



# INSTRUCTION

March 9, 2001  
NUMBER O-8530.2

~~Created by:~~

ASD(C3I)

SUBJECT: Support to Computer Network Defense (CND)

- References:
- (a) DoD Directive O-8530.1, "Computer Network Defense," January 8, 2001
  - (b) "DoD Command, Control, Communications, Intelligence, Surveillance and Reconnaissance (C4ISR) Architecture Framework," Version 2.0, December 18, 1997
  - (c) Joint Technical Architecture (JTA), Version 3.0, November 29, 1999
  - (d) DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP) ," December 30, 1997
  - (e) through (l), see enclosure 1

## 1. PURPOSE

This Instruction:

- 1.1. Implements policy, assigns responsibilities, and prescribes procedures under reference (a) necessary to provide the essential structure and support to the U.S. Space Command (USCINCSpace) for Computer Network Defense (CND) within Department of Defense information systems and computer networks.
- 1.2. Defines CND Services (CNDS).
- 1.3. Establishes the CND Service certification and accreditation process.
- 1.4. Requires CND compliance with references (b) and (c).
- 1.5 Provides for Information Assurance Red Team notification, reporting and coordination to insure deconfliction of Red Team and CND activities.

## 2. APPLICABILITY AND SCOPE

This Instruction:

- 2.1. 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").
- 2.2. Applies to all DoD information systems and computer networks.

### 3. DEFINITIONS

Terms used in this Instruction are defined in enclosure 2.

### 4. POLICY

This Instruction implements the policies defined in DoD Directive O-8530.1 (reference (a)).

### 5. RESPONSIBILITIES

Pursuant to reference (a):

5.1. The Assistant Secretary of Defense for Command, Control, Communications and Intelligence ASD (C3I) shall:

5.1.1. Oversee and review implementation of this Instruction.

5.1.2. Appoint, in coordination with Chairman, Joint Chiefs of Staff (CJCS) and USD(AT&L), the DoD CND Architect.

5.1.3. Ensure the establishment of the CNDS certification and accreditation process.

5.1.4. Ensure the establishment of a Defense-wide Information Assurance Vulnerability Alert (IAVA) notification, reporting, coordination and compliance process (see enclosure 6).

5.1.5. Ensure the establishment of a Defense-wide Information Assurance Red Teaming notification, reporting, and coordination process.

5.1.6. Ensure that CND requirements are addressed as part of the DoD Information Technology Security Certification and Accreditation Process (DITSCAP) (DoD Instruction 5200.40 (reference (d)) and in information technology (IT) registration and configuration management guidance and systems.

5.2. The Director, Defense Information Systems Agency shall:

5.2.1. Develop, in coordination with USCINCSpace and Director, NSA, the CNDS certification and accreditation process (See enclosure 5).

5.2.2. Function as the CNDS Certification Authority (CNDS/CA) for General Service CNDS.

5.2.3. Function as the Systems Integrator for Defense-wide CND related systems in accordance with DoD Instruction 4630.8 (reference (e)).

5.2.4. Manage the IAVA process (see enclosure 6).

5.2.5. Coordinate all red team and penetration tests for General Service Enclaves.

5.3. The Director, National Security Agency shall:

- 5.3.1. Assist the Director, DISA, in developing the CNDS certification and accreditation process.
- 5.3.2. Function as the CNDS/CA for Special Enclave CNDS.
- 5.3.3. Function as the Program Manager for Defense-wide CND research and technology (R&T).
- 5.3.4. Establish and maintain a trusted agent network and procedures for the reporting of Information Assurance Red Teaming activities.
- 5.3.5. Provide specialized Attack Sensing and Warning (AS&W) support to USCINCSpace and the DoD Components.

