



DoD O-8530.1-M

**DEPARTMENT OF DEFENSE
COMPUTER NETWORK DEFENSE (CND) SERVICE
PROVIDER CERTIFICATION AND
ACCREDITATION PROCESS**

PROGRAM MANUAL

December 17, 2003

**Assistant Secretary of Defense for
Networks and Information Integration
(ASD(NII))/DoD CIO**

FOR OFFICIAL USE ONLY



OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

NETWORKS AND INFORMATION
INTEGRATION

December 17, 2003

FOREWORD

This Manual is issued under the authority of DoD Directive O-8530.1, "Computer Network Defense (CND)," January 8, 2001. It provides direction to the DoD Components for obtaining Certification and Accreditation (C&A) of their Computer Network Defense Services (CNDS).

This Manual applies to the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (hereafter referred to collectively as "the DoD Components"), all DoD-owned or -controlled information systems that receive, process, store, display or transmit DoD information, regardless of mission assurance category, classification or sensitivity, including but not limited to:

DoD information systems that support special environments, e.g., Special Access Programs (SAP) and Special Access Requirements (SAR), as supplemented by the special needs of the program, platform IT interconnections, e.g., weapons systems, sensors, medical technologies or utility distribution systems, external networks, information systems under contract to the Department of Defense, outsourced information-based processes such as those supporting e-Business or e-Commerce processes, information systems of Nonappropriated Fund Instrumentalities, stand-alone information systems, mobile computing devices such as laptops, handhelds, and personal digital assistants operating in either wired or wireless mode, and other information technologies as may be developed.

Nothing in this manual shall alter or supercede the existing authorities and policies of the Director of Central Intelligence (DCI) regarding the protection of Sensitive Compartmented Information (SCI) and special access programs for intelligence as directed by Executive Order 12333 and other laws and regulations.

This manual does not apply to weapons systems as defined by DoD Directive 5137.1 including components, both hardware and software, that are physically part of, dedicated to, or essential in real time to a weapon system's mission performance where no IT interconnection to a DoD GENSER or Special Enclave network is present.

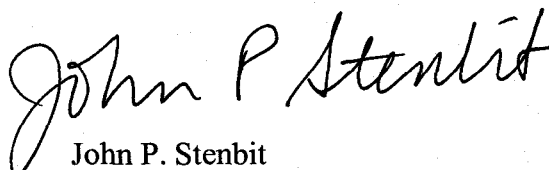
This manual is effective immediately and is mandatory for use by all the DoD Components.

Send recommended changes to this Manual to:

Defense Information Systems Agency
Attn: OP53/Plans and Standards
DISA Headquarters Bldg 12
701 South Courthouse Road



The DoD Components may obtain copies of this Manual through their own publications channels. Approved for release to DoD Components; distribution limited. Authorized registered users may obtain copies of the publication from the Defense Technical Information Center, 8725 John J. Kingman Road, Fort Belvoir, VA 22060-6218. Other Federal Agencies may obtain copies from the U.S. Department of Commerce, National Technical Information Service, 5285 Port Royal Road, Springfield, VA 22161. Copies are also available via controlled Internet access only at: <https://powhatan.iii.e.disa.mil/index2.html>.



John P. Stenbit
Department of Defense
Chief Information Officer

TABLE OF CONTENTS

	<u>Page</u>
FOREWARD	2
TABLE OF CONTENTS	4
FIGURES	6
REFERENCES	7
ABBREVIATIONS AND/OR ACRONYMS	8
C1. CHAPTER 1 - INTRODUCTION	9
C1.1. BACKGROUND	9
C1.2. CNDS C&A OBJECTIVES	10
C1.3. APPLICABILITY AND SCOPE	10
C2. CHAPTER 2 - C&A PROCESS	13
C2.1. C&A PROCESS OVERVIEW	13
C3. CHAPTER 3 - PHASE 1 REGISTRATION	15
C3.1. PHASE 1 ACTIVITIES	15
C4. CHAPTER 4 - PHASE 2 VERIFICATION	19
C4.1. PHASE 2 ACTIVITIES	19
C5. CHAPTER 5 - PHASE 3 VALIDATION	21
C5.1. PHASE 3 ACTIVITIES	21
C6. CHAPTER 6 - PHASE 4 POST ACCREDITATION	26
C6.1. PHASE 4 ACTIVITIES	26
C7. CHAPTER 7 - CNDS C&A MANAGEMENT	28
C7.1. ROLES AND RESPONSIBILITIES	28
APPENDICES	31

AP1. APPENDIX 1 - DEFINITIONS	31
AP2. APPENDIX 2 - APPLICATION PACKAGE DOCUMENTATION	36
AP3. APPENDIX 3 - LETTER OF REQUEST	41

FIGURES

<u>Figure</u>	<u>Title</u>	<u>Page</u>
C1.F1.	CNDS Evaluation Framework	11
C2.F1.	Phased Approach for CNDS C&A	13
C3.F1.	Registration Phase Process	18
C4.F1.	Verification Phase Process	20
C5.F1.	Validation Phase Process	25
C6.F1.	Post Accreditation Phase Process	27

REFERENCES

- (a) DoD Directive O-8530.1, "Computer Network Defense (CND)," January 8, 2001
- (b) DoD Instruction O-8530.2, "Support to Computer Network Defense (CND)," March 9, 2001
- (c) Executive Order 12333, "United States Intelligence Activities," December 4, 1981
- (d) DoD Directive 5137.1, "Assistant Secretary Of Defense For Command, Control, Communications, And Intelligence (ASD(C3I))," February 12, 1992
- (e) DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)," December 30, 1997

AL1. ABBREVIATIONS AND ACRONYMS

AL1.1.	<u>AA</u>	Accrediting Authority
AL1.2.	<u>AS&W</u>	Attack Sensing and Warning
AL1.3.	<u>C&A</u>	Certification & Accreditation
AL1.4.	<u>CERT</u>	Computer Emergency Response Team
AL1.5.	<u>CIRT</u>	Computer Incident Response Team
AL1.6.	<u>CND</u>	Computer Network Defense
AL1.7.	<u>CNDS</u>	Computer Network Defense Services
AL1.8.	<u>CNDS/CA</u>	Computer Network Defense Services Certification Authority
AL1.9.	<u>CNDS/PM</u>	Computer Network Defense Services Program Manager
AL1.10.	<u>C/S/A</u>	Combatant Command/Service/Agency
AL1.11.	<u>DISA</u>	Defense Information Systems Agency
AL1.12.	<u>DITSCAP</u>	DoD Information Technology Security Certification and Accreditation Process
AL1.13.	<u>DoD</u>	Department of Defense
AL1.14.	<u>DoDI</u>	Department of Defense Instruction
AL1.15.	<u>ESM</u>	Evaluator's Scoring Metrics
AL1.16.	<u>ETA</u>	Education, Training and Awareness
AL1.17.	<u>GENSER</u>	General Service
AL1.18.	<u>I&W</u>	Indications and Warning
AL1.19.	<u>IA</u>	Information Assurance
AL1.20.	<u>IASE</u>	Information Assurance Support Environment
AL1.21.	<u>IATO</u>	Interim Approval to Operate
AL1.22.	<u>IAVA</u>	Information Assurance Vulnerability Alert
AL1.23.	<u>IAVM</u>	Information Assurance Vulnerability Management
AL1.24.	<u>INFOCON</u>	Information Operations Condition
AL1.25.	<u>IS</u>	Information System
AL1.26.	<u>IT</u>	Information Technology
AL1.27.	<u>INFOSEC</u>	Information Systems Security
AL1.28.	<u>MOU</u>	Memorandum of Understanding
AL1.29.	<u>NIACAP</u>	National Information Assurance Certification and Accreditation Process
AL1.30.	<u>NIST</u>	National Institute of Standards and Technology
AL1.31.	<u>NSA</u>	National Security Agency
AL1.32.	<u>NSTISSD</u>	National Security Telecommunications and Information Systems Security Directive
AL1.33.	<u>NSTISSI</u>	National Security Telecommunications and Information Systems Security Instruction
AL1.34.	<u>POC</u>	Point of Contact
AL1.35.	<u>SAP</u>	Special Access Program
AL1.36.	<u>SAR</u>	Special Access Requirement
AL1.37.	<u>SOP</u>	Standard Operating Procedure
AL1.38.	<u>USSTRATCOM</u>	United States Strategic Command
AL1.39.	<u>VAA</u>	Vulnerability Analysis and Assessment

C1. CHAPTER 1

INTRODUCTION

C1.1. BACKGROUND

C1.1.1. By the authority of DoD Directive O-8530.1, "Computer Network Defense (CND)," and DoD Instruction O-8530.2, "Support to Computer Network Defense" (references (a) and (b)), the DoD Components shall establish or provide for Computer Network Defense Services (CNDS). These policies direct United States Strategic Command (USSTRATCOM) for supporting and coordinating the planning and execution of CND, developing national requirements for CND, and serving as the Accrediting Authority (AA) for the CNDS Certification Authorities (CNDS/CA). DoD CND policies mandate all owners of DoD information systems and computer networks enter into a service relationship with a CNDS Provider.

C1.1.2. Reference (a) establishes the CND Operational Hierarchy and the CNDS C&A process. The Department of Defense requires a CND capability that can quickly adapt to near-term changes and continuously evolve to meet long range threat and technology trends. Additionally, the Department of Defense requires a CND capability that unites all Components under the coordination and direction of a single lead, the USSTRATCOM, to conduct multi-Component and Defense-wide CND operations. The CNDS C&A Process is an integral element in fulfilling this requirement by providing a methodology to certify and accredit the performance and capabilities of Component-wide Primary CNDS Providers who support and provide protection for DoD IT systems.

