

**Security Plans to System Security Authorization
Agreements:**

***A Guide for Using the NIACAP Methodology to Develop
Quality System Security Plan Certification and
Accreditation Packages***

Developed by the
U.S. Department of Commerce
Office of the Secretary/Office of the Chief Information Officer
IT Security Program Manager

15 June 2003 (version 3)

Introduction

The U.S. Department of Commerce Information Technology (IT) Security Program Manager developed this guide to aid Commerce program officials, Chief Information Officers (CIOs), IT Security Officers (ITSOs), and other staff in developing quality system security plans using the *National Information Assurance Certification and Accreditation Process* (NIACAP). The NIACAP methodology is described in National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 1000, and it provides a logical sequence of activities for development of a quality system security plan and comprehensive system certification and accreditation (C&A) package for the system.

Development of a quality C&A package is critical to provide assurance that all Commerce IT systems contain adequate, functioning security controls. Although the National Institute of Standards and Technology (NIST) provides valuable guidance for development of system security plans and inclusion of security controls in systems, these guides do not provide a methodology for preparing a complete package for use to certify and accredit systems. NIST issued Federal Information Processing Standard 102, *Guideline for Computer Security Certification and Accreditation*, in 1983. However, the standard does not address recent federal requirements issued by OMB or take into account issues related to interconnected computing environments. Therefore, NIST is currently updating the standard to reflect NIACAP methodology and other best practices. Using the NIACAP methodology ensures that consideration for the adequacy of system security controls have been made during all system life cycle phases:

- from defining the system and designing security requirements;
- to verifying compliance with the requirements during system development;
- to validating the adequacy before full system operation, and finally
- to monitoring security controls throughout system operation until its disposal.

This guide provides answers to frequently asked questions arising from recent Departmentwide training in the C&A process. As a result of these common concerns, this guide also provides crosswalks of the documentation outlines and terminology for three key requirements:

- NIST Special Publication (SP) 800-18, *Guide for Developing Security Plans for Information Technology Systems* (December 1998), which outlines the requirements for completion of system security plans for major applications and general support systems.
- NIST SP 800-26, *Security Self-Assessment Guide for Information Technology Systems* (November 2001), which outlines critical system security controls; and
- National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 1000, *National Information Assurance Certification and Accreditation Process* (NIACAP), which outlines the requirements for completion of the System Security Authorization Agreement (SSAA) that comprises the complete C&A package.

If you have questions or comments regarding this guide, contact Nancy DeFrancesco, the IT Security Program Manager, at (202) 482-3490, or at NDeFrancesco@doc.gov.

Table of Contents

<u>Introduction</u>	i
<u>Frequently Asked C&A Questions</u>	1
<u>NIST 800-18 System Security Plan Outline</u>	2
<u>NIST 800-26 System Security Controls Outline</u>	3
<u>NIACAP SSAA Outline</u>	4
<u>Terminology Crosswalk</u>	5
<u>System Security Certification and Accreditation Package Checklist</u>	6
<u>Crosswalk of NIST SP 800-18 System Security Plan Outline to NIACAP System Security Authorization Agreement Outline</u>	8
Using the NIACAP Methodology to Develop the System Security Plan	
<u>Phase 1: System Definition</u>	15
<u>Phase 2: Controls Verification in System Development</u>	16
<u>Phase 3: Controls Validation in the Operational Environment</u>	17
<u>Phase 4: Post Accreditation</u>	18

Frequently Asked Certification and Accreditation (C&A) Questions

Does the Department require that I follow NIACAP or NIST guidance?

The Department requires that all Commerce IT systems have a security plan documented in accordance with [NIST Special Publication 800-18](#). Also, the Department requires that the security controls of all systems be assessed in accordance with [NIST Special Publication 800-26](#). Finally, the Department requires that all Commerce IT systems be certified and accredited. One process to accomplish C&A is defined by [NIACAP](#), and this process is mandated for certification and accreditation (C&A) of all national security systems. To maintain consistency in C&A of all Commerce IT systems, the Department has adopted NIACAP as the best practice methodology for C&A. The NIACAP methodology facilitates development of the System Security Plan Certification and Accreditation Package (SSPCAP) required by the Department, which combines elements of the NIACAP System Security Authorization Agreement (SSAA) package, with the NIST SP 800-18 system security plan elements and controls.

Do I have to redo all my system security plans to comply with NIACAP?

No. However, you must develop a system C&A package for all systems. The primary component of the C&A package is the system security plan. You should, as part of your initial system C&A and periodic system recertifications, review your security C&A package documentation for consistency with the required elements of the SSPCAP.