5.4. The Commander in Chief, United States Space Command (USCINCSpace) shall:

- 5.4.1. Establish, in coordination with the DoD Components, DoD-wide procedures for dissemination of CND and related advisories, alerts and warning notices, including those originating outside of the Department of Defense, monitor compliance with issued IAVAs, and direct DoD-wide actions, including DoD-wide Information Operations Condition (INFOCON) changes, to defend DoD computer network operations.
- 5.4.2. Provide the Secretary of Defense through the Chairman, Joint Chiefs of Staff (CJCS), a periodic operational assessment of the readiness of the DoD Components to defend DoD information systems and computer networks.
- 5.4.3. Employ combatant command authority and tactical control (TACON) of assigned forces to plan and execute operations to protect and defend DoD computer networks or other vital national security interests as directed by the Secretary of Defense, against any intentional unauthorized computer network intrusion or attack.
- 5.4.4. Develop and request changes to Standing Rules of Engagement for Computer Network Defense.
- 5.4.5. Conduct and coordinate CND deliberate and crisis action planning and execution for computer network defense as directed in accordance with the Joint Operations Planning and Execution System.
- 5.4.6. Coordinate with the Director, NSA to maintain awareness of and deconflict Red Teaming activities and operations associated with DoD information systems and computer networks.
- 5.4.7. Assist the Director, DISA in developing the CNDS certification and accreditation process and serve as Accrediting Authority for the CNDS/CAs

5.5. The Heads of the Components shall:

5.5.1. Establish Component-level CND Services to coordinate and direct Component-wide CND and ensure system and personnel certification and accreditation in accordance with established DoD requirements and procedures.

5.5.2. Provide USCINCSpace with operational assessments and comply with USCINCSpace operational direction for the planning and conduct of CND and the integration of Information Assurance activities into CND operations.

5.5.3. Comply with the reporting requirements of CJCSI 6510.01 series (reference (f)) and additional reporting requirements coordinated by USCINCSpace.

5.5.4. Contribute to computer network situational awareness by providing operational requirements and priorities, operational status and the user's perspective on computer network status (e.g., availability, reliability).

5.5.5. Maintain an inventory of all Component information systems and computer networks (i.e., systems separately accredited by a Designated Approving/Accrediting Authority (DAA) under the provisions of DoD Instruction 5200.40 (reference (d))) and their associated CNDS providers. This inventory information shall be made available to the DoD Chief Information Officer and USCINCSpace.

5.5.6. Manage the designation of Component-owned Special Enclaves and ensure that all designated Special Enclaves are assigned to a CNDS.

5.5.7. Ensure that CNDS support is a condition of information and computer system IT security certification and accreditation in accordance with reference (d).

5.5.8. Provide guidance on service arrangements with non-Component CNDS providers.

5.5.9. In coordination with the CNDS/CAs and USCINCSpace, develop a coordinated and common DoD curriculum for CND education, training and awareness.

5.5.10. Participate in planning and establish Component requirements for a Defense-wide common operational picture (COP).

5.5.11. Plan, program, and monitor Component-assigned responsibilities for development of information systems or databases supporting Defense-wide CND.

5.5.12. In coordination with the Systems Integrator, establish Component sensor grid requirements and plan and program for their implementation.

5.5.13. Coordinate system development and integration with the Systems Integrator and the R&T Program Manager.

5.5.14. Support CND Architect sponsored activities and respond to requests for information.

## 6. PROCEDURES

### 6.1. The CNDS Certification Authorities shall:

6.1.1. In coordination with the CND Architect, develop and implement the CND certification and accreditation process.

6.1.2. Provide technical, analytical and coordination CND services (e.g., the analysis and reporting of intrusions, incidents and event, dissemination of alerts and warning notices, computer diagnostics, short term CND trend and pattern analysis, IAVA monitoring) to the DoD Component CNDS providers and to USCINCSpace.

6.1.3. In coordination with the Heads of Components and Defense-wide Information Assurance initiatives, develop a coordinated curriculum for CND education, training, and awareness that addresses requirements identified by the CNDS providers and the certification and accreditation process.

6.1.4. In coordination with the CNDS providers and the R&T Program Manager, identify requirements and ensure that new technologies are effectively transitioned into CNDS practices.

### 6.2. The Component CNDS Providers shall:

6.2.1. Comply with the operational direction of USCINCSpace for the conduct of CND and the integration of Information Assurance activities into CND operations.

6.2.2. Comply with the reporting requirements of CJCSI 6510.01 series (reference (f)) and additional reporting requirements coordinated by USCINCSpace.