C1.1.3. Under the CND Operational Hierarchy, the CNDS C&A process is designed to certify and accredit CNDS providers and further enhance the security of DoD IT systems that are certified and accredited under DoDI 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)." To ensure the effective implementation of the CND Operational Hierarchy and delivery of CNDS to all DoD IT systems, DoD Components will:

C1.1.3.1 Ensure that all Component information systems and computer networks are supported by a CNDS certified and accredited provider, and that support is established as a condition of system accreditation in accordance with DoDI 5200.40.

C1.1.3.2. Ensure that all Component-established CND Services are certified and accredited.

C1.1.4 DoD Components must appoint a Primary CNDS Provider (hereafter referred to as "Provider") as the focal point for implementing and conducting Component-wide CNDS. Where CNDS for a Component are distributed among multiple providers, support providers will assist the primary provider in coordination and integration of Component CNDS. Providers shall be certified and accredited to deliver, coordinate, and/or manage CNDS throughout their subscriber networks.

C1.1.5. This Manual shall assist Providers with their efforts in obtaining C&A for CNDS. This Manual provides standardized activities leading to accreditation and defines the CNDS C&A process. Copies of this manual are available via controlled Internet access only at: <https://powhatan.iie.disa.mil/index2.html>.

C1.1.6. This Program Manual provides an overview and procedures for the DoD CNDS C&A process. Chapter 1 introduces the CNDS C&A program and Chapter 2 is a brief overview of the entire process. Chapters 3 through 6 of this guidance describe each phase of the C&A process and clarify the actions necessary for obtaining accreditation. A diagram at the end of each process phase depicts the responsibilities of the relevant organizations throughout the CNDS C&A process. Chapter 7 of this document defines specific roles and responsibilities for management of the C&A process. The terms used in this manual are defined in Appendix 1. Appendix 2 contains an itemized list of essential documentation supporting the initiation of the C&A process. Appendix 3 contains a template for the Letter of Request that is submitted with the Provider's Application Package.

C1.1.7. This Program assures increased defensive services across the DoD enterprise. In the DoD net-centric environment, any vulnerability in the enterprise is a shared vulnerability. Conversely, enterprise-wide defensive standards ensure a shared, robust defense in a net-centric environment.

C1.2. CNDS C&A OBJECTIVES

C1.2.1. The primary goal of the CNDS C&A process is assessing the performance of Providers to advance CNDS execution and delivery. A secondary goal is increasing awareness, understanding and coordination of CNDS to facilitate information sharing and exchange among all Providers. The C&A evaluation process incorporates an approach for assessing mission effectiveness and operational performance against a number of critical success factors. These factors include:

C1.2.1.1. CNDS mission accountability.

C1.2.1.2. CNDS capability development and process improvements.

C1.2.1.3. CNDS performance measurement for requirements planning and as input for future capability investments.

C1.2.1.4. Support of the legislative requirements of both Subtitle III of Title 40 of the United States Code (formerly the Clinger-Cohen Act) and the Federal Information Security Management Act of 2002 (FISMA)(Chapter 35 of Title 44, United States Code).

C1.3. APPLICABILITY AND SCOPE

C1.3.1. C&A is required for all Component-established CNDS. This Manual and the process identified herein apply to all DoD Providers responsible for CNDS throughout their

Component information systems and networks. The three primary CNDS areas of Protect, Monitor, Analyze and Detect, and Respond are depicted in Figure C1.F1. These services include actions employed for preventing or mitigating computer network attacks that may cause disruption, denial, degradation, destruction, exploitation, or access to computer networks, information systems or their contents, or the theft of information. Capability Sustainment reflects those areas that the CNDSP must perform internally to sustain their ability to provide services to subscribers. The CNDS Evaluation Framework includes the three primary CNDS areas and Capability Sustainment.

Figure C1.F1. CNDS Evaluation Framework

COMPUTER NETWORK DEFENSE SERVICES			
PROTECT	MONITOR, ANALYZE & DETECT	RESPOND	CAPABILITY SUSTAINMENT
Vulnerability Analysis and Assessment (VAA) Support CND Red Teaming Virus Protection Support Subscriber Protection Support and Training Information Operations Condition (INFOCON) Implementation Information Assurance Vulnerability Management (IAVM)	Network Security Monitoring/Intrusion Detection Attack Sensing & Warning (AS&W) Indications & Warning (I&W) / Situational Awareness	Incident Reporting Incident Response Incident Response Analysis	MOUs and Contracts CND Policies/Procedures CND Technology Development, Evaluation and Implementation Personnel Levels and Training/Certification Security Administration Primary CNDS Provider Information Systems

C1.3.2. Special Enclave/General Service (GENSER) Designation. For the purposes of CND, all DoD information systems and computer networks are classified at one of two security levels, Special Enclave or GENSER. CNDS must be provided and certified at one or both of these security levels, depending upon the classification of the enclaves defended.

C1.3.2.1. Special Enclave. Special Enclaves are those DoD information systems and/or networks with special security requirements (e.g., Special Access Programs (SAP), Special Access Requirements (SAR)). Special Enclave systems and networks shall be assigned to certified Providers for Special Enclave Services.

C1.3.2.1.1. The National Security Agency (NSA) shall function as the CNDS/CA for the CNDS Providers to Special Enclave computer networks or systems.

C1.3.2.1.2. The Provider is accountable for ensuring Component-wide delivery of CNDS to Special Enclaves. The Provider must also be aware of other organization(s) providing CNDS to Special Enclave networks within the Component.

C1.3.2.2. General Service. General Service (GENSER) are those DoD information systems or computer networks (e.g., NIPRNET and SIPRNET) not otherwise specifically designated as a Special Enclave because of special security requirements. GENSER systems and networks shall be assigned to certified Providers for GENSER Services.

C1.3.2.2.1. The Defense Information Systems Agency (DISA) shall function as the CNDS/CA for the CNDS Providers to GENSER computer networks or systems.

C1.3.3. Dual GENSER/Special Enclave C&A. Providers overseeing both GENSER and Special Enclaves shall be evaluated and certified at each security level. The C&A process defined within this Manual applies equally to GENSER and Special Enclave Providers. However, when initiated, the entire C&A process shall occur separately for each security level due to security considerations. Providers undergoing dual GENSER and Special Enclave C&A must be aware of the following guidelines:

C1.3.3.1. Application packages must be submitted individually for GENSER and Special Enclave CNDS.

C1.3.3.2. Separate evaluation teams shall perform each assessment using the Evaluator's Scoring Metrics (ESM). The ESM is organized based on the CNDS Evaluation Framework depicted in Figure C1.F1. Individual reports shall be generated for each evaluation. DISA is responsible for GENSER evaluations, while NSA is responsible for Special Enclave evaluations.

C1.3.3.3. Each security level shall be certified and accredited separately.

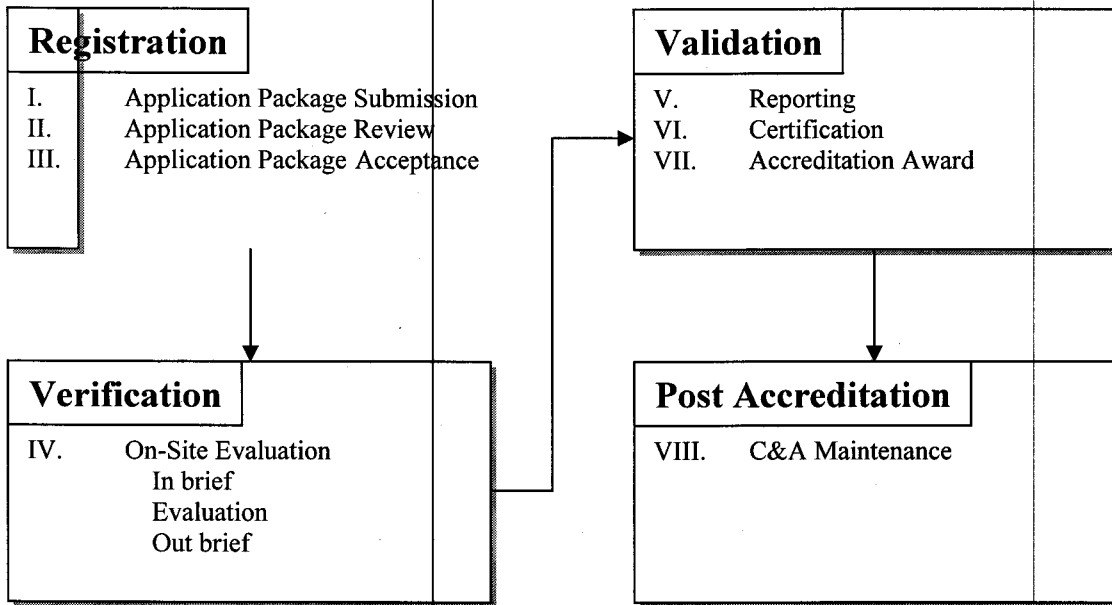
C2. CHAPTER 2

CNDS C&A PROCESS

C2.1. CNDS C&A PROCESS OVERVIEW

C2.1.1. The CNDS C&A process is based on a four-phase approach ultimately leading to accreditation. The process provides DoD with a standardized means to assess a Provider's level of capability based on identified performance criteria (Information Assurance (IA) best practices, self-assessment tools, and DoD requirements). The phases include Registration, Verification, Validation, and Post Accreditation. Figure C2.F1 depicts each process phase and the functional steps leading to a successful accreditation.

Figure C2.F1. Phased Approach for CNDS C&A



C2.1.1.1. **Phase 1, Registration.** The Registration Phase initiates the CNDS C&A process. The Provider submits the application package to the DoD CND Architect. This package is reviewed by both the CND Architect and the relevant CNDS/CA(s) to determine if the Provider is ready for C&A. Each CNDS/CA shall select and prepare an evaluation team and coordinate with the Provider to schedule the evaluation visit.

C2.1.1.2. **Phase 2, Verification.** The Verification Phase includes activities related to the on-site C&A evaluation. The evaluation team assesses the Provider, along with any additional CNDS organizations under the purview of that Provider. After the on-site evaluation, the evaluation team shall provide an out brief to the Provider.

