction established in Chief of Naval Operations Instruction (OPNAVINST) 5239.1B. These modules provide procedural, technical, administrative, and supplemental guidance for all information systems, whether business or tactical, used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or receipt of data. Each module focuses on a distinct subject and describes a standard methodology for planning, implementing and executing that element of the IA program within the Department of the Navy (DON).

This module, "Information Assurance Certification and Accreditation Publication," provides the DON IA C&A approach for Sites, Installed Program of Record (POR), and Locally Acquired systems.

Reviewed and Approved by:

CNO N643 Louise Davidson 9 JAN 01

TABLE OF CONTENTS

SECTION 1.0 1

INTRODUCTION 1

1.1 SCOPE AND PURPOSE 1

SECTION 2.0 3

**SITE, INSTALLED POR, AND LOCALLY ACQUIRED SYSTEMS
CERTIFICATION AND ACCREDITATION PROCESS..... 3**

2.1 DEFINITION PHASE (PHASE 1)..... 3

 2.1.1 Document Mission Need 4

 2.1.2 Registration 4

 2.1.3 Negotiation 4

2.2 VERIFICATION PHASE (PHASE 2)..... 5

 2.2.1 Site Procurement of an Information System 5

 2.2.2 Site Receives Program of Record (POR) Information System 5

2.3 VALIDATION PHASE (PHASE 3) 6

 2.3.1 Security Test and Evaluation (ST&E) 6

 2.3.2 Residual Risk Assessment 7

 2.3.3 Operational Environment Certification 7

 2.3.4 DAA Accreditation Decision 8

2.4 POST ACCREDITATION PHASE (PHASE 4)..... 8

SECTION 3.0 9

APPLICATION OF THE PROCESS..... 9

3.1 Tailored SSAAs 11

 3.1.1 Site SSAA 11

 3.1.2 Locally Acquired SSAA 11

3.2 Assistance 13

TABLE OF FIGURES

Figure 3-1 Site, Installed POR, and Locally Acquired Information System C&A Approach..... 10
Figure 3-2 SSAA Relationships..... 11
Figure 3-3 Site SSAA Structure..... 12
Figure 3-4 Locally Acquired SSAA Structure..... 12

SECTION 1.0 INTRODUCTION

This module introduces the second volume of the Department of the Navy (DON) Information Assurance (IA) Certification and Accreditation (C&A) Publication (IA Pub). This Pub extends the Chief of Naval Operations (CNO) policy directed in OPNAVINST 5239.1B, Department of the Navy Information Assurance Program, by providing IA guidance, procedures, and processes to assist the DoN in implementing its Information Assurance C&A Program.

1.1 SCOPE AND PURPOSE

This volume of module 5239-13 describes the DON's approach to C&A for sites, installed Programs of Record (POR), and locally acquired systems.

Within this publication the term "Program of Record" system identifies systems for which program requirements have been officially documented and approved through the acquisition community (via an Operational Requirements Document (ORD), or Acquisition Plan (AP), etc.) or through the budget community (with details displayed in the various budget exhibits). Within the DoN, Program of Record systems are typically acquired by the Systems Commands (or other second echelon organizations) for use by the operating forces.

This publication provides an approach by which the site can achieve accreditation of all the systems within a DAA's area of operational responsibility. This approach provides the ability to integrate POR certified systems/components and locally acquired systems into a single site System Security Authorization Agreement (SSAA). The scope of this publication includes certification and accreditation of systems that are typically categorized as Administrative and Mission Support (see IA Publication 5239-01).

“Administrative information systems are defined as those information systems handling information that is necessary for the conduct of the day-to-day business, but does not materially affect support to deployed forces or the readiness of contingency forces in the short term (may be classified, but is more likely to be sensitive or unclassified).”

“Mission Support information systems are defined as those systems handling information that is important to the support of deployed and contingency forces. It must be absolutely accurate, but can sustain minimal delay without seriously affecting operational readiness or mission effectiveness (may be classified, but is more likely to be sensitive or unclassified).”

The local procurement of compartmented or multi-level security information systems to support a mission requirement is not typical but does occur. Additionally, Program of Record (POR) information systems are provided to operational sites. This publication also addresses how these certification and accreditation efforts are to be accomplished.