6.2.3. Provide for the coordination services (see paragraph E5.4.5) of the appropriate CNDS/CA.

6.2.4. Maintain an inventory of all supported entities and associated information systems and computer networks.

6.2.5. Provide CND Services in accordance with enclosure 4.

### 6.3. The CND Law Enforcement and Counterintelligence (LE&CI) Center shall:

6.3.1. Serve as the primary interface with the National Infrastructure Protection Center (NIPC) for CND related law enforcement and counterintelligence issues.

6.3.2. Receive operational direction for law enforcement from the Defense Criminal Investigative Organizations and respond to the information requirements of the USCINCSpace and Component CNDS providers.

6.3.3. Coordinate, deconflict, and facilitate law enforcement and counterintelligence CND investigations and operations among the DoD Components.

6.3.4. Provide analytical services to support CND investigations and operations and the COP.

6.3.5. Support CND planning and policy development.

6.3.6. Coordinate release of CND LE&CI information, with appropriate consent, from originating agencies to support information sharing across the DoD Components.

6.4. The National Security Incident Response Center (NSIRC) shall:

6.4.1. Provide specialized Attack Sensing and Warning (AS&W) analysis for discovery of Defense-wide and long-term trends and patterns.

6.4.2. Provide overall focus and coordination for the AS&W function.

6.4.3. Provide direct AS&W support to USCINCSpace.

6.4.4. Provide AS&W assistance as required to Component CNDS providers.

6.5. The DoD CND Architect shall:

6.5.1. Develop and implement CND operational architectures to support USCINCSpace.

6.5.2. Support the DoD Components in all CND architecture activities.

6.5.3. Support the ASD(C3I) in periodic review of CND capabilities and requirements.

6.5.4. Oversee the establishment and implementation of the CND certification and accreditation process.

6.5.5. Oversee the activities of the CND Research and Technology Program Manager and Systems Integrator.

6.5.6. Manage the Special Enclave designation process.

6.6. The CND Research and Technology (R&T) Program Manager shall:

6.6.1. Provide technical direction and coordination for the development and evaluation of CND tools and techniques.

6.6.2. In coordination with the CNDS/CAs, ensure the effective transition of new capabilities into CNDS practices.

6.6.3. In coordination with the DoD Components and the Defense-wide Information Assurance Program (DIAP), provide a comprehensive view of all CND-related technology gaps,

shortfalls, research, development and transition requirements to the Director of Defense Research and Engineering (DDR&E)

6.6.4. Develop the CND Technology Transition Plan and Program.

6.6.5. Program for common Defense-wide CND Technology Transitions and provide support to the DIAP and the DDR&E in programming for related research and development (R&D).

6.6.6. Provide support to the CND Architect, OSD, the Joint Staff and USCINCSpace in the identification and resolution of CND technology transition and R&D program issues.

6.7. The CND Systems Integrator shall:

6.7.1. Develop and coordinate the Sensor Grid Plan and Program.

6.7.2. Develop and coordinate the COP Plan and Program.

6.7.3. Provide support to the CND Architect, OSD, the Joint Staff and USCINCSpace in the identification and resolution of CND systems (e.g., capabilities, tools) integration issues.

## 7. INFORMATION REQUIREMENTS

7.1. The Information Systems Registration with DoD Chief Information Officer reporting requirement referred to in this Instruction has been assigned Report Control Symbol DD-C3I(AR)2096 in accordance with DoD 8910.1-M (reference (g)).

7.2. The Information Assurance Vulnerability Alert (IAVA) reporting referred to in subparagraph 5.1.4 is exempt from licensing in accordance with paragraph C4.4.2 of reference (g).

7.3. The reporting of Information Assurance Red Teaming Activities is exempt from licensing in accordance with paragraph C4.4.2 of reference (g).

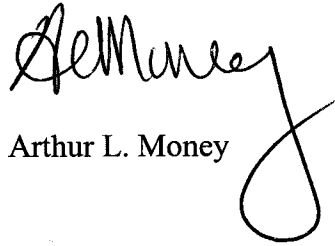
7.4. The operational assessment referred to in subparagraph 5.4.2 is exempt from licensing in accordance with paragraph C4.4.4 of reference (g).

7.5. The Certificate Authority reporting of intrusions, incidents and events and dissemination of alerts and warnings notices are exempt from licensing in accordance with paragraph C4.4.2 of reference (g).

7.6. Additional information requirements, unless exempt, shall be developed, approved and licensed in accordance with reference (g).