C2.1.1.3. **Phase 3, Validation.** In the Validation Phase, the evaluation team prepares a Deficiency Report and a Certification Report for CNDS/CA review. The CNDS/CA reviews the

Deficiency Report and then forwards it to the Provider. The CNDS/CA reviews the Certification Report, makes a certification determination, and then forwards the Certification Report and an appropriate recommendation for accreditation to the CND Architect. The CND Architect shall review the CNDS/CA's findings and decide on a final accreditation recommendation to the AA. Validation culminates with an accreditation decision by the AA to the Component.

C2.1.1.4. Phase 4, Post Accreditation Phase. The Post Accreditation Phase includes activities by the Provider to maintain C&A status, monitor changes to the CNDS mission, and prepare and apply for recertification. Periodic self-assessments shall be conducted during this phase. Recertification is required every three years or when there is a significant change to CNDS Provider operations, policies and procedures, and performance levels.

C3. CHAPTER 3

PHASE 1 REGISTRATION

C3.1. PHASE 1 ACTIVITIES

C3.1.1. Phase 1 consists of three activities: Application Package Submission, Application Package Review and Application Package Acceptance. These activities compile the information necessary for identifying the Primary Provider organization, the CNDS provided, and commencing the C&A process. Figure C3.F1 depicts the Registration Phase Process.

C3.1.2. Application Package Submission. The Provider submits a formal application package to the CND Architect. The application package contains a Letter of Request for C&A and all documentation applicable to Provider operations and this process. Appendix 2 of this Program Manual details a checklist of documentation and information necessary for developing the CNDS application package. The Provider shall submit all unclassified documentation (to include items marked FOUO) in electronic format, preferably compact disk (CD), along with a hardcopy of the Letter of Request. For documentation listed in Appendix 2 which is classified, the Provider shall submit a Point of Contact (POC) with phone number and e-mail address that shall provide the information, when requested.

C3.1.2.1. The Letter of Request shall be submitted in writing and be signed by the appropriate Component's Primary Provider Commander or Director. The Letter of Request designates the applicant as the Component's Primary Provider and requests entry into the C&A process. The Letter of Request must identify the Component's Primary Provider organization and any sub-units including primary and alternate POCs, phone numbers, and e-mail addresses. Appendix 3 includes an example of a Letter of Request.

C3.1.2.2. The documents collected for the application package are the focal point for identifying, characterizing, analyzing, and assessing the Provider for C&A. The application package must contain information required to evaluate the delivery of CNDS and provide specific information pertaining to organizational capabilities and attributes. A complete application package shall ensure greater success for C&A.

C3.1.2.2.1. Providers should be familiar with DoD Directive O-8530.1 and DoD Instruction O-8530.2, which provide CND policy and guidance.

C3.1.2.2.2. The Evaluator's Scoring Metrics (ESM) and this Manual establish the foundation of the C&A evaluation process. Providers should have detailed knowledge of these publications before submitting an application package. The ESM are maintained separately from this manual and shall be updated at least annually. This provides the agility to ensure a timely update and implementing of metrics reflecting new and emerging policies, best practices and technologies in a dynamic and maturing CNDS environment. The ESM are available at the Information Assurance Support Environment (IASE) website located at: <https://powhatan.iie.disa.mil/index2.html>.

C3.1.2.2.3. The change management process for ESM updates begins no later than 10 months following the date of the current ESM. The process may begin earlier if the DoD CND Architect, in consultation with the GENSER and Special Enclave CAs, determines an early update is warranted. All packages currently in progress may be grandfathered to follow the previous ESM version. The change management process entails:

C3.1.2.2.3.1. Assembling a working group for reviewing the metrics against past CNDS evaluations, new policies, procedures, and best practices for developing suggested changes.

C3.1.2.2.3.2. Staffing the revised ESM via the IASE website for DoD Component comment.

C3.1.2.2.3.3. Posting the new ESM version next to the previous version on the IASE website showing notification of a new version for all self assessments. Additionally, the DoD Component's Primary Providers shall be notified by e-mail when a new ESM is posted.

C3.1.2.3. Component CNDS C&A information shall be maintained in a CNDS/CA documentation repository. The CNDS/CA's documentation repository shall be used for supporting CNDS/CA program management, enhancing the C&A process, developing CNDS training and tracking Component improvement in the delivery of CNDS. Third party dissemination of Provider information and documentation is prohibited without authorization from the originating Provider.

C3.1.2.4. Documentation shall be handled at the appropriate classification and/or sensitivity level by all parties involved in the C&A process.

C3.1.3. Application Package Review. The CND Architect receives, registers, and reviews the application package, then forwards a copy to each of the two CNDS/CA(s), as appropriate. Then the CND Architect designates one of the two CNDS/CA(s) to direct the remainder of the C&A process.

C3.1.3.1. CNDS/CA Review. The CNDS/CA(s) shall assign evaluators to review, analyze and discuss all furnished documentation. The number of evaluators assigned shall vary depending on the organization size and the scope of services being evaluated. Evaluators shall be selected based on their knowledge, skill, and ability. Evaluators shall be capable of identifying deviations from performance criteria and providing guidance and recommendations to applicant questions or concerns.

C3.1.3.1.1. Evaluators shall be cleared for the classification of the data handled.

C3.1.3.1.2. If an application package contains insufficient documentation, the lead CNDS/CA shall coordinate with the Provider to resolve any discrepancies.

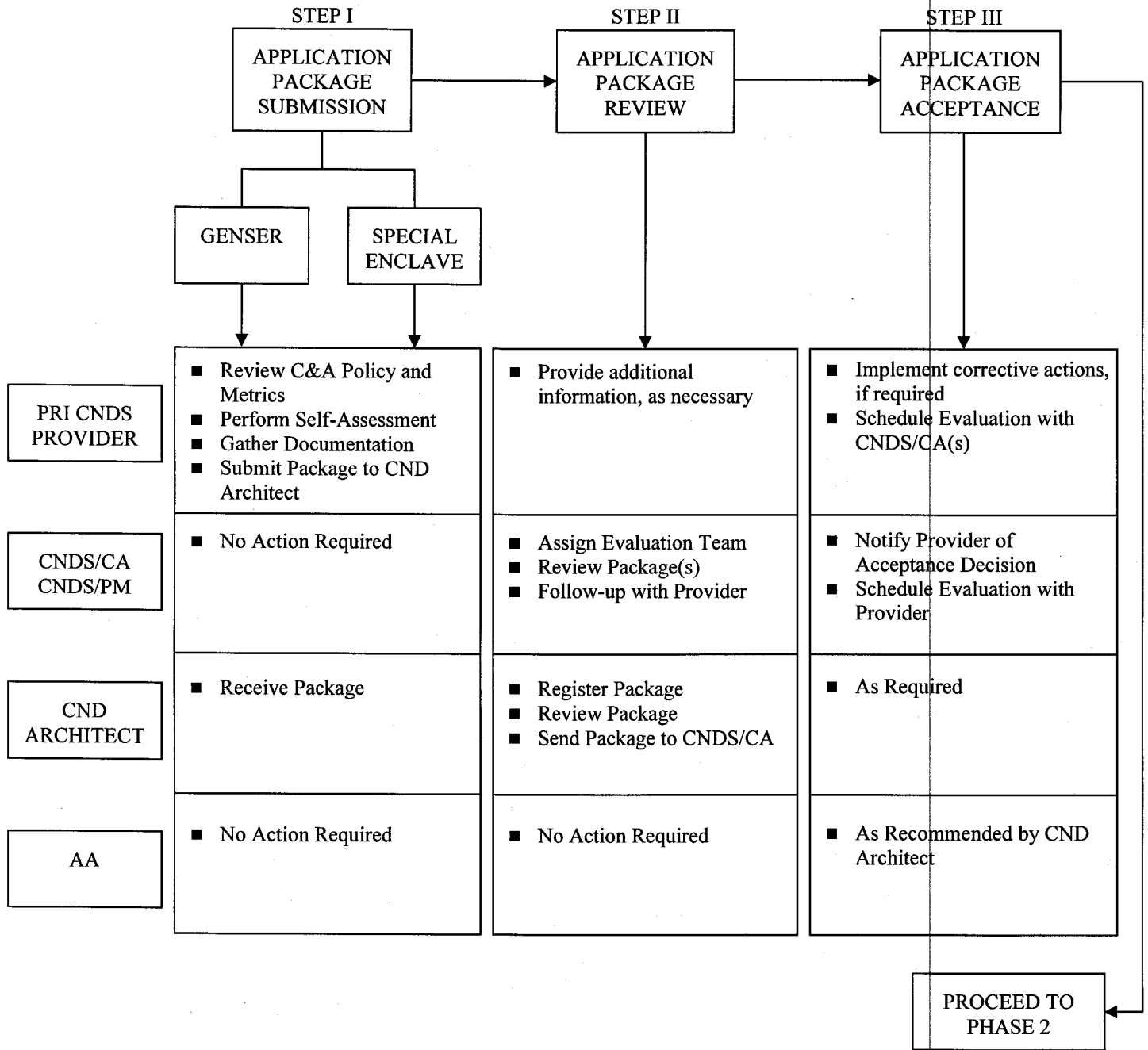
C3.1.4. Application Package Acceptance. Phase 1 concludes with the acceptance of the application package by the CNDS/CA and the CND Architect. If the Provider's package is

accepted, the CNDS/CA shall continue the C&A process. The CNDS/CA shall coordinate with the Provider to schedule the on-site evaluation.

C3.1.4.1. The CNDS/CA may require Providers to implement corrective actions regarding the self-assessment results and specific performance metrics before the on-site evaluation. This allows the Provider sufficient opportunity for correcting actions or developing justification(s) for deviating from expected standards identified in the ESM.