SECTION 2.0

SITE, INSTALLED POR, AND LOCALLY ACQUIRED SYSTEMS CERTIFICATION AND ACCREDITATION PROCESS

It is DoN Information Assurance Policy that information and resources are appropriately safeguarded at all times, to support defense in depth across DoN and Department of Defense (DoD). Safeguards shall be applied such that information and resources maintain the appropriate level of confidentiality, integrity, availability, and accountability based upon mission criticality, level of required IA, and classification or sensitivity level of information entered, processed, stored, and/or transmitted. The safeguarding of information and systems shall be accomplished through the employment of defensive layers that include the Information Assurance (IA) disciplines.

Certification is the means by which these safeguards are assessed. Certification is applied to provide an approving authority with the details required to make an informed decision about the protection and defense of the information and/or system. This section addresses the approach to engage the Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) phases to certify and accredit a site, installed POR, and/or locally acquired system.

2.1 DEFINITION PHASE (PHASE 1)

“The Definition phase shall include activities to document the system mission, environment, and architecture; identify the threat; define the levels of effort; identify the certification authority (CA) and the DAA; and document the necessary security requirements for C&A. Phase 1 shall culminate with a documented agreement, between the program manager, the DAA, the CA, and the user representative of the approach and the results of the phase 1 activities.” This documented agreement is known as the System Security Authorization Agreement (SSAA).

Representatives from the Fleet Commander-In-Chiefs have developed a SSAA template. This template may be used for Certifying and Accrediting Fleet CINC systems. The template has been posted on the DoN INFOSEC World Wide Web (WWW) site at “<https://www.infosec.navy.mil>”. This template provides the outline for capturing the following elements within the DITSCAP Phase I.

- System Mission
- System Environment
- System Architecture
- Threat Identification

- Level of C&A Effort
- Identification of the Certification Authority
- Identification of the Designated Approving Authority,

Phase 1, as stated in the DITSCAP, “contains three process activities, document mission need, registration, and negotiation. Phase 1 starts with the input of the mission need statement (or other justification for the system) and ends by producing the SSAA.”

2.1.1 Document Mission Need

When procurement is initiated for the purchase of a locally acquired Information Technology (IT) product, the justification for purchase includes the mission need. Development of a POR system is initiated due to demonstration of a mission need. Installation of a POR system at a DoN site is the fulfillment of that mission need.

2.1.2 Registration

Registration is the process activity of the DITSCAP that initiates the dialogue among the DAA, the ISSM/ISSO, and the user representative for sites, installed POR, and locally acquired systems. As part of the Registration tasks, information is collected and evaluated, applicable requirements are determined, risk management and vulnerability assessment actions are begun, and the level of effort required for C&A is determined and planned.

The Fleet CINC representatives have already assessed the operational environments and classification levels of the information being processed. This assessment has already been incorporated in the Security Test and Evaluation (ST&E) Checklist templates provided on <https://infosec.navy.mil>. Completing this ST&E checklist and executing an automated security assessment tool satisfy the required level of C&A effort.

The site’s ISSM/ISSO should be informed that a new IT product will be installed at the local site. It is the role of the ISSM to ensure that the systems within the activity achieve their C&A.

2.1.3 Negotiation

The key parties of the DAA, ISSM/ISSO, and User Representatives should negotiate the associated level of effort. During negotiation, all participants involved in the system's local acquisition, installation, operation, certification and accreditation agree on the implementation strategy to be used to satisfy the security requirements identified during system registration. Negotiation has

already been performed at the Fleet CINC level by the Fleet CINC representatives and was used in the development of this publication.

2.2 VERIFICATION PHASE (PHASE 2)

The verification phase (Phase 2) involves the process of determining compliance of the evolving IS specification, design, or code with the security requirements and approach agreed on by the users, acquisition authority, and the DAA. Phase 2 process activities follow the evolution of system development. Tasks performed during Phase 2 include assessing the impact of system modification, certification analysis, preparation of the vulnerability assessment and refinement of the SSAA.

Systems addressed by this publication are not expected to involve any of the DoD Directive 5000.1 Phase II life-cycle development activities or stated process activities as discussed in the DITSCAP due to their nature, i.e., they are installed as directed from a POR or are purchased locally. These systems have either already completed Phase 2 of the SSAA through the acquisition program of record, or they have already been designed and can be purchased off the shelf. There may be exceptions as discussed in the following paragraphs (see Figure 3-1).