8. EFFECTIVE DATE

This Instruction is effective immediately.

A handwritten signature in black ink, appearing to read "A. Money", with a large, stylized flourish extending from the end of the signature.

Arthur L. Money

Enclosures – 6

- E1. References, continued
- E2. Definitions
- E3. Computer Network Defense (CND) Concept
- E4. Computer Network Defense (CND) Services
- E5. Computer Network Defense (CND) Support Functions
- E6. Information Assurance Vulnerability Alert (IAVA)



E1. ENCLOSURE 1

REFERENCES, continued

- (e) DoD Instruction 4630.8, "Procedures for Compatibility, Interoperability, and Integration of Command, Control, Communication and Intelligence Systems," November 18, 1992
- (f) CJCS Instruction 6510.01B, "Defensive Information Operations Implementation," August 22, 1997
- (g) DoD 8910.1-M, "DoD Procedures for Management of Information Requirements," June 30, 1998
- (h) Presidential Report: Defending America's Cyberspace: National Plan for Information Systems Protection, Version 1.0, Prepared by the National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism, June, 2000
- (i) Executive Order 12333, "United States Intelligence Activities," December 4, 1981
- (j) DoD Directive 5240.1, "Activities of DoD Intelligence Components that Affect U.S. Persons," April 25, 1988
- (k) DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons," December 1982
- (l) National Security Telecommunications and Information Systems Security Directive (NSTISSD) No. 503, "Incident Response and Vulnerability Reporting for National Security Systems," August 30, 1993

## E2. ENCLOSURE 2

### DEFINITIONS

E2.1.1. Accreditation. Formal declaration by the Designated Approving/Accrediting Authority (DAA) that an information system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.

E2.1.2. 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. Attack sensing and warning also includes attack/intrusion related intelligence collection tasking and dissemination; limited immediate response recommendations; and limited potential impact assessments.

E2.1.3. Certification. Comprehensive evaluation of the technical and non-technical security features of an information system and other safeguards, made in support of the accreditation process, to establish the extent that a particular design and implementation meets a set of specified security requirements.

E2.1.4. 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.

E2.1.5. 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.

E2.1.6. Computer Network Attack (CNA). Operations to disrupt, deny, degrade, or destroy information resident on computers and computer networks or the computers and networks themselves.

E2.1.7. 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, and 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.

E2.1.8. CND Operational Hierarchy. The way DoD is organized to conduct CND. The Department of Defense is organized into three tiers to conduct CND. Tier One provides DoD-wide CND operational direction or support to all DoD Components. Tier Two provides DoD Component-wide operational direction or support and responds to direction from Tier One. Tier Three provides local operational direction or support and responds to direction from a designated Tier Two entity. Tier One entities include the USCINCSpace and supporting entities such as the CND Service Certification Authorities (DISA and NSA), the CND Law Enforcement and Counterintelligence Center, and the National Security Incident Response Center. Tier Two includes CNDS providers designated by Heads of Components to coordinate Component-wide CND. Tier Three includes all entities responding to direction from DoD Component Tier Two CNDS, e.g., local control centers that manage and control information systems, networks and services, either deployed or fixed at DoD Installations.

E2.1.9. CND Common Operational Picture (COP). A distributed capability that provides local, intermediate, and DoD-wide visual situational awareness of CND actions and their impact; collaboration; and decision support. The CND COP is a view on the Network Operations Common Operational Picture (NETOPS COP).

E2.1.10. CND Law Enforcement and Counterintelligence Center. An organization that coordinates LE&CI investigations and operations in support of CND and is staffed by all Defense Criminal Investigative and Counterintelligence Organizations.

E2.1.11. CND Sensor Grid. A coordinated constellation of decentrally owned and implemented intrusion and anomaly detection systems deployed throughout DoD information systems and computer networks. The CND sensor grid is a component of the NETOPS sensor grid.

E2.1.12. CND Service (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.

E2.1.13. CNDS Certification. An integrated suite of CNDS certification standards; self-assessment and independent assessment processes; improvement methods and tools; and inter-CNDS information exchange and communications protocols established by the CNDS/CA.

E2.1.14. CNDS Certification Authority (CNDS/CA). An entity responsible for certifying CNDS providers, coordinating among supported CNDS providers, and managing information dissemination supporting CND operations.