Do I develop an SSAA or a System Security Plan?

You develop a combination of both – the “best of both worlds.” The System Security Plan already contains most elements of the SSAA, and the additional elements of the SSAA results in a complete C&A package, including a project/work plan for performing the C&A activities. A checklist is provided beginning on page 6 of this guide to follow in developing a System Security Plan C&A Package (SSPCAP).

Where do I start if my systems are already in the operational phase?

All C&A efforts begin at [Phase 1, System Definition](#). If you have systems that are currently operating in a production environment but are not certified and accredited, you would first document the system’s mission and business purpose, system architecture, system environment, system requirements, and organizational roles and responsibilities. Because [Phase 2](#) pertains to systems under development, and your system is already operational, you would proceed to [Phase 3, Validation of Controls in the Operational Environment](#).

- 1 Define the System**
 - 1.2 System Identification
 - 1.2.1 System Name/Title
 - 1.2.2 Responsible Organization
 - 1.2.3 Information Contact(s)
 - 1.2.4 Assignment of Security Responsibility
 - 1.3 System Operational Status
 - 1.4 General Description/Purpose
 - 1.5 System Environment
 - 1.6 System Interconnection/Information Sharing
 - 1.7 Sensitivity of Information Handled
 - 1.7.1 Laws, Regulations, and Policies Affecting the System
 - 1.7.2 General Description of Sensitivity

- 2 Management Controls**
 - 2.1 Risk Assessment and Management
 - 2.2 Review of Security Controls
 - 2.3 Rules of Behavior
 - 2.4 Planning for Security in the Life Cycle
 - 2.4.1 Initiation Phase
 - 2.4.2 Development/Acquisition Phase
 - 2.4.3 Implementation Phase
 - 2.4.4 Operation/Maintenance Phase
 - 2.4.5 Disposal Phase
 - 2.5 Authorize Processing

- 3 Operational Controls**
 - 3.MA. Major Application – Operational Controls
 - 3.MA.1 Personnel Security
 - 3.MA.2 Physical and Environmental Protection
 - 3.MA.2.1 Explanation of Physical and Environment Security
 - 3.MA.2.2 Computer Room Example
 - 3.MA.3 Production, Input/Output Controls
 - 3.MA.4 Contingency Planning
 - 3.MA.5 Application Software Maintenance Controls
 - 3.MA.6 Data Integrity/Validation Controls
 - 3.MA.7 Documentation
 - 3.MA.8 Security Awareness and Training

 - 3.GSS. General Support System – Operational Controls
 - 3.GSS.1 Personnel Controls
 - 3.GSS.2 Physical and Environmental Protection
 - 3.GSS.2.1 Explanation of Physical and Environment Security
 - 3.GSS.2.2 Computer Room Example
 - 3.GSS.3 Production, Input/Output Controls
 - 3.GSS.4 Contingency Planning (Continuity of Support)
 - 3.GSS.5 Hardware and System Software Maintenance Controls
 - 3.GSS.6 Integrity Controls
 - 3.GSS.7 Documentation
 - 3.GSS.8 Security Awareness and Training
 - 3.GSS.9 Incident Response Capability

- 4 Technical Controls**
 - 4.MA. Major Application - Technical Controls
 - 4.MA.1 Identification and Authentication
 - 4.MA.1.1 Identification
 - 4.MA.1.2 Authentication
 - 4.MA.2 Logical Access Controls (Authorization/Access Controls)
 - 4.MA.3 Public Access Controls
 - 4.MA.4 Audit Trails

 - 4.GSS. General Support System - Technical Controls
 - 4.GSS.1 Identification and Authentication
 - 4.GSS.1.1 Identification
 - 4.GSS.1.2 Authentication
 - 4.GSS.2 Logical Access Controls (Authorization/Access Controls)
 - 4.GSS.3 Audit Trails

NIST SP 800-26 *Security Self-Assessment Guide for Information Technology Systems*
(November 2001)
System Controls Outline

Management Controls

1. Risk Management
2. Review of Security Controls
3. Life Cycle
4. Authorize Processing (Certification & Accreditation)
5. System Security Plan

Operational Controls

6. Personnel Security
7. Physical and Environmental Protection
8. Production, Input/Output Controls
9. Contingency Planning
10. Hardware and System Software Maintenance
11. Data Integrity
12. Documentation
13. Security Awareness, Training, and Education
14. Incident Response Capability

Technical Controls

15. Identification and Authentication
16. Logical Access Controls
17. Audit Trails

National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 1000
National Information Assurance Certification and Accreditation Process (NIACAP)
System Security Authorization Agreement (SSAA) Outline