C3.1.4.2. In some cases, because of the review of the application, the CNDS/CA may determine the Provider shall not be able to attain C&A. When this occurs the CNDS/CA shall provide justification to the DoD CND Architect. The DoD CND Architect shall then determine appropriate actions based on the circumstances.

Figure C3.F1. Registration Phase Process



C4. CHAPTER 4

PHASE 2 VERIFICATION

C4.1. PHASE 2 ACTIVITIES

C4.1.1. Phase 2 consists of the on-site evaluation. The evaluation activity verifies the Provider is performing at a level consistent with CNDS certification standards (i.e., the ESM). Evaluation activities are dependent on the types of enclaves (Special Enclave, GENSER, or both) under the Provider's purview. Figure C4.F1 depicts the Verification Phase Process.

C4.1.2. On-site Evaluation. The on-site evaluation determines if the Provider's procedures, processes, and operational activities meet C&A standards established in the ESM. Evaluation activities verify standards of performance within the scope of the Provider's mission through observation, interviews and/or demonstration of services. Evaluators compare these activities to the application package and documentation checklist to make a complete assessment of the Provider.

C4.1.2.1. Evaluation Process. The evaluation may require one week to accomplish. The CNDS/CA and the evaluation team shall try to minimize impact to the Provider's normal operations. The team shall accomplish the following activities during the on-site evaluation:

C4.1.2.1.1. An in-brief with the Provider's senior management.

C4.1.2.1.2. Interviews of Provider personnel, utilizing the ESM.

C4.1.2.1.3. Observations of selected CNDS processes and procedures.

C4.1.2.1.4. Demonstrations of CNDS hardware and software utilities.

C4.1.2.1.5. Documenting, observing, and recommending CNDS best practices.

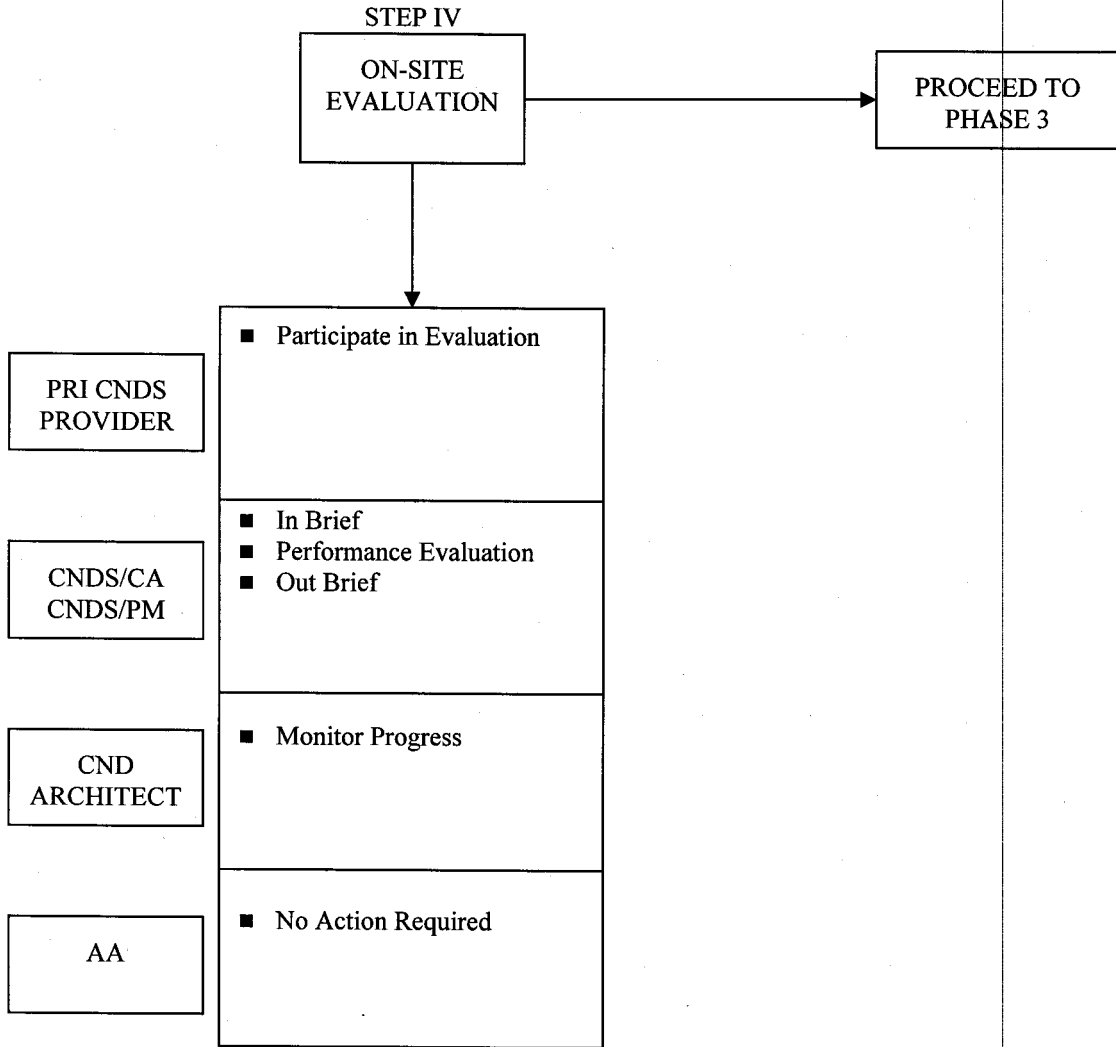
C4.1.2.1.6. An out-brief to Provider staff personnel and management.

C4.1.2.2. Evaluation Scoring. The evaluation teams shall utilize the ESM for assessing the Provider. Providers shall be evaluated against CNDS standards and best practices deemed crucial for success within the four CNDS areas: Protect; Monitor, Analyze & Detect; Respond; and Capability Sustainment. Performance is measured against a set of metrics ranging in priority from I through IV and assigned a point system.

C4.1.2.2.1. Priority I metrics are the most critical. Priority I metrics receive one point for full compliance or zero for non-compliance. These metrics are either "Pass" or "Fail"; no partial credit is awarded.

C4.1.2.2.2. Priority II – IV metrics address less critical CNDS factors, but are no less important than Priority I metrics. These metrics receive one point for full compliance, 0.3 points for partial compliance, or zero for non-compliance.

Figure C4.F1. Verification Phase Process



C5. CHAPTER 5

PHASE 3 VALIDATION

C5.1. PHASE 3 ACTIVITIES

C5.1.1. Phase 3 includes the following activities: Reporting, Certification and Accreditation Award. These activities certify the Provider complies with minimum CNDS performance standards and is awarded an accreditation level by the Accrediting Authority (USSTRATCOM). Figure C5.F1 depicts the Validation Phase Process.

C5.1.2. Reporting. The evaluation team prepares a Certification Report and a Deficiency Report for the enclave(s) evaluated.

C5.1.2.1. Certification Report. The Certification Report provides an overall assessment of CNDS capability and includes actions to refine Provider performance. The report contains ESM scores, observations of processes gathered during the evaluation, and identified deficiencies and recommendations. The Certification Report includes both commendable actions, and any weaknesses identified in mission capabilities, practices, and procedures. The report is forwarded to the CNDS/CA for review, endorsement and accreditation recommendation.

C5.1.2.1.1. A Certification Report shall be prepared for each security level (e.g., Special Enclave and/or GENSER) evaluated. Reports shall be classified and handled as required and distribution restricted on a "need to know" basis.

C5.1.2.2. Deficiency Report. The Deficiency Report is created by each CNDS/CA for the Provider. The report includes a detailed explanation of each deficiency identified by the evaluation team and corrective actions. The Provider utilizes the report for initiating CNDS improvements. A Deficiency Report shall be prepared for each security level evaluated and distribution restricted on a "need to know" basis.

C5.1.3. Certification. The CNDS/CAs review their respective Certification Report, then certify their assessment scores and results, and make an appropriate accreditation recommendation to the CND Architect.

C5.1.3.1. If the CNDS/CA determines that the Provider complies with the minimum performance requirements, the CNDS/CA issues a letter of certification along with a recommendation to accredit to the CND Architect. The CNDS/CA may also make supplemental recommendations to the Provider for process improvements.

C5.1.3.2. If the CNDS/CA concludes the Provider has not achieved minimum performance standards, the CNDS/CA shall deny certification. A letter of non-certification shall be issued to the CND Architect, including reasons that substantiate the decision. The Provider shall not be eligible for accreditation.

C5.1.3.3. The Certification Report, accompanying letter, CNDS/CA recommendation(s) and any supporting documentation shall be consolidated into an accreditation package, and submitted to the CND Architect for review and approval, or recommendation for an Interim Approval to Operate (IATO).

C5.1.3.3.1. If the CNDS/CA certifies the Provider, the CND Architect shall review the accreditation package and submit the package, including an accreditation recommendation, to the AA for review and final decision.

C5.1.3.3.2. If the CNDS/CA does not certify the Provider, the CND Architect shall recommend that the AA grant an IATO to the Provider.

C5.1.4. Accreditation Decision. After receipt and review of the accreditation package, the AA, USSTRATCOM, makes the final decision for the Accreditation award. Based upon the review of the accreditation package from the CND Architect, the AA shall award an IATO or one of three Accreditation Levels.

C5.1.4.1. IATO. If the AA elects to withhold accreditation and award an IATO, the decision shall include the specific reasons for accreditation denial and suggest possible solutions for the identified deficiencies. An IATO shall be awarded to any organization that fails to meet one or more of the minimum Priority percentages. The AA shall issue the IATO and explicit direction concerning compliance guidelines to the Provider.

C5.1.4.1.1. The IATO shall be granted for a maximum period of 180 days.

C5.1.4.1.2. The Provider shall submit a Provider Improvement Plan within 45 days of the IATO notification date.

C5.1.4.1.2.1. The Provider Improvement Plan shall include proposed resolution actions, schedules and milestones focusing on the shortfalls identified within the Deficiency Report.