E2.1.15. CNDS Providers. Those organizations responsible for delivering protection, detection and response services to its users. CNDS providers must provide for the coordination service support of a CNDS Certification Authority. CNDS is commonly provided by a Computer Emergency or Incident Response Team (CERT/CIRT) and may be associated with a Network Operations and Security Center (NOSC).

E2.1.16. Counterintelligence. Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities.

E2.1.17. Counterintelligence Activities. The four functions of counterintelligence are operations; investigations; collection and reporting; and analysis, production, and dissemination.

E2.1.18. Counterintelligence Investigation. Includes inquiries and other activities undertaken to determine whether a particular United States person is acting for, or on behalf of, a foreign power for purposes of conducting espionage and other intelligence activities, sabotage, assassinations, international terrorist activities, and actions to neutralize such acts.

E2.1.19. General Service Network or System. For the purposes of CND, all DoD information systems and computer networks are classified at one of two security levels, General Service or Special Enclave. All DoD information systems and/or computer networks will be considered General Service (e.g., NIPRNET & SIPRNET) unless designated as Special Enclave because of special security requirements.

E2.1.20. Indications and Warning. 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/coalition military, political, or economic interests or to U.S. citizens abroad. It includes forewarning of enemy actions or intentions; the imminence of hostilities; insurgency; nuclear/non-nuclear attack on the United States, its overseas forces, or allied/coalition nations; hostile reactions to U.S. reconnaissance activities; terrorists' attacks; and other similar events.

E2.1.21. Information Assurance Red Teaming. An independent threat based activity aimed at improving information assurance readiness by emulating a potential adversary's attack or exploitation capabilities. See also Red Team.

E2.1.22. Information Assurance Vulnerability Alert (IAVA). The comprehensive distribution process for notifying CINCs, Services and Agencies (C/S/A) about vulnerability alerts and countermeasures information. The IAVA process requires C/S/A receipt acknowledgment and provides specific time parameters for implementing appropriate countermeasures depending on the criticality of the vulnerability.

E2.1.23. Information Operations Condition (INFOCON). The INFOCON is a comprehensive defense posture and response based on the status of information systems, military operations, and intelligence assessments of adversary capabilities and intent. The INFOCON system presents a structured, coordinated approach to defend against a computer network attack. INFOCON measures focus on computer network-based protective measures. Each level reflects a defensive posture based on the risk of impact to military operations through the intentional disruption of friendly information systems. INFOCON levels are: NORMAL (normal activity); ALPHA (increased risk of attack); BRAVO (specific risk of attack); CHARLIE (limited attack); and DELTA (general attack). Countermeasures at each level include preventive actions, actions taken during an attack, and damage control/mitigating actions.

E2.1.24. Information System. The entire infrastructure, organization, personnel and components for the collection, processing, storage, transmission, display, dissemination and disposition of information. For the purposes of this Directive, it is an information system that has been separately accredited by a DAA under provisions of DoD Instruction 5200.40 (reference (d)).

E2.1.25. National Infrastructure Protection Center (NIPC). The NIPC is both a national security and law enforcement effort to detect, deter, assess, warn of, respond to, and investigate computer intrusions and unlawful acts both physical and "cyber," that threaten or target our critical infrastructures. The NIPC provides a national focal point for gathering information on threats to critical infrastructures. Additionally, the NIPC will provide the principal means for facilitating and coordinating the Federal Government's resources to an incident or mitigating an attack.

E2.1.26. Network Operations (NETOPS). An organizational and procedural framework intended to provide DoD information system and computer network owners the means to manage their information systems and computer networks. This framework allows information system and computer network owners to effectively execute their mission priorities, support DoD missions, and maintain their information systems and computer networks. This framework integrates the mission areas of network management, information dissemination management, and information assurance.

E2.1.27. 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. (See Information Assurance Red Team).

E2.1.28. Special Enclave. DoD information systems and/or computer networks with special security requirements (e.g., Special Access Programs (SAP), Special Access Requirements (SAR)) and designated as Special Enclave by the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence.

E2.1.29. Vulnerability Analysis and Assessment. 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.