1.0 MISSION DESCRIPTION AND SYSTEM IDENTIFICATION

- 1.1 System Name and Identification
- 1.2 System Description
- 1.3 Functional Description
 - 1.3.1 System Capabilities
 - 1.3.2 System Criticality
 - 1.3.3 Classification and Sensitivity of Data Processed
 - 1.3.4 System User Description and Clearance Levels
 - 1.3.5 Life Cycle of the System
- 1.4 System Concept of Operations (CONOPS) summary

2.0 ENVIRONMENT DESCRIPTION

- 2.1 Operating environment
 - 2.1.1 Facility Description
 - 2.1.2 Physical Security
 - 2.1.3 Administrative Issues
 - 2.1.4 Personnel
 - 2.1.5 COMSEC
 - 2.1.6 TEMPEST
 - 2.1.7 Maintenance Procedures
 - 2.1.8 Training Plans
- 2.2 Software Development and Maintenance Environment
- 2.3 Threat Description

3.0 SYSTEM ARCHITECTURAL DESCRIPTION

- 3.1 System Description
- 3.2 System Interfaces and External Connections
- 3.3 Data Flow
- 3.4 Accreditation Boundary

4.0 SYSTEM SECURITY REQUIREMENTS

- 4.1 National and Organizational Security Requirements
- 4.2 Governing Security Requisites
- 4.3 Data Security Requirements
- 4.4 Security CONOPS
- 4.5 Network Connection Rules
- 4.6 Configuration and Change Management Requirements
- 4.7 Reaccreditation Requirements

5.0 ORGANIZATIONS AND RESOURCES

- 5.1 Organizations
- 5.2 Resources
- 5.3 Training
- 5.4 Other Supporting Organizations

6.0 NIACAP WORK PLAN

- 6.1 Tailoring Factors
 - 6.1.1 Programmatic Considerations
 - 6.1.2 Security Environment
 - 6.1.3 IT System Characteristics
 - 6.1.4 Reuse of Previously Approved Solutions
- 6.2 Tasks and Milestones
- 6.3 Schedule Summary
- 6.4 Level of Effort
- 6.5 Roles and Responsibilities

Appendices should be added to include system C&A documents; optional appendices may be added to meet specific needs. All documentation relevant to the systems' C&A should be included in the SSAA.

APPENDIX A	Acronym list
APPENDIX B	Definitions
APPENDIX C	References
APPENDIX D	Security Requirements and/or Requirements Traceability Matrix
APPENDIX E	Security Test and Evaluation Plan and Procedures
APPENDIX F	Certification Results
APPENDIX G	Risk Assessment Results
APPENDIX H	Certifier's Recommendation
APPENDIX I	System Security Policy
APPENDIX J	System Rules of Behavior
APPENDIX K	Security Operating Procedures
APPENDIX L	Contingency Plan(s)
APPENDIX M	Security Awareness and Training Plan
APPENDIX N	Personnel Controls and Technical Security Controls
APPENDIX O	Incident Response Plan
APPENDIX P	Memorandums of Agreement – System Interconnect Agreements
APPENDIX Q	Applicable System Development Artifacts or System Documentation
APPENDIX R	Accreditation Documentation and Accreditation Statement

Terminology Crosswalk

<u>NIACAP Term</u>	<u>Commerce Equivalent Term</u>
Accreditation	Accreditation, Approval to Operate, or Authorization to Process
Certification	Certification, Operational Tests of Controls, Vulnerability Testing, Penetration Testing
Concept of Operations (CONOPS)	System mission and business function(s)
Contingency Plan Plan,	Contingency Plan, Business Continuity Disaster Recovery Plan, Continuity of Operations Plan (COOP, IT portion thereof)
Designated Approving Authority (DAA)	Designated Approving Authority (DAA)
Incident Response Plan	Incident Handling and Response Procedures
Information System Security Officer (ISSO)	IT Security Officer (ITSO)
Program Manager	System Developer
Risk Assessment	Risk Assessment
Rules of Behavior	Rules of Behavior, Acceptable Use Policy
Security Awareness and Training Plan	Security Awareness and Training Procedure
Security Operating Procedures	Standard Operating Procedures for System Security
System Administrator	Information System Security Officer (ISSO)
System Certifier	System Certifier
System Security Authorization Agreement (SSAA)	System Security Plan and associated C&A Package
System Security Policy	System Security Policy (system-specific security configuration standards)
User Representative	Owner of System under Development