2.2.1 Site Procurement of an Information System

Sites can procure their own systems to satisfy their mission requirements. Typically, a local procurement addresses administrative or mission support systems that operate in the dedicated or system high mode. These systems' Verification Phase activities are generically documented by this publication.

Sites can also locally procure systems that operate in the compartmented or multi-level security mode. If the procurement includes an SSAA completed through the Verification Phase, the site would update the site's SSAA as described in section 2.3 of this publication. However, if the procurement of a compartmented or multi-level security information system does not include the SSAA through the Verification Phase, the site is required to follow the guidance stated in IA Publication 5239-13 Volume III prior to integration into the site's SSAA.

2.2.2 Site Receives Program of Record (POR) Information System

Sites may also receive POR systems as upgrades to existing systems or in support of new technologies. The DoD acquisition process provides the means for Program Managers of POR systems to develop the required information security documentation, such as the SSAA. However, this may not always happen. For POR information systems that are received at the site

without an SSAA (including the Type Accreditation decision from the Developmental DAA) the site should not accept the installation as complete. If the site does choose to accept the subject POR, proceed to IA Publication 5239-13 Volume III to accomplish the required C&A efforts.

The POR system that arrives at the local site with the required SSAA has (or should have) already completed the Verification Phase activities and achieved a Type Accreditation. The site should update the site's SSAA as discussed in section 2.3 of this guide to include this installed POR system in the site's accreditation.

2.3 VALIDATION PHASE (PHASE 3)

“The Validation phase shall include activities to evaluate the fully integrated system to validate system operation in a specified computing environment with an acceptable level of residual risk. Validation shall culminate in an approval to operate.” Validation (Phase 3) consists of process activities that occur after the system is integrated and culminates in the accreditation of the IT system.

2.3.1 Security Test and Evaluation (ST&E)

The objective of ST&E is to assess the technical and non-technical security features and assumptions of the configuration and implementation to ascertain that security features affecting confidentiality, integrity, availability, and accountability have been implemented, and perform properly. Certification Test and Evaluation (CT&E) is typically performed during the Verification Phase. The CT&E verifies the correct operation of the designed technical security requirements. For systems that are either installed POR or locally acquired without the C&A evidence from Phase II, ST&E shall validate the correct implementation of technical security configuration (i.e., Communications Security, Computer Security, Emission Security (i.e., TEMPEST)). In addition, the ST&E should focus on Physical Security, Personnel Security, Procedural Security, Security Education, Training, and Awareness, and the development of countermeasures to perceived threats.

ST&E for the site, installed POR, and locally acquired information systems shall consist of performing the activities listed in the ST&E checklist, which can be downloaded from <https://infosec.navy.mil>. This checklist has been developed and coordinated by the Fleet CINC representatives and the DoN Certification Agents. The checklist addresses the security requirements. The results of the checklist will provide evidence of the amount of residual risk. These results are used to validate the security behavior of the system and the assumptions of the security objectives. This checklist is for use in performing the certification and

accreditation of locally acquired systems with a Basic level of information assurance.

Networked systems shall run an automated security assessment tool against the network to determine the security posture of the system's configuration. The results of this tool will be used in assessing the risk to operating the systems

Locally acquired systems that are networked shall run an automated security assessment tool against the networked configuration. Recommended automated security assessment tools are identified on the <https://infosec.navy.mil> web site under "COMPUSEC tools". Alternatively, if the networked systems are accessible from the MILNET and/or NIPRNET, an On-Line Survey can be performed by the Fleet Information Warfare Center. The results of the network testing are also used in assessing the residual risk in operating the systems.

Operational sites should confirm the appropriate installation and configuration of POR systems prior to their acceptance. The installation and configuration validation procedures should be included in the System Operation Verification Test (SOVT) process or similar site acceptance testing process. This constitutes the ST&E for the system. Copies of the installation and configuration validation procedures (i.e., POR ST&E templates) should be obtained from the POR system support organization.

Each domain of locally acquired systems should complete the appropriate ST&E referenced in this publication. (Complete separate ST&Es for unclassified and classified systems). The DON requires completion of the applicable ST&E(s) and incorporation of them into the SSAA for documentation of validation and assessment of risk.