## E3. ENCLOSURE 3

### COMPUTER NETWORK DEFENSE (CND) CONCEPT

#### E3.1. INTRODUCTION

E3.1.1. This Enclosure provides a general overview of the DoD operational capability in Computer Network Defense and its relationship to national initiatives by identifying existing and proposed processes, activities and organizations, and describing CND, the Strategic Environment, and the CND Operational Hierarchy. CND Services and CND Support Functions are described in greater detail at enclosures 4 and 5.

E3.1.2. Within the Department of Defense, Computer Network Defense has emerged as a distinct mission with a dedicated professional workforce and organizational structure. The Department of Defense has designated the USCINCSpace as the military lead for CND operations, and is developing a standard suite of CND Services that can be scaled to cover all DoD information systems and computer networks. The USCINCSpace provides overall coordination and direction for CND Services; however, all DoD Components have the responsibility to ensure their information systems and networks are defended. The DoD Components must establish a Component-level CND capability, coordinate its development with the USCINCSpace, and support the USCINCSpace in the conduct of Defense-wide CND operations. Additionally, all DoD Components must actively contribute to the continued definition and maturation of an evolving mission area that employs or is employed by six interrelated capabilities: Information Assurance, Network Operations, Information Operations, Critical Infrastructure Protection, Law Enforcement, and Counterintelligence.

E3.1.3. CND Services are the actions taken to protect, monitor, analyze, detect and respond to unauthorized activity within DoD information systems and computer networks. While CND Services are normally provided by Computer Emergency or Incident Response Team (CERT/CIRT) organizations, the terms are not synonymous. CNDS does not include some services normally provided by a CERT/CIRT (e.g., recovery of a computer system's failure due to software incompatibility is a traditional CERT function but not a CNDS since it is not a result of unauthorized activity).

E3.1.3.1. CND Protection includes the management of the Department of Defense's Information Operations Conditions system and deliberate actions taken to modify an information system or computer network configuration or assurance posture in response to a CND alert or threat information. It also includes support for activities such as the Information Assurance Vulnerability Alert system; vulnerability analysis and assessments; and Information Assurance (and CND) education, training, and awareness.

E3.1.3.2. CND Monitoring, analysis, and detection actions provide CND situational awareness, attack sensing and warning and indications and warning. Multiple communities within the Department of Defense, e.g., network operations, CND Services, intelligence, counterintelligence, and law enforcement contribute to situational awareness. Attack sensing and warning (AS&W) includes a managed network of intrusion, misuse, and anomaly detection

systems, supporting data fusion and analysis, diagnostics, long term trend and pattern analysis, and warning communications channels and procedures. AS&W senses changes in DoD computer networks. Indications and warning, by contrast, senses changes in adversaries. The intelligence community provides indications and warning for foreign threats – nation states and transnational groups. The law enforcement community provides threat information about domestic individuals and groups, and the counterintelligence community provides threat information about insider support to nation states and transnational groups.

E3.1.3.3. CND Response actions are governed by the authorities that define unauthorized activity:

Authority	Examples of Unauthorized Activity	Examples of Response Actions
Administrative	Violation of Department or system owner security policy	Revocation or suspension of system access or privileges
Legal	Intrusion, Denial of Service, Theft, System Vandalism or Destruction, Espionage, Coordinated attack, Coordinated exploitation	Investigation Prosecution
National Security	System Destruction, Espionage, Coordinated attack, Coordinated exploitation	The application of national economic, military, and/or diplomatic power to defeat or deter

Figure E3.F1. Authorities Governing Activity within DoD Information Systems and Computer Networks

E3.1.4. CND Support Functions include:

E3.1.4.1. Means to address CND Services for information systems and networks with special security requirements (General Service/Special Enclave Designation);

E3.1.4.2. A CND Services certification and accreditation process to ensure capability development, improvement and performance measurement;

E3.1.4.3. CND Architecture, program management of CND research and technology; and

E3.1.4.4. CND-related systems integration.

E3.1.5. The Strategic Environment, CND Services and CND Support Functions are enumerated and illustrated in the CND overview below (figure E3.F2.). The CND Operational Hierarchy will be addressed separately in section E3.3.