System Security Plan Certification and Accreditation Package Checklist

Checklist Item	Included in System C&A Package?		
	Yes	No	Target Date for Completion
SECTION A. SYSTEM SECURITY PLAN			
1 Define the System			
1.2 System Identification			
1.2.1 System Name/Title			
1.2.2 Responsible Organization			
1.2.3 Information Contact(s)			
1.2.4 Assignment of Security Responsibility			
1.3 System Operational Status			
1.4 General Description/Purpose			
1.5 System Environment			
1.6 System Interconnection/Information Sharing (SSAA Appendix P)			
1.7 Sensitivity of Information Handled			
1.7.1 Laws, Regulations, and Policies Affecting the System (SSAA Appendices A, B, and C if necessary, plus Appendix D)			
1.7.2 General Description of Sensitivity			
2 Management Controls			
2.1 Risk Assessment and Management (SSAA Appendix G)			
2.2 Review of Security Controls			
2.3 Rules of Behavior (SSAA Appendix J)			
2.4 Planning for Security in the Life Cycle (SSAA Appendix I)			
2.4.1 Initiation Phase			
2.4.2 Development/ Acquisition Phase			
2.4.3 Implementation Phase			
2.4.4 Operation/ Maintenance Phase			
2.4.5 Disposal Phase			
2.5 Authorize Processing			
Accreditation Documentation (SSAA Appendix R)			
Accreditation Statement (SSAA Appendix R)			
3 Operational Controls (SSAA Appendices K, L, M, N, O, and Q)			
<i>3.MA Major Application – Operational Controls</i>			
3.MA.1 Personnel Security			
3.MA.2 Physical and Environmental Protection			
3.MA.2.1 Explanation of Physical and Environment Security			
3.MA.2.2 Computer Room Example			
3.MA.3 Production, Input/Output Controls			
3.MA.4 Contingency Planning			
3.MA.5 Application Software Maintenance Controls			
3.MA.6 Data Integrity/Validation Controls			
3.MA.7 Documentation			
3.MA.8 Security Awareness and Training			
<i>3.GSS General Support System – Operational Controls</i>			
3.GSS.1 Personnel Controls			
3.GSS.2 Physical and Environmental Protection			
3.GSS.2.1 Explanation of Physical and Environment Security			
3.GSS.2.2 Computer Room Example			
3.GSS.3 Production, Input/Output Controls			
3.GSS.4 Contingency Planning (Continuity of Support)			

Checklist Item	Included in System C&A Package?		
	Yes	No	Target Date for Completion
3.GSS.5 Hardware and System Software Maintenance Controls			
3.GSS.6 Integrity Controls			
3.GSS.7 Documentation			
3.GSS.8 Security Awareness and Training			
3.GSS.9 Incident Response Capability			
4 Technical Controls (SSAA Appendix N)			
<i>4.MA Major Application Technical Controls</i>			
4.MA.1 Identification and Authentication			
4.MA.1.1 Identification			
4.MA.1.2 Authentication			
4.MA.2 Logical Access Controls (Authorization/Access Controls)			
4.MA.3 Public Access Controls			
4.MA.4 Audit Trails			
<i>4.GSS General Support System Technical Controls</i>			
4.GSS.1 Identification and Authentication			
4.GSS.1.1 Identification			
4.GSS.1.2 Authentication			
4.GSS.2 Logical Access Controls (Authorization/Access Controls)			
4.GSS.3 Audit Trails			
SECTION B: CERTIFICATION PACKAGE			
1.0 NIACAP Work Plan			
1.1 Tailoring Factors			
1.1.1 Programmatic Considerations			
1.1.2 Security Environment			
1.1.3 IT System Characteristics			
1.1.4 Reuse of Previously Approved Solutions			
1.2 Tasks and Milestones			
1.3 Schedule Summary			
1.4 Level of Effort			
1.5 Roles and Responsibilities			
2.0 Security Test and Evaluation Plan and Procedures (SSAA Appendix E)			
2.1 Certification Results (SSAA Appendix F)			
2.2 Certifier's Recommendation (SSAA Appendix H)			

Crosswalk of NIST SP 800-18 System Security Plan Outline to the NIACAP System Security Authorization Agreement Outline

NIST SP 800-18 Security Plan Outline	NIACAP SSAA Outline	SSPCAP Phase Activities		
1 Plan Development – All Systems				
1.2 System Identification	1.0 Mission Description and System Identification	Phase 1	----	-----
1.2.1 System Name/Title	1.1 System Name and Identification	Collect data		
1.2.2 Responsible Organization	5.0 Organizations and Resources	Update Security Plan, generate appendices as needed		
1.2.3 Information Contact(s)	5.1 Organizations			
1.2.4 Assignment of Security Responsibility	5.2 Resources 5.4 Other Supporting Organizations			
1.3 System Operational Status	1.2 System Description			
1.4 General Description/Purpose	1.3 Functional Description			
	1.3.1 System Capabilities			
	1.3.4 System User Description and Clearance Levels			
	1.4 System Concept of Operations (CONOPS) summary			
	3.0 System Architectural Description			
	3.1 System Description			
	3.3. Data Flow			
	3.4 Accreditation Boundary			