C5.1.4.1.2.2. The CNDS/CA and the Provider must agree to all activities and schedules defined within the Provider Improvement Plan.

C5.1.4.1.3. The Provider shall be required to perform a self-assessment utilizing the ESM upon completion of deficiency resolution. The assessment results shall be provided to the CNDS/CA within 120 days of IATO notification and before any re-evaluation is scheduled.

C5.1.4.1.4. Corrective actions that cannot be implemented by the Provider shall be identified, to include rationale, in the Provider Improvement Plan submitted to the CNDS/CA and the CND Architect. The AA shall notify and involve the Headquarters Component of the required remediation support.

C5.1.4.1.5. The CNDS/CA and Provider shall schedule an evaluation within 150 days of the IATO notification date. The follow-on evaluation shall assess the resolution actions

applied by the Provider. The Provider shall be granted the appropriate level of accreditation upon determination by the CNDS/CA, CND Architect, and AA of a successful improvement effort.

C5.1.4.2. Level 1 Accreditation – Minimum Acceptable Performance. The AA shall award a Level 1 Accreditation to a Provider meeting the minimum percentages of compliance in all four Priority levels of the metrics within the ESM. Attaining all of the following minimum percentages shall result in a Level 1 Accreditation:

C5.1.4.2.1. Priority I Metrics – 90% compliance.

C5.1.4.2.2. Priority II Metrics – 75% compliance.

C5.1.4.2.3. Priority III Metrics – 50% compliance.

C5.1.4.2.4. Priority IV Metrics – 25% compliance.

C5.1.4.3. Level 2 Accreditation – Commendable Performance. The AA shall award a Level 2 Accreditation to a Provider achieving the following compliance percentages in all four Priority levels:

C5.1.4.3.1. Priority I Metrics – 95% compliance.

C5.1.4.3.2. Priority II Metrics – 90% compliance.

C5.1.4.3.3. Priority III Metrics – 75% compliance.

C5.1.4.3.4. Priority IV Metrics – 50% compliance.

C5.1.4.4. Level 3 Accreditation – Exemplary Performance. This level of accreditation shall recognize exemplary Provider performance. The AA shall award an Exemplary Performance Accreditation to a Provider achieving the following compliance percentages in all four Priority levels:

C5.1.4.4.1. Priority I Metrics – 100% compliance.

C5.1.4.4.2. Priority II Metrics – 100% compliance.

C5.1.4.4.3. Priority III Metrics – 90% compliance.

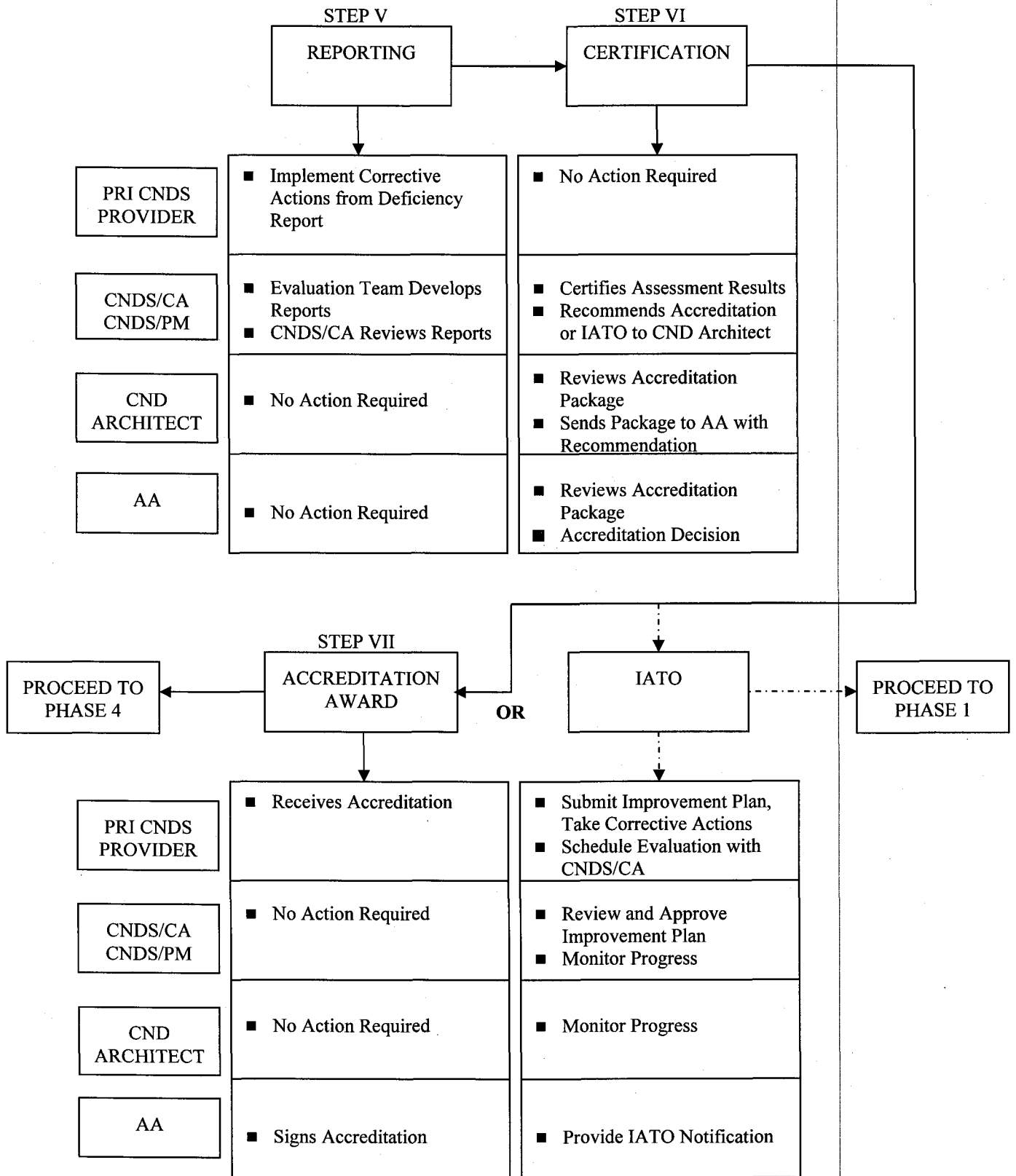
C5.1.4.4.4. Priority IV Metrics – 90% compliance.

C5.1.4.5. A final certification and accreditation decision shall be issued to the Provider by the AA. The decision shall contain all recommendations by the CNDS/CA(s), the CND Architect, and any supporting documentation. The C&A process now advances to Phase 4, Post-Accreditation.

C5.1.4.6. If the AA elects to withhold accreditation and issue an IATO to the Primary CNDS Provider, then that decision shall be issued to the Primary CNDS Provider by the AA and shall include the specific reasons for accreditation denial. The C&A process then reverts to Phase I and IATO actions shall commence, as described above.

C5.1.4.6.1. Under extreme circumstances, an extension of the initial IATO may be considered by the AA.

C5.F1. Validation Phase Process



C6. CHAPTER 6

PHASE 4 POST ACCREDITATION

C6.1. PHASE 4 ACTIVITIES

C6.1.1. Phase 4 consists of activities required to maintain the capability for providing CNDS in accordance with C&A standards. Post accreditation phase activities include maintaining of Provider operations, policies and procedures, and periodic self-assessments. Figure C6.F1 depicts the Post Accreditation Phase Process.

C6.1.2. Phase 4 begins when the Provider is accredited, and continues until a significant change in operations occurs or the accreditation period has expired. In both cases, the C&A process restarts at Phase I.

C6.1.3. C&A Maintenance. The Provider must maintain its capability for providing effective CNDS in accordance with Accreditation standards. The Provider shall accomplish this by sustaining current performance levels and closely monitoring for any changes that may significantly affect mission, personnel and/or performance.

C6.1.3.1. Self-assessments. The Provider shall perform periodic self-assessments utilizing the ESM. These evaluations are an effective means for monitoring performance and detecting both positive and negative changes in Provider operations.