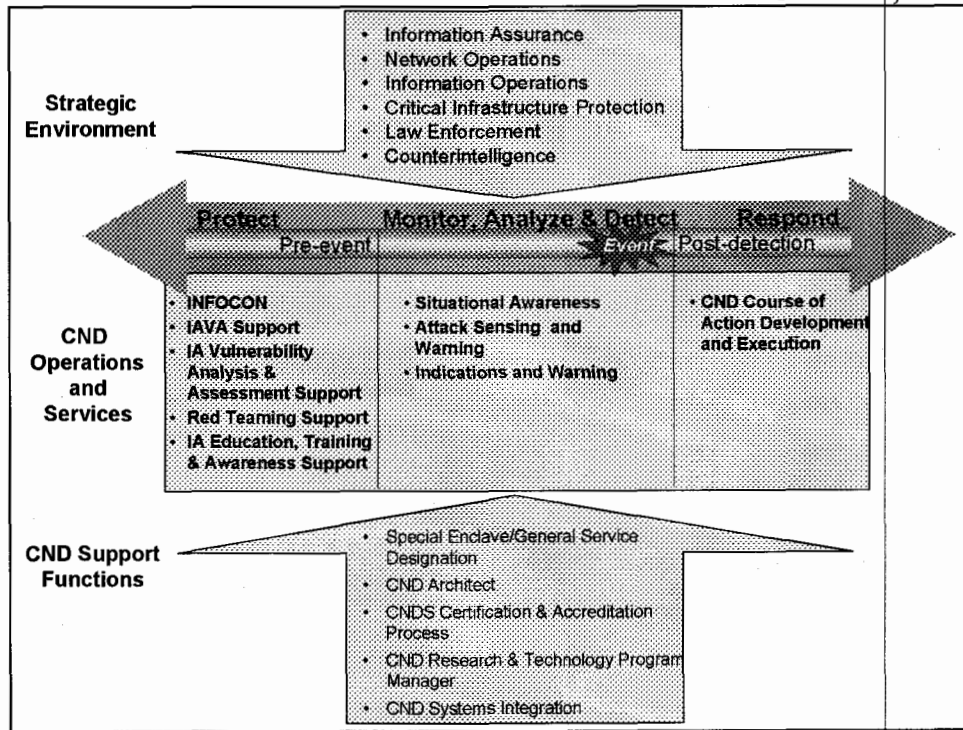


Figure E3.F2. Overview of Computer Network Defense

**E3.2. THE STRATEGIC ENVIRONMENT**

E3.2.1. Information Assurance (IA) addresses information availability, integrity, confidentiality, identification and authentication, and non-repudiation across the information technology life cycle. It does this by evaluating and integrating information assurance in Readiness, Policy, Research and Technology, Architectural Standards and System Transformation, Acquisition Support and Product Development, Human Resources Management, and Network Operations. Network Operations integrates Network Management, Information Dissemination Management, and IA.