NIST SP 800-18 Security Plan Outline	NIACAP SSAA Outline	SSPCAP Phase Activities		
1.5 System Environment	2.0 Environment Description 2.1 Operating Environment 2.1.1 Facility Description 2.1.2 Administrative Issues 2.1.4 Personnel 2.1.5 COMSEC 2.1.6 TEMPEST	Phase 1 Collect data Update Security Plan, generate appendices as needed	-----	-----
1.6 System Interconnection/ Information Sharing	3.2 System Interfaces and External Connections Appendix P Memorandums of Agreement – System Interconnect Agreements			
1.7 Sensitivity of Information Handled 1.7.2 General Description of Sensitivity	1.3.2 System Criticality (national critical, mission critical, or business essential) 1.3.3 Classification and Sensitivity of Data Processed			

NIST SP 800-18 Security Plan Outline	NIACAP SSAA Outline	SSPCAP Phase Activities		
1.7.1 Laws, Regulations, and Policies Affecting the System	4.0 System Security Requirements 4.1 National and Organizational Security Requirements 4.2 Governing Security Requisites 4.3 Data Security Requirements 4.4 Security CONOPS 4.5 Network Connection Rules 4.6 Configuration and Change Management Requirements 4.7 Reaccreditation Requirements Appendix D Security Requirements and/or Requirements Traceability Matrix Appendix I System Security Policy Appendix K Security Operating Procedures	Phase 1 Collect data Update Security Plan, generate appendices as needed	----	-----

NIST SP 800-18 Security Plan Outline	NIACAP SSAA Outline	SSPCAP Phase Activities		
2 Management Controls				
2.1 Risk Assessment and Management	2.3 Threat Description Appendix G Risk Assessment Results	Phase 1 Obtain threat assessment Begin vulnerability and risk assessment Update Security Plan, generate appendices as needed	Phase 2 Perform risk and vulnerability assessment Update Security Plan, generate appendices as needed	Phase 3 Analyze risk assessment results Compare assessment results to certification test results Develop risk mitigation strategy
2.2 Review of Security Controls	Appendix E Security Test and Evaluation Plan and Procedures Appendix F Certification Results	----	----	----
2.3 Rules of Behavior	Appendix J System Rules of Behavior	Phase 1 Develop Rules Update Security Plan, generate appendices as needed	----	----

NIST SP 800-18 Security Plan Outline	NIACAP SSAA Outline	SSPCAP Phase Activities		
<p>2.4 Planning for Security in the Life Cycle</p> <p>2.4.1 Initiation Phase</p> <p>2.4.2 Development/ Acquisition Phase</p> <p>2.4.3 Implementation Phase</p> <p>2.4.4 Operation/ Maintenance Phase</p> <p>2.4.5 Disposal Phase</p>	<p>1.3.5 Life Cycle of the System</p> <p>2.1.7 Maintenance Procedures</p>	<p>Phase 1</p> <p>Collect data</p> <p>Update Security Plan, generate appendices as needed</p>	<p>----</p>	<p>----</p>
<p>2.5 Authorize Processing</p>	<p>Appendix H Certifier's Recommendation</p> <p>Appendix R Accreditation Documentation and Accreditation Statement</p>	<p>----</p>	<p>Phase 2</p> <p>Certify development system/ determine if operational system ready for certification testing</p> <p>Finalize system security plan</p>	<p>Phase 3</p> <p>Certify operational system</p> <p>Accredit system</p>

NIST SP 800-18 Security Plan Outline	NIACAP SSAA Outline	SSPCAP Phase Activities		
3. Operational Controls and 4. Technical Controls				
3.MA.1 Personnel Security 3.MA.2 Physical and Environmental Protection 3.MA.2.1 Explanation of Physical and Environment Security 3.MA.2.2 Computer Room Example 3.MA.3 Production, Input/Output Controls 3.GSS.1 Personnel Controls 3.GSS.2 Physical and Environmental Protection 3.GSS.2.1 Explanation of Physical and Environment Security 3.GSS.2.2 Computer Room Example 3.GSS.3 Production, Input/Output Controls	Appendix N Personnel Controls and Technical Security Controls	Phase 1	Phase 2	Phase 3
		Identify requirements	Verify compliance of controls documented in Security Plan with system requirements	Validate/Test operational and technical controls in operational environment
3.MA.4 Contingency Planning 3.GSS.4 Contingency Planning (Continuity of Support)			Update Security Plan to document operational controls, generate appendices as needed	<ul style="list-style-type: none"> • Perform security test and evaluation review of operational controls – Review personnel security procedures – Observe physical and environmental controls – Evaluate contingency plan