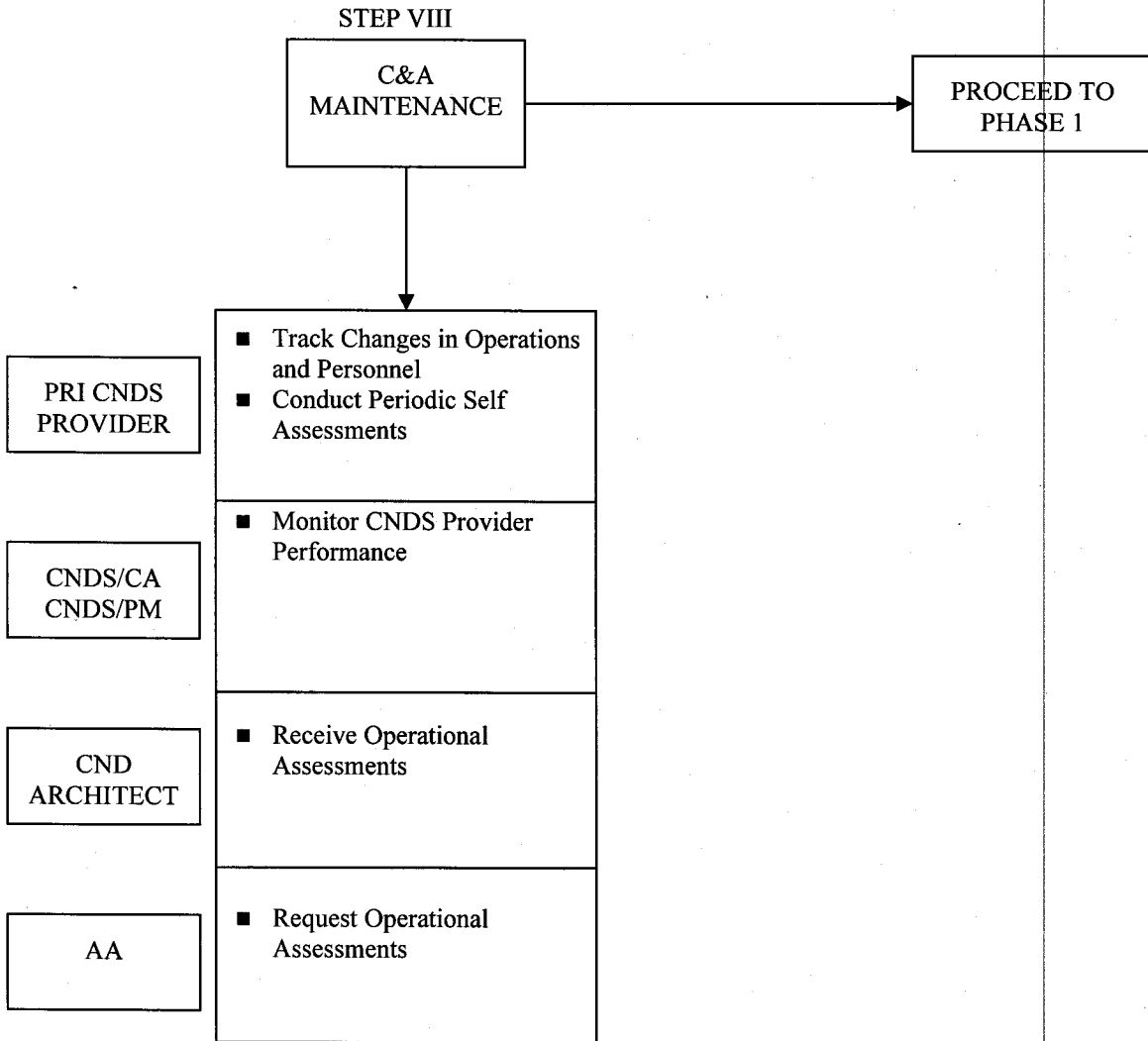
C6.1.3.2. Personnel. The Provider shall ensure operating policies and procedures are fully documented for maintaining performance levels and mitigating the turbulence caused by significant personnel turnover. Additionally, the Provider should continuously review their CNDS training program to ensure it sustains and improves CNDS skills, and trains personnel in the performance of their CNDS duties.

C6.1.3.3. Operations. Changes in the Provider's environment may significantly impact performance. The addition of new mission capabilities or requirements, an increase in the number of supported subscribers, and a dramatic increase in incidents and attempted intrusions are a few examples. The Provider should continuously assess the operational environment and be prepared to implement contingency plans facilitating a surge in CNDS support for meeting new operational challenges.

C6.1.3.4. Policies and Procedures. CND is dynamic by its nature. Providers must keep policies and procedures current with DoD guidance.

C6.1.4. Recertification. The Provider shall ensure recertification is performed at least every 3 years or when a significant change occurs in items mentioned above. Additionally, operational assessments and performance-based analysis may provide indications signaling a need for the AA to determine if a Provider's certification and accreditation status is being sustained.

C6.F1. Post Accreditation Phase Process



C7. CHAPTER 7

CNDS C&A MANAGEMENT

C7.1. ROLES AND RESPONSIBILITIES

C7.1.1. Key participants in the CNDS C&A Process are the CND Architect, the AA, the CNDS/CAs, Primary CNDS Providers, Heads of the Components, and CNDS Evaluators.

C7.1.2. DoD CND Architect. The DoD CND Architect, IA Directorate, ASD (NII), manages the overall CNDS C&A program for DoD. The DoD CND Architect shall:

C7.1.2.1. Oversee the establishment and implementation of the CNDS certification and accreditation process.

C7.1.2.2. Manage the Special Enclave designation process.

C7.1.2.3. Support and deconflict the roles and responsibilities among CNDS/CAs, Primary CNDS Providers, and DoD Components relevant to CNDS C&A.

C7.1.2.4. Ensure that CNDS C&A requirements are addressed and integrated into the DoD Information Technology Security Certification and Accreditation Process (DITSCAP), National Information Assurance Certification and Accreditation Process (NIACAP), and in information technology (IT) registration and configuration management guidance and systems.

C7.1.3. CNDS Accreditation Authority (AA). USSTRATCOM is the AA for CNDS. In its role as the AA, USSTRATCOM shall:

C7.1.3.1. In coordination with the DoD CND Architect, DISA and NSA, oversee the implementing and executing of the CNDS certification and accreditation process.

C7.1.3.2. Provide a periodic operational assessment of the DoD Components readiness for defending DoD information systems and computer networks, through the Chairman of the Joint Chiefs of Staff, to the Office of the Secretary of Defense.

C7.1.4. CNDS Certification Authorities (CNDS/CAs). DISA and NSA are designated CNDS/CAs for General Service and Special Enclaves respectively. The CNDS/CAs shall conduct CNDS certifications throughout the Department of Defense. The CNDS/CAs shall:

C7.1.4.1. In coordination with the CND Architect and USSTRATCOM, develop and implement the CNDS C&A program.

C7.1.4.2. Assist the DoD CND Architect in assessing the effectiveness and performance of Primary CNDS Providers.

C7.1.4.3. Monitor and advocate CNDS best practices and technical solutions by enhancing CND detection, protection, and response, and supporting the development of Primary CNDS Provider capabilities.

C7.1.4.4. Coordinate relevant CNDS issues and requirements between the DoD CND Architect and Primary CNDS Providers.

C7.1.4.5. Provide CNDS technical, analytical, and coordination support to Primary CNDS Providers relevant to C&A and this guidance.

C7.1.4.6. Advocate common CNDS policies, procedures, training, and information exchanges to support CNDS best practices.

C7.1.4.7. Develop, maintain, and update a CNDS C&A education, training, and awareness program.

C7.1.4.8. Monitor changes in Primary CNDS Provider certification status, Provider Improvement Plans, and conduct periodic CNDS recertification.

C7.1.4.9 Provide experienced technical members for supporting CNDS certification activities.

C7.1.5. CNDS Program Manager (PM). The CNDS/PMs support their respective CNDS/CA and the DoD CND Architect. The CNDS Program Manager(s) shall:

C7.1.5.1. Coordinate the planning, implementation, and delivery of support defined in this Manual and as directed by their respective CNDS/CA.

C7.1.5.2. In the execution of their responsibilities with respect to the CNDS C&A program, provide on-going Primary CNDS Provider interface in coordinating CNDS C&A activities.

C7.1.6. Primary CNDS Providers. Primary CNDS Providers are designated and authorized for executing, monitoring, and managing component-wide CNDS for both GENSER and Special Enclave security levels. Primary CNDS Providers shall:

C7.1.6.1. Achieve and maintain CNDS C&A in accordance with DoD requirements and this Manual.

C7.1.6.2. Notify the appropriate CNDS/CA when or if a change in certification status occurs.

C7.1.6.3. Ensure and maintain CNDS best practices, procedures, and technology consistent with the CNDS ESM.

C7.1.6.4. Maintain an inventory of all subscriber entities and associated information systems and computer networks.

C7.1.7. The Heads of DoD Components shall:

C7.1.7.1. Coordinate their CNDS activities and implement procedures in accordance with guidance issued by Commander, USSTRATCOM, DoD Directive O-8530.1 and DoD Instruction O-8530.2.

C7.1.7.2. Support and implement DoD-wide CND operational direction from USSTRATCOM.

C7.1.7.3. Designate the Component's Primary Provider for coordinating and directing Component-wide CNDS. Require the Primary CNDS Provider be certified and accredited in accordance with established DoD requirements and this Manual.

C7.1.7.4. Ensure that CNDS support is a condition of information and computer system IT security certification and accreditation.

C7.1.7.5. Ensure management of networks and CND operations are fully coordinated and integrated with the CNDS C&A process.

C7.1.7.6. Provide guidance on service arrangements with non-Component Primary CNDS Providers.

C7.1.7.7. In coordination with the CNDS/CAs, provide a coordinated and common DoD curriculum for CND education, training and awareness.

C7.1.7.8. Maintain an inventory of IT systems and networks accredited under DoDI 5200.40 and identify their Primary CNDS Providers.

C7.1.7.9. Support CND Architect and CNDS/CA sponsored activities and requests for information.

C7.1.8. CNDS Evaluators shall:

C7.1.8.1. Maintain the requisite knowledge and experience for applying the methods, procedures, and techniques identified in relevant DoD, NSTISSI, and public law for supporting CNDS certifications.

C7.1.8.2. Provide CNDS technical, analytical, and coordination support to Primary CNDS Providers relevant to C & A and this guidance.

C7.1.8.3. Review CNDS application packages and conduct on-site certification evaluations.

AP1. APPENDIX 1

DEFINITIONS

DL1.1.1. Accountability. Property shall allow auditing of IS activities for tracing to persons or processes that may be held responsible for their actions. Accountability includes authenticity and non-repudiation.

DL1.1.2. Accrediting Authority (AA). Official with the authority to formally approve a CNDS Provider's level of performance. USSTRATCOM is the AA for the CNDS C&A process.

DL1.1.3. Architecture. The configuration of any equipment or interconnected system or subsystems of equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information; includes computers, ancillary equipment, and services, including support services and related resources.

DL1.1.4. Assurance. Measure of confidence that security features, practices, procedures and architecture of an IS accurately mediates and enforces the security policy.

DL1.1.5. Attack Sensing and Warning (AS&W). The detection, correlation, identification and characterization of intentional unauthorized activity, including computer intrusion or attack, across a large spectrum coupled with the notification to command and decision-makers so that an appropriate response can be developed. AS&W also includes attack/intrusion related intelligence collection tasking and dissemination; limited immediate response recommendations; and limited potential impact assessments.