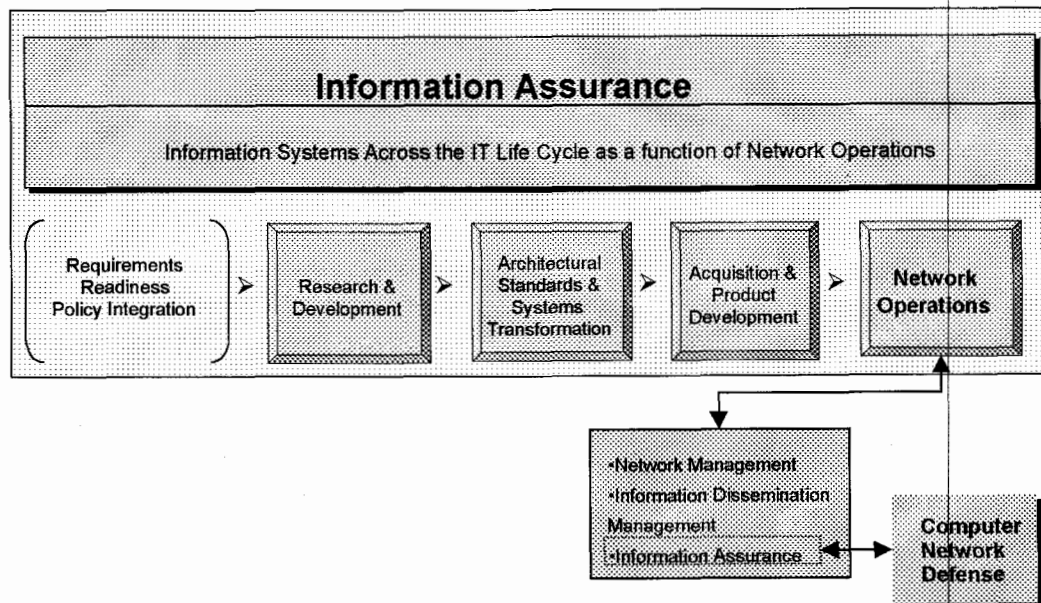


Figure E3.F3. Information Assurance Across the IT Life Cycle and CND as an Element of Network Operations



E3.2.2. Effective CND is predicated upon a robust Information Assurance posture; however, all policies, standards, technologies, and practices that apply across the IT life cycle and contribute to that posture are not managed as part of CND.

E3.2.3. Network Operations (NETOPS), as illustrated in the "pulldown" in Figure E3.F3., is an emerging management framework that addresses the relationships Network Management, Information Dissemination Management, and Information Assurance. Information Assurance provides the link between information operations and network operations (figure E3.F4.).

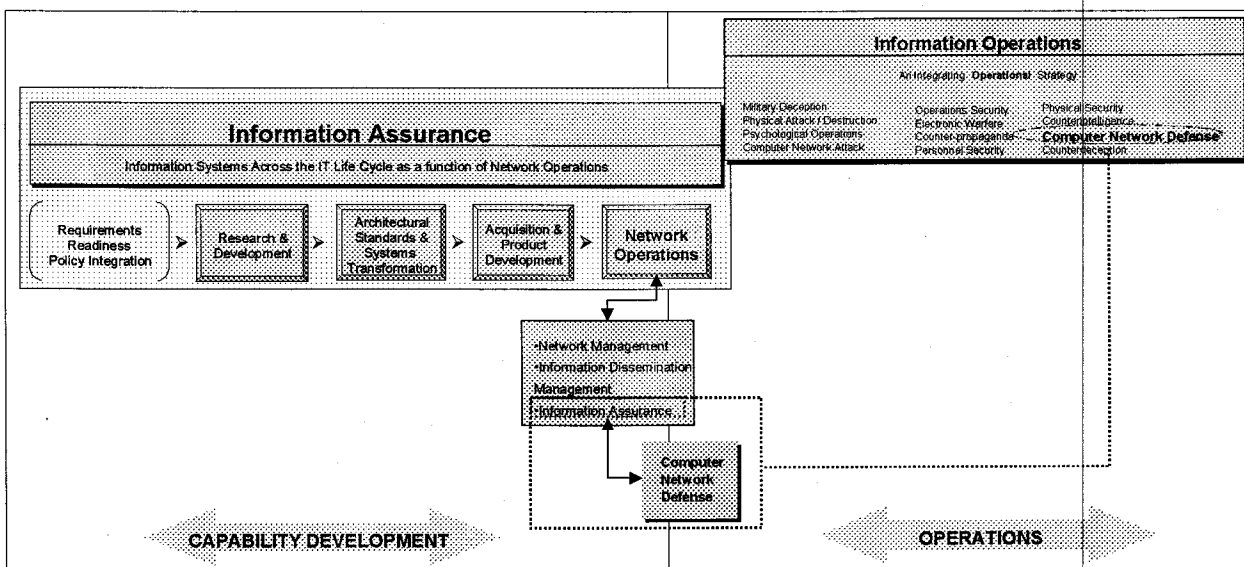


Figure E3.F4. Information Assurance as the link between Information Operations and NETOPS

E3.2.4. Information Operations is distinguished from Information Assurance in that it does not apply to the entire information systems life cycle. Rather it represents operations that employ CND with other activities such as military deception, psychological operations and electronic warfare to affect or defend information and information systems and contribute to achieving information superiority (figure E3.F4.).

E3.2.5. Computer Network Defense contributes to information superiority by providing:

E3.2.5.1. Situational awareness of computer network defense information and exchange within DoD information systems and computer networks; and

E3.2.5.2. An integrated operational capability to protect, monitor, analyze, detect, and respond to unauthorized activity within DoD information systems and computer networks.