NIST SP 800-18 Security Plan Outline	NIACAP SSAA Outline	SSPCAP Phase Activities		
3.MA.5 Application Software Maintenance Controls 3.GSS.5 Hardware and System Software Maintenance Controls	2.2 Software Development and Maintenance Environment Appendix N Personnel Controls and Technical Security Controls	Phase 1 Identify requirements Update Security Plan, generate appendices as needed	Phase 2 Verify compliance of controls documented in Security Plan with system requirements Update Security Plan to document operational and technical controls, generate appendices as needed	Phase 3 Validate/Test operational and technical controls in operational environment
3.MA.6 Data Integrity/Validation Controls 3.GSS.6 Integrity Controls	Appendix N Personnel Controls and Technical Security Controls			<ul style="list-style-type: none"> •Perform security test and evaluation review of operational controls
3.MA.7 Documentation 3.GSS.7 Documentation	Appendix Q Applicable System Development Artifacts or System Documentation			<ul style="list-style-type: none"> – Review hardware/software maintenance and change management procedures
3.MA.8 Security Awareness and Training 3.GSS.8 Security Awareness and Training	2.1.8 Training Plans 5.3 Training Appendix M Security Awareness and Training Plan			<ul style="list-style-type: none"> – Review completeness of system documentation
3.GSS.9 Incident Response Capability	Appendix O Incident Response Plan			<ul style="list-style-type: none"> – Evaluate incident response procedures
4.MA.1 Identification and Authentication 4.MA.1.1 Identification 4.MA.1.2 Authentication 4.MA.2 Logical Access Controls (Authorization/Access Controls) 4.MA.3 Public Access Controls 4.MA.4 Audit Trails 4.GSS.1 Identification and Authentication 4.GSS.1.1 Identification 4.GSS.1.2 Authentication 4.GSS.2 Logical Access Controls (Authorization/Access Controls) 4.GSS.3 Audit Trails	Appendix Q Applicable System Development Artifacts or System Documentation			<ul style="list-style-type: none"> •Perform penetration testing to validate technical controls

NIST SP 800-18 Security Plan Outline	NIACAP SSAA Outline	SSPCAP Phase Activities		
Add appendix as needed	NIACAP Work Plan	Generate work plan	----	----
Add appendix as needed	Appendix A Acronym list	Generate appendices as needed		
Add appendix as needed	Appendix B Definitions			
Add appendix as needed	Appendix C References			

Certification and Accreditation Phase 1: System Definition

Roles and Responsibilities:

- DAA assigns certifier and resources for certifier team, establishes certification level based on system sensitivity/criticality.
- System Certifier/team tailors NIACAP to certification level; develops NIACAP Work Plan; conducts interviews of program manager (if any), user representative(s) (if any), and system administrator(s)/ISSOs; gathers data and collects documentation; begins vulnerability and risk assessment; and updates system security plan and generates appendices as needed.
- ITSO assists DAA and system certifier.

NIACAP SSAA Elements Addressed

- 1.0 Mission Description and System Identification
- 2.0 Environment Description
- 3.0 System Architectural Description
- 4.0 System Security Requirements
- 5.0 Organizations and Resources

- Appendix A Acronym List
- Appendix B Definitions
- Appendix C References
- Appendix D Requirements Traceability Matrix
- Appendix I System Security Policy
- Appendix J System Rules of Behavior
- Appendix K Security Operating Procedures
- 6.0 NIACAP Work Plan

NIST SP 800-18 System Security Plan C&A Package Elements Addressed

- 1 Define the System
 - 1.2 System Identification
 - 1.3 System Operational Status
 - 1.4 General Description/Purpose
 - 1.5 System Environment
 - 1.7 Sensitivity of Information Handled
- 2 Management Controls
 - 2.3 Rules of Behavior
 - 2.4 Planning for Security in the Life Cycle

- Acronym List
- Definitions
- References
- Requirements Traceability Matrix
- System Security Policy
- System Rules of Behavior
- Security Operating Procedures
- NIACAP Work Plan