DL1.1.6. Audit. Independent review and examination of records and activities for assessing the adequacy of system controls, for ensuring compliance with established policies and operational procedures, and for recommending changes in controls, policies, or procedures.

DL1.1.7. CND Architect. Provides oversight and direction for the CNDS Provider certification and accreditation process. Oversees and coordinates Defense-wide CND activities related to the design and development of systems supporting the CND COP, the CND sensor grid, the deconfliction and integration activities of the CND Research and Technology Program Manager; and the establishment and certification of CNDS. The CND Architect facilitates the development of the CND aspects of the operational, systems and technical architecture views and ensures CND requirements are incorporated into the DoD C4ISR Architectural Framework and Joint Technical Architecture.

DL1.1.8. CND Services (CNDS). A DoD service provided or subscribed to by owners of DoD information systems and/or computer networks in order to maintain and provide CND situational awareness; implement CND protect measures; monitor and analyze in order to detect unauthorized activity; and implement CND operational direction.

DL1.1.9. CNDS Accreditation. Formal declaration by the AA that the Primary CNDS Provider operates at a level meeting or exceeding CNDS certification standards and is approved to provide CNDS in accordance with DoD Instruction (reference (b)).

DL1.1.10. CNDS Certification. An evaluation of the technical and non-technical services of a Primary CNDS Provider completed in support of the CNDS Accreditation process. The evaluation determines the extent a CNDS Provider performs specified CNDS criteria. The certification integrates CNDS standards, self and independent assessment processes, improvement methods and tools, and information exchange among the CNDS/CAs and CNDS Providers.

DL1.1.11. CNDS Certification Authority (CNDS/CA). The entities responsible for certifying Primary CNDS Providers, coordinating among supported CNDS Providers, and managing information dissemination supporting CND operations. DISA shall function as the CNDS/CA for General Service CNDS. NSA shall function as the CNDS/CA for Special Enclave CNDS.

DL1.1.12. CNDS Program Manager (CNDS/PM). Incumbents of this role ensure the optimum mix of cost, schedule, performance, and program supportability throughout the life cycle of the CNDS C&A program.

DL1.1.13. Computer Emergency Response Team/Computer Incident Response Team (CERT/CIRT). An organization chartered by an information systems owner to coordinate or accomplish necessary actions in response to computer emergency incidents that threaten the availability or integrity of its information systems.

DL1.1.14. Computer Network. Two or more computers connected with one another for the purpose of communicating data electronically. A computer network includes the physical connection of a variety of computers, communication devices and supporting peripheral equipment and a cohesive set of protocols that allows them to exchange information in a near-seamless fashion.

DL1.1.15. Computer Network Attack (CNA). Operations to disrupt, deny, degrade, or destroy information resident on computers and computer networks or the computers and networks themselves.

DL1.1.16. Computer Network Defense (CND). Actions taken to protect, monitor, analyze, detect and respond to unauthorized activity within DoD information systems and computer networks. NOTE: The unauthorized activity may include disruption, denial, degradation, destruction, exploitation, or access to computer networks, information systems or their contents, or theft of information. CND protection activity employs information assurance protection activity and includes deliberate actions taken to modify an assurance configuration or condition in response to a CND alert or threat information. Monitoring, analysis, detection activities, including trend and pattern analysis, are performed by multiple disciplines within the Department of Defense, e.g., network operations, CND Services, intelligence, counterintelligence, and law enforcement. CND response can include recommendations or

actions by network operations (including information assurance), restoration priorities, law enforcement, military forces and other US Government agencies.

DL1.1.17. Configuration Management. Management of security features and assurances through control of changes made to hardware, software, firmware, documentation, test fixtures, and test documentation throughout the life cycle of an Information System (IS).

DL1.1.18. DoD Information System. Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes AIS applications, enclaves, outsourced IT-based processes, and platform IT interconnections.

DL1.1.19. DoD Information Technology Security Certification and Accreditation Process (DITSCAP). The standard DoD process for identifying information security requirements, providing security solutions, and managing IS security activities.

DL1.1.20. Enclave. Collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security. Enclaves always assume the highest mission assurance category and security classification of the AIS applications or outsourced IT-based processes they support, and derive their security needs from those systems. They provide standard IA capabilities, such as boundary defense, incident detection and response, and key management, and also deliver common applications, such as office automation and electronic mail. Enclaves are analogous to general support systems as defined in OMB A-130. Enclaves may be specific to an organization or a mission, and the computing environments may be organized by physical proximity or by function independent of location. Examples of enclaves include local area networks and the applications they host, backbone networks, and data processing centers.

DL1.1.21. General Service (GENSER) Network or System. For the purposes of CND, all DoD information systems and computer networks are classified at one of two security levels, GENSER or Special Enclave. All DoD information systems and/or computer networks will be considered GENSER (e.g., NIPRNET & SIPRNET) unless designated as Special Enclave because of special security requirements.

DL1.1.22. Indications and Warning (I&W). Those intelligence activities intended to detect and report time sensitive intelligence information on foreign developments that could involve a threat to the United States or allied and/or coalition military, political, or economic interests or to US citizens abroad. It includes forewarning of enemy actions or intentions; the imminence of hostilities; insurgency; nuclear or non-nuclear attack on the United States, its overseas forces, or allied and/or coalition nations; hostile reactions to US reconnaissance activities; terrorists' attacks; and other similar events.

DL1.1.23. Information Assurance (IA). Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

DL1.1.24. Information Assurance Vulnerability Alert (IAVA). The comprehensive distribution process for notifying Combatant Commands, Services and Agencies (C/S/As) about vulnerability alerts and countermeasures information. The IAVA process requires C/S/A acknowledgment and provides specific time parameters for implementing appropriate countermeasures depending on the criticality of the vulnerability. The IAVA process is now referred to as Information Assurance Vulnerability Management (IAVM).

DL1.1.25. Information Operations Condition (INFOCON). The INFOCON is a defense posture and response system for DoD information systems and networks.

DL1.1.26. Information System Security (INFOSEC). Protection of ISs against unauthorized access to information, whether in storage, processing, or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats.

DL1.1.27. Information Technology (IT). Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information by the DoD Component. For purposes of the preceding sentence, equipment is used by a DoD Component if the equipment is used by the DoD Component directly or is used by a contractor under a contract with the DoD Component that (1) requires the use of such equipment, or (2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term "information technology" includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. Notwithstanding the above, the term "information technology" does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract.

DL1.1.28. Interim Approval to Operate (IATO). Temporary approval granted by the AA for a Primary CNDS Provider to deliver CND Services based on results of a C&A evaluation of the organization

DL1.1.29. Primary CNDS Providers. The organization(s) designated by a DOD Component to provide Component-wide monitoring of the GENSER and/or Component-owned Special Enclave CNDS within the Component. This is the organization that is certified and accredited by this Program for GENSER and Special Enclave CNDS, as appropriate. This organization may actually provide all the CNDS required for GENSER and Special Enclave information systems/networks, or may monitor/manage those CNDS that it conducts for the Component and CNDS provided by other DOD Component Primary Providers. Reference (b) allows for CNDS to be provided by another Component's CNDS Primary Provider. In such cases, this relationship must be formally established in writing. Any such arrangement must occur with a CNDS Primary Provider that is certified and accredited.

DL1.1.30. Provider Improvement Plan. Plan submitted by Primary CNDS Provider under IATO. Plan shall detail resolutions and schedules proposed by the Provider and shall be approved by the CNDS/CA.

DL1.1.31. Red Team. An independent threat based activity aimed at readiness improvements through simulation of an opposing force. Red teaming activity includes becoming knowledgeable of a target system, matching an adversary's approach, gathering appropriate tools to attack the system, training, launching an attack, then working with system owners to demonstrate vulnerabilities and suggest countermeasures.

DL1.1.32. Risk. A combination of the likelihood that a threat will occur, the likelihood that a threat occurrence will result in an adverse impact, and the severity of the resulting impact.

DL1.1.33. Security. Measures and controls that ensure confidentiality, integrity, availability, and accountability of the information processed and stored by a computer.

DL1.1.34. Security Requirements. Types and levels of protection necessary for equipment, data, information, applications, and facilities to meet security policy.

DL1.1.35. Special Enclave. DoD information systems and/or computer networks with special security requirements (e.g., Special Access Programs (SAP), Special Access Requirements (SAR)).

DL1.1.36. Support Provider. CNDS Providers not designated the primary provider in arrangements where CNDS for a Component are distributed among multiple providers. Support providers follow the direction of the primary provider in coordination and integration of Component CNDS.