2.3.2 Residual Risk Assessment

This risk-based management review task assesses the operation and implementation of the system to determine if the risk to confidentiality, integrity, availability, and accountability security objectives is being maintained at an acceptable level. The risk management review assesses the vulnerabilities with respect to the threat method of attack, capability, motivation, and objective. The operational procedures and safeguards shall be evaluated to determine their effectiveness and ability to offset risk.

2.3.3 Operational Environment Certification

By signing the SSAA, the ISSM/ISSO documents the extent to which the system meets the requirements implied by the ST&E Checklist and automated security assessment tool. In addition, by signing the Phase 3 SSAA, the ISSM/ISSO certifies to the DAA the extent to which the set of specified security

requirements, as required by the DoN Information Assurance Program, are implemented in the operational environment. Supplemental recommendations might be made to improve the system's security posture. Such recommendations should provide input to future system enhancements and change-management decisions.

2.3.4 DAA Accreditation Decision

Accreditation is the authorization that permits an information system to process, store, and/or transmit information. This authorization is an informed decision about the protection and defense of the information and/or information system based upon the certification process.

The DAA can use the assessment of the checklist and automated security tool results to determine whether the risk in operating the system(s) is acceptable. The courses of action a DAA can take are discussed in IA Publication 5239-13 Volume I.

2.4 POST ACCREDITATION PHASE (PHASE 4)

The Post Accreditation phase (Phase 4) shall include activities to monitor system management and operation to ensure an acceptable level of residual risk is preserved. Security management, change-management, and periodic compliance validation reviews are conducted. Phase 4 begins after the system has been integrated into the operational environment and accredited. Phase 4 shall continue until the system is removed from service, a major change is planned for the system, or a periodic compliance validation is required.

SECTION 3.0

APPLICATION OF THE PROCESS

Removing the details of how the approach meets the spirit of the DITSCAP, this section provides the simple application of the C&A process for site, installed POR, and locally acquired systems.

Secretary of the Navy has directed in SECNAVINST 5239 that all DoN systems shall be accredited. Figure 3-1, Site, Installed POR, and Locally Acquired System C&A Approach, provides a block diagram of the steps that must be conducted for this level of effort.

The recommended application of the process is to develop one SSAA for a site. This SSAA will contain a separate section for each group of logically associated Administrative/Mission Support information systems of a similar classification level and a separate section POR information system. This SSAA can be easily developed using the referenced template. Once the SSAA is completed, the checklist and automated security assessment tool can be used to validate that the systems provide a DAA approved level of IA by analyzing the extent to which systems meet a set of implied specified requirements.

The activities required accomplishing certification and accreditation of these systems or components are provided below.

- Inform the ISSM/ISSO that a system is being installed.
- Update the site's SSAA and/or create an SSAA to include this system or component.
- Execute the ST&E checklist and automated security assessment tool
- Assess results of ST&E and security assessment tool report with regard to risk
- Re-sign the Site/System SSAA certifying the Operational environment's compliance with the stated requirements.
- Update/receive DAA accreditation