**Certification
Requirements Review
Meeting**

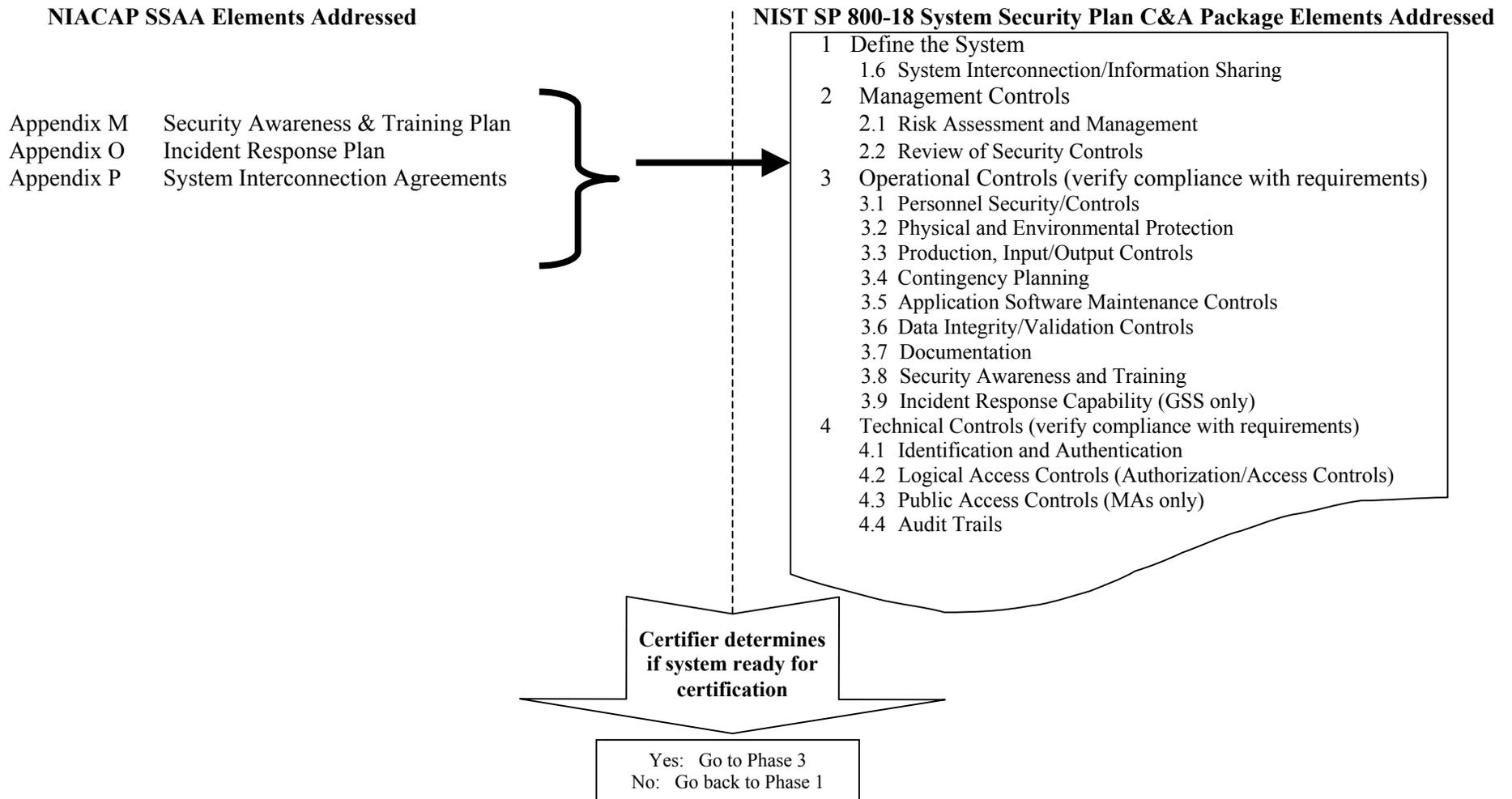
Yes: Go to Phase 2
No: Go back to Phase 1

Certification and Accreditation Phase 2: Controls Verification in System Development*

***Important Note:** Phase 2 is ordinarily for systems under development; however, if a system is already operational and has not yet been certified, many of the Phase 2 steps will need to be accomplished (such as Risk Assessment, verification of security controls for compliance with system security requirements, and finalizing the system security plan).

Roles and Responsibilities:

- DAA monitors system certification team progress according to NIACAP Work Plan.
- System Certifier/team verifies compliance of security plan to system security requirements; assesses vulnerabilities; review Rules of Behavior and Security Operating Procedures; finalizes security plan and generates appendices as needed.
- ITSO and ISSOs assist DAA and system certifier.