DL1.1.37. Vulnerability Analysis and Assessment (VAA). In Information Operations, a systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

AP2. APPENDIX 2APPLICATION PACKAGE DOCUMENTATION

Required Documents	POC	POC Phone	Comments
<u>I. Primary CNDS Provider Information</u>			
A. Unit Name and Physical Address			
B. Unit POC Rank, Name, Phone Numbers, NIPRNET address and SIPRNET address			
C. Unit Organization Diagram/Chart. This diagram shall reveal how the primary CNDS Provider is organized to conduct/monitor Component-wide CNDS for both GENSER and Special Enclave information systems/networks. The diagram shall also indicate any relationships to any other/subordinate Component CNDS Providers and be explained in detail. For example, for Special Enclave CNDS, the Primary CNDS Provider may have a Memorandum of Understanding/Agreement with the Component's Special Access Program (SAP) Control Office where the SAP Control Office is the assigned CNDS Provider for Special Enclaves and that organization ensures the CNDS for information systems/networks within the Component-owned SAPs. Such a possible relationship would be annotated on the diagram/chart and fully explained on an attachment. It would include what monitoring of those Special Enclave CNDS is performed by the Primary CNDS Provider, and what reporting or communications is given to the Primary CNDS			
D. Charter (if applicable) with Mission Statement			
E. Slides/Presentations pertaining to the CNDS Provider's mission and/or the four CND areas			
F. Personnel Points of Contact including: <ol style="list-style-type: none"> 1. Commander/Director 2. (C&A) at each organization and sub-unit 3. POCs within each of the four CNDS areas of Protect, Detect, 			

Required Documents	POC	POC Phone	Comments
Response, & Sustainment 4. Overall technical responsibility 5. Contractor Program Manager (PM) (if CND Service Provider includes contractors)			
G. Listing of subscriber organizations to include: 1. Points of contact (System Administrator, ISSO/ISSM, Phone numbers, and addresses 2. Inventory of CND subscriber networks (by mission category)			
H. Service policy guidance on CND and CNDS activities			
I. MOUs or Agreements between the Primary CNDS Provider and other organizations to conduct/monitor CNDS for GENSER and Special Enclave information systems/networks.			
II. <u>Self-Assessment (using the ESM), one for each security level (i.e., GENSER and Special Enclave)</u>			
III. <u>Primary CNDS Provider Policies and Procedures for GENSER CNDS</u>			
A. Protection Policies and Procedures/SOPs			
1. Policies and procedures for Vulnerability Analysis Scanning (VAS) tools			
2. VAA or Red Team recommendations to subscribers			
3. Anti-Virus Policy and associated procedural documents			
4. Subscriber network diagrams			
5. System hardening guidelines			
6. Assessments of subscriber ETA CND program			
7. Copies of training presentations and/or documentation (CND best practices, malicious code awareness, INFOCON and IAVM policies and procedures)			
8. INFOCON procedures (Subscriber supplemental INFOCON procedures if exist)			
9. IAVA Implementation and Monitoring procedures			

Required Documents	POC	POC Phone	Comments
B. Monitor, Analyze, and Detect Policies and Procedures/SOPs			
1. Network Security Monitoring policies and procedures			
2. Warnings and Notifications distribution procedures			
3. Firewall Configuration Best Practices (for distribution to subscribers)			
4. Threat Warning and Notification Distribution Procedures			
5. Policy/Procedures for Incident Analysis			
C. Response Policies and Procedures/SOPs			
1. Incident Reporting Procedures			
2. Procedures for Incident Reporting to Law Enforcement and Counterintelligence			
3. Incident Reporting Guidelines for classified networks			
4. Incident Handling and Response Procedures (including classified networks)			
5. Surge Operations Procedures including Personnel Recall Procedures			
D. GENSER CNDS Sustainment Policies and Procedures/SOPs. (Includes CNDS Training, Command Inspection Program, etc.)			
1. MOUs and/or other written agreements w/subscriber defining services provided			
2. Copy of order designating CNDSP as service provider			
3. Policies for information sharing w/DoD organizations			
4. Policy and procedures for support to law enforcement investigations			
5. Policy for support and information sharing to intelligence community			
6. Procedures for foreign national access to information and information systems			
7. CNDS Provider Five Year Plan			

Required Documents	POC	POC Phone	Comments
8. CNDS Provider Financial Plan			
9. Organization Chart			
10. Procedures for testing new CND technologies			
11. Procedures for testing patches before deployment			
12. Documented Training Program (contains ETA requirements for CNDS Provider staff) that includes policies, procedures, and/or standards that support an organized CNDS training program. Also provide information on:			
a. In-house training tools and techniques			
b. Training courses offered or acquired by the CNDS Provider			
13. Documented workforce plan			
14. Quality Assurance Policy			
15. Physical Security Policy			
16. Policies and procedures for personnel security			
17. Documentation/briefing copies of OPSEC program			
18. Physical Access Control procedures			
19. Employee screening procedures			
20. Anti-Virus Policy for internal networks			
21. Internal INFOCON procedures			
22. Contingency Plan			
23. Disaster Recovery Plan			
24. Emergency Response Plan			
25. Systems/Data Backup Plan			
26. IAVM compliance procedure			
<u>IV. Primary CNDS Provider Policies and Procedures for Special Enclave CNDS (see the above listing for the GENSER Enclaves for documents required, as they will essentially be the same)</u>			
A. Protection Policies and Procedures			
B. Detection/Monitoring Polices and Procedures			

Required Documents	POC	POC Phone	Comments
C. Analysis/Response Policies and Procedures			
D. Special Enclave CNDS Sustainment Policies and Procedures. (Includes CNDS Training, Command Inspection Program, etc.)			
V. <u>Inspection results within past 3 years, which provide insight to the Component's performance in providing CNDS to both GENSER and Special Enclaves.</u>			
A. DoD IG Reports			
B. Component-level inspection reports			
C. Other inspections/evaluations of Component CNDS			

NOTE:

Some of the documents listed may be composite parts of a larger document. For example, the Contingency Plan may contain an Emergency Plan, Disaster Recovery Plan, and other related documents. The requirement is that each document/subject matter listed must be addressed, whether as listed in the table, or as parts of a larger document. Use the "Comments" column to explain any such circumstances.

AP3. APPENDIX 3

LETTER OF REQUEST

[DoD Component Primary Provider Letterhead]

To:
DoD CND Architect
Department of Defense
Room 3D239
6000, The Pentagon
Washington, DC 20301-6000

Subject: Letter of Application for Primary CNDS Provider Certification & Accreditation (C&A)

In accordance with DoDI O-8530.2 and DoD Manual O-8530.1, this letter serves as the [*Enter the Component Primary Provider Title*] application for Certification & Accreditation as a Primary CNDS Provider.

[*Enter the Organization Title of Primary CNDS Provider*] is the Primary CNDS Provider for [*Enter the DoD Component Title(s)*]. [*Enter the Organization Title of Primary CNDS Provider*] is located at [*Address of Primary CNDS Provider*]. Your Point-of-Contact for all coordination will be:

[*POC rank and name*]
[*POC title*]
[*POC commercial phone number*]
[*POC NIPRNet address*]
[*POC SIPRNet address*]

The [*Enter the Primary CNDS Provider organizational name*] has assembled the required documentation, as listed in DoD Manual O-8530.1, and provides it to you via the enclosed Compact Disk (CD). If there are other documents or information required, the POC above shall respond.

Included in the CD is our self-assessment using the Evaluator's Scoring Metrics (ESM). The self-assessment was conducted during the period of [*time period entered*] and resulted in GENSER and Special Enclave scores which are as follows:

GENSER CND Services:

Priority I Metrics Compliance Percentage = [*Enter compliance percentage here*]
Priority II Metrics Compliance Percentage = [*Enter compliance percentage here*]
Priority III Metrics Compliance Percentage = [*Enter compliance percentage here*]
Priority IV Metrics Compliance Percentage = [*Enter compliance percentage here*]

As a result of these self-assessment scores, we believe that the [*Primary CNDS Provider organizational name*] will attain an Accreditation Level for GENSER CND Services of [*Enter self-assessment Accreditation Level from ESM calculations*].

Special Enclave CND Services:

Priority I Metrics Compliance Percentage = [*Enter compliance percentage here*]

Priority II Metrics Compliance Percentage = [*Enter compliance percentage here*]

Priority III Metrics Compliance Percentage = [*Enter compliance percentage here*]

Priority IV Metrics Compliance Percentage = [*Enter compliance percentage here*]

As a result of these self-assessment scores, we believe that the [*Primary CNDS Provider organizational name*] will attain an Accreditation Level for Special Enclave CND Services of [*Enter self-assessment Accreditation Level from ESM calculations*].

[SIGNED]

Appropriate Primary Provider Authority

Encl: Compact Disk w/Application Documentation

*Completed
SMB
12/19/03*

**Unclassified
OASD(NII) Suspense Tracking System**

SUBJECT: Proposed DoD Manual O-8530.1-M "Computer Network Defense Service Provider Certification and Accreditation Process"
Action Required: Appropriate action
Date Received: 12/05/2003 11:44 AM

Due to DASD	Due to ASD	Final Date Due	DASD Control #	NII Control #	OSD Control #
		12/18/2003		IA 12-006/03	

Remarks:

ASD (NII)	(Stenbit)	A
Senior Military Assistant	(Hanson, C.)	<i>12/16</i>
Executive Correspondent Assistant	(Miller)	
Executive Assistant	(Stevenson)	
Principal Deputy	(Wells)	<i>2/15</i>
Military Assistant	(Newman)	
Dir, Research & Strategic Planning	(Alberts)	
Director, Admin & Mgt	(McCarthy)	
Director, International Affairs	(Manno)	
NASA Liaison	(DiMarcantonio)	

A-Net:	Read File:
DASD (Deputy CIO)	(Guthrie) <i>A</i>
Principal Director	(Myers) <i>Miller</i>
Dir, Information Services	(Dyson)
Director, Architecture & Interoperability	(Osterholz)
Director, Information Assurance	(Lentz) <i>A</i>
Dir, Information Management	(Krieger)
Director, Commercial Policies & Oversight (Acting)	(Boyd)
Dir, Planning, Policy & Integration (Acting)	(France)

DASD (S3C3) (Acting)	(Wells)
Principal Director	(Wormser)
Director, Space Policy	(Trottier)
Director, Spectrum Management	(Younes)
Director, C2 Policy	(Diggs)
Director, Wireless	(Jost)
Dir, Sensitive Info Integration	(Vacant)
Decision Support Center	(Griffiths)

DASD (Resources)	(Roby)
Principal Director	(Vacant)
Director, Congressional Review & Analysis	(Condon)
Director, Resource, Program & Budget	(Hammersley)
Director, Strategic Resource Planning	(Yoemans)
Dir, NII Resource Management	(Fattahian)

Director, DISA	(Raduege)

DASD (C3, Space & IT Programs)	(Frankel)
Principal Director	(Landon)
Director, Communications Programs	(Criste)
Director, Space Programs (Acting)	(Gamble)
Director, C2 Programs	(Callier)
Director, Acquisition (Acting)	(Lewis)

Updated: 11/14/2003

*Keep on
congrats
get to
date*

Unclassified
(Upon removal of attachments, this page is unclassified)