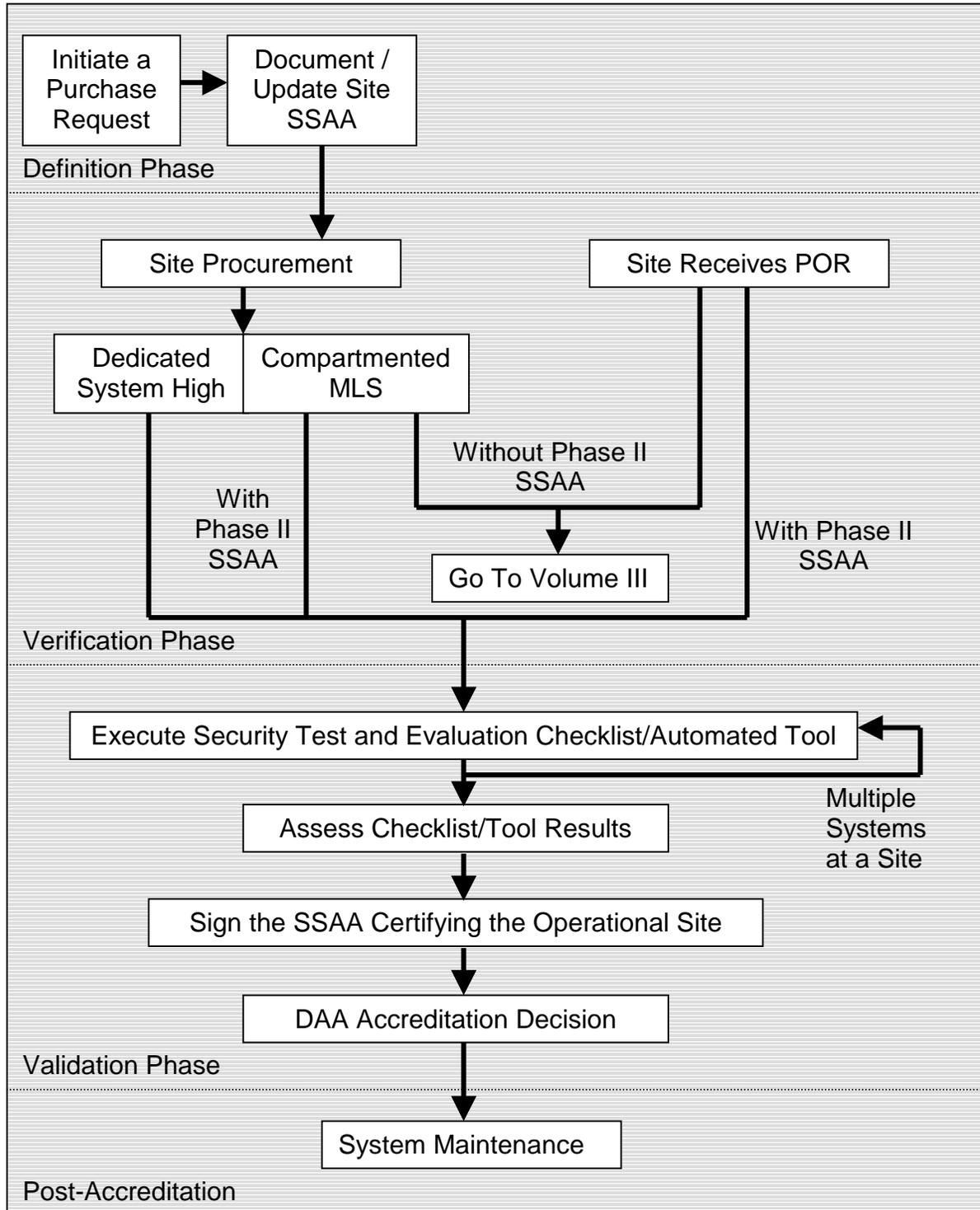


Figure 3-1 Site, Installed POR, and Locally Acquired Information System C&A Approach

3.1 Tailored SSAAs

This section provides insight into the tailoring of the SSAA to meet the operational application of a SSAA for Site, Installed Program of Record and Locally Acquired Systems. Figure 3-2 illustrates the relationships between these SSAAs. The DoN has determined that systems of similar security policies may be addressed in a single SSAA.

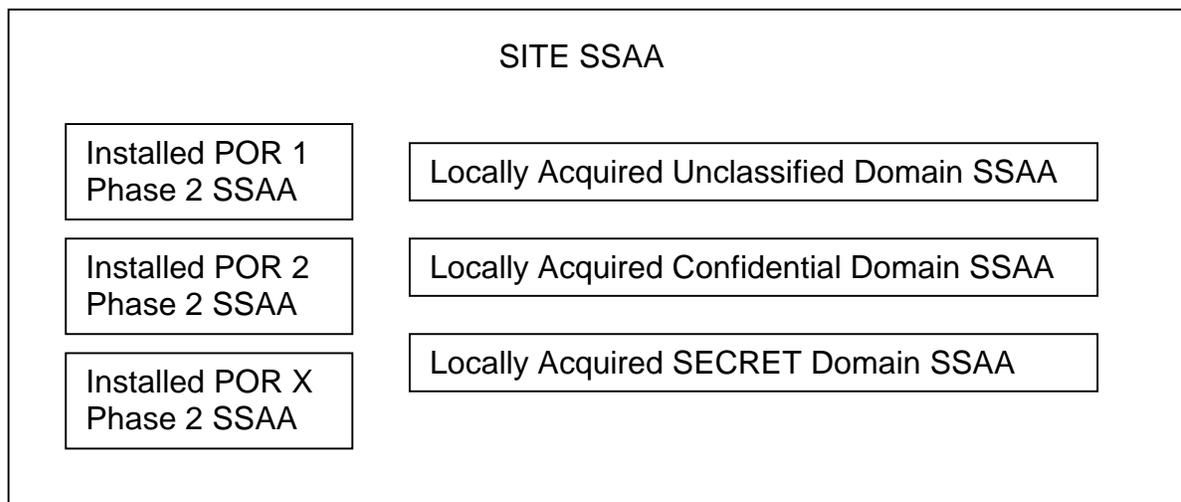


Figure 3-2 SSAA Relationships

3.1.1 Site SSAA

As discussed, a site SSAA is generated to provide a mechanism by which a local DAA may accredit the systems within an area of responsibility. The site SSAA consolidates installed POR SSAAs and locally acquired system SSAAs into one comprehensive SSAA. A template of this SSAA is available on <https://infosec.navy.mil>. The structure of a site SSAA is tailored to address only those protections and controls that apply at a site level (see figure 3-3).

3.1.2 Locally Acquired SSAA

The locally acquired system SSAA is also tailored due to the Basic IA level of effort applied. If a site SSAA is or will be developed, the structure of the locally acquired SSAA is presented in figure 3-4. If a site SSAA will not be developed, the locally acquired SSAA must also include the information presented in figure 3-3. A locally acquired SSAA template is provided on <https://infosec.navy.mil>.

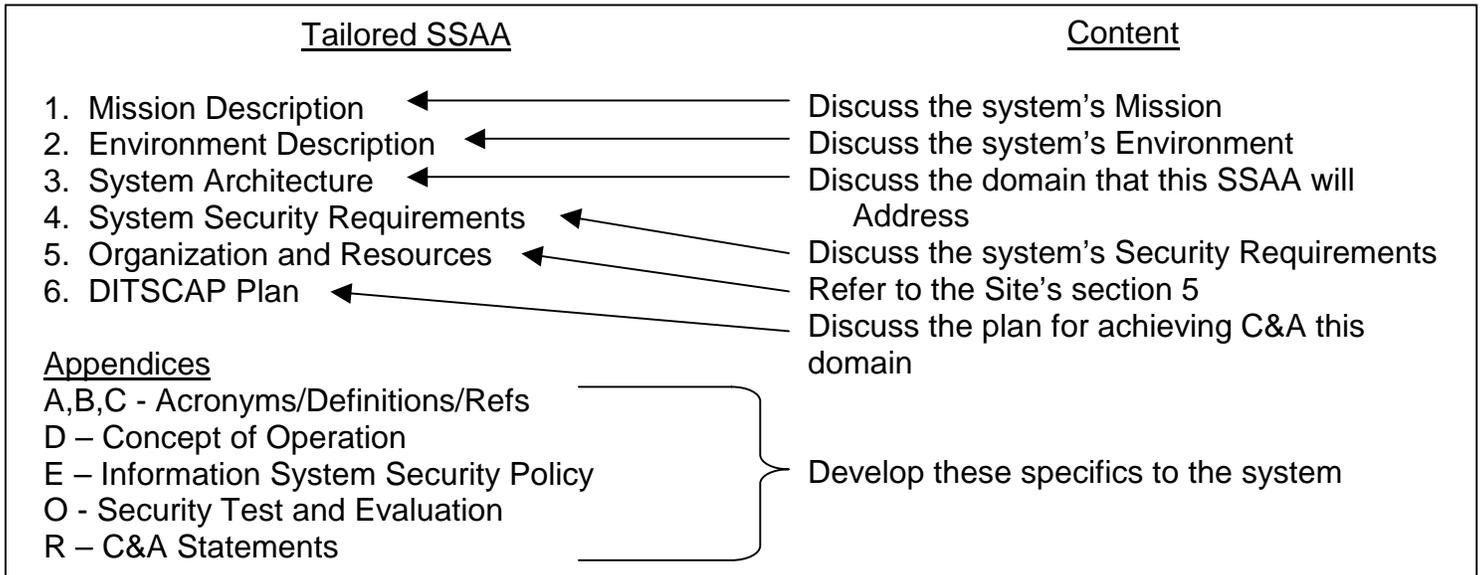


Figure 3-3 Site SSAA Structure

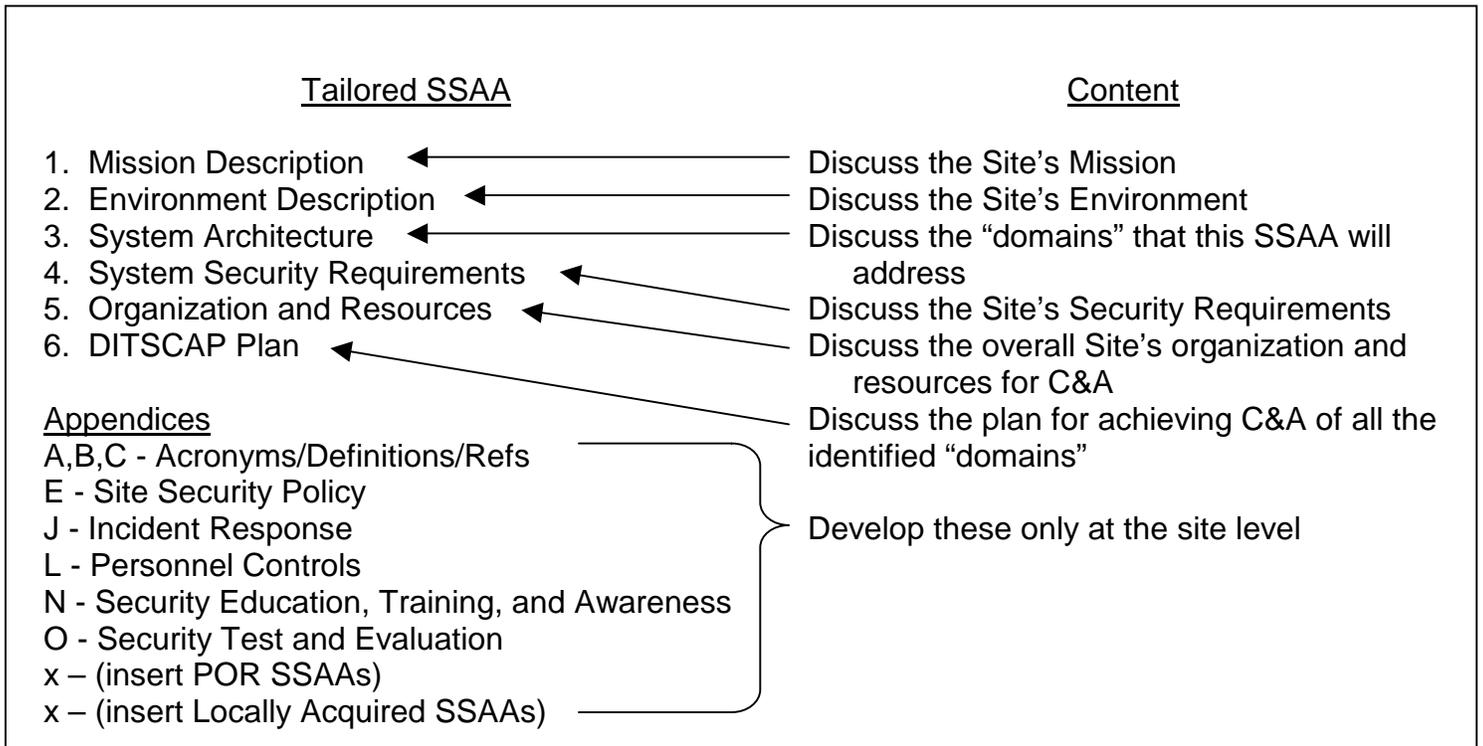


Figure 3-4 Locally Acquired SSAA Structure

3.2 Assistance

Questions on implementing this process can be addressed by the INFOSEC Help desk at 1-800-304-4636. The DoN Certification Agents can provide assistance at the Naval Research Laboratory and Space and Naval Warfare System Centers.