Certification and Accreditation Phase 3: Controls Validation Before System Operation

Roles and Responsibilities:

- DAA accredits system for processing.
- System Certifier/team: conducts security test and evaluation of operational controls documented in the security plan finalized at the end of Phase 2 (performs analysis of IT security program management, performs site evaluation, evaluates contingency plan, analyzes results of risk assessment, and develops risk management strategy); performs penetration testing of technical controls documented in the security plan; and provides DAA written certification recommendation along with certification package (approved security plan and appendices).
- ITSO and ISSOs assist DAA and system certifier.

NIACAP SSAA Elements Addressed

- Appendix E Security Test and Evaluation Plan and Procedures
- Appendix F Certification Results
- Appendix G Risk Assessment Results
- Appendix H Certifier’s Recommendation
- Appendix L Contingency Plan(s)
- Appendix N Personnel Controls and Technical Security Controls
- Appendix Q Applicable System Development Artifacts or System Documentation
- Appendix R Accreditation Documentation and Accreditation Statement

NIST SP 800-18 System Security Plan C&A Package Elements Addressed

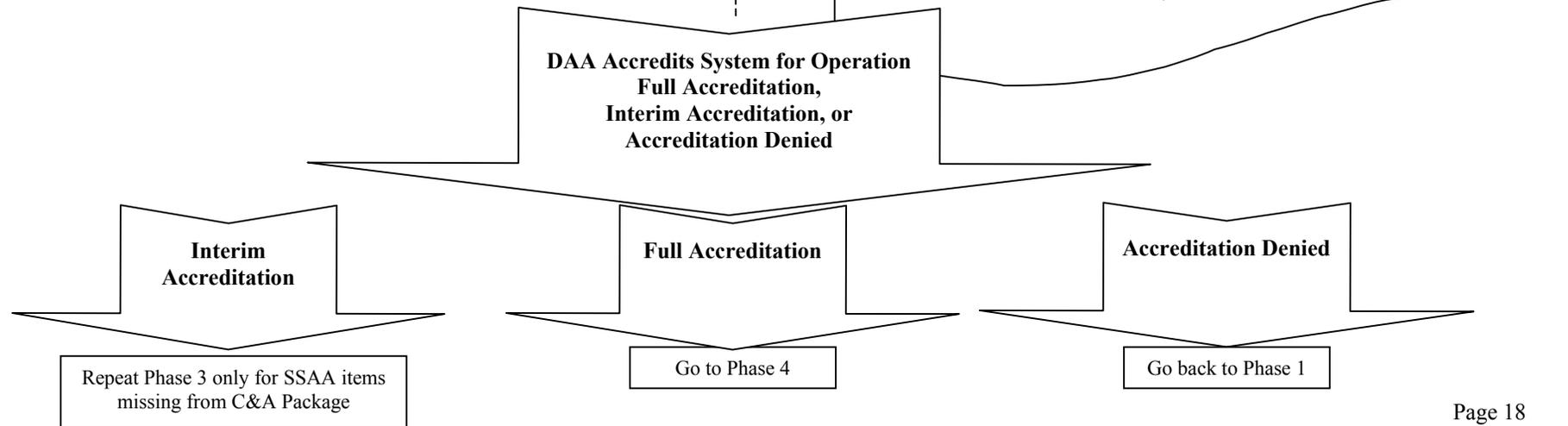
TEST THE OPERATIONAL AND TECHNICAL CONTROLS DOCUMENTED IN THE FINALIZED SECURITY PLAN

- > Perform security test & evaluation to validate operational controls are in place and effective
- > Perform penetration testing of technical controls to validate they are in place and functioning as intended

- 2 Management Controls
 - 2.5 Authorize Processing

Add necessary appendices to final Security Plan C&A Package:

- Contingency plan, risk assessment mitigation strategy, security test and evaluation plan and certification test results; Certifier’s recommendation, accreditation statement



Certification and Accreditation Phase 4: Post Accreditation Controls Monitoring

Roles and Responsibilities:

- DAA performs ongoing risk management reviews of security controls and adequacy of system security plan; initiates recertification upon every major system modification or at least every 3 years.
- System Certifier/team for this certification project disbands.
- ITSO assists DAA in ongoing review and testing of security controls.

NIACAP SSAA Elements Addressed

No changes to SSAA documentation unless approved by DAA

Review physical, personnel, and management controls

Maintain/test contingency plan

Follow change management procedures

Review system security management

Perform risk management review

NIST SP 800-18 System Security Plan C&A Package Elements Addressed

No changes to Security Plan documentation unless approved by DAA through established change management procedures

Perform periodic reviews of security controls

DAA determines recertification necessary due to major modification
-or-
DAA determines it has been at least 3 years since last certification/recertification

If Yes: Go to Phase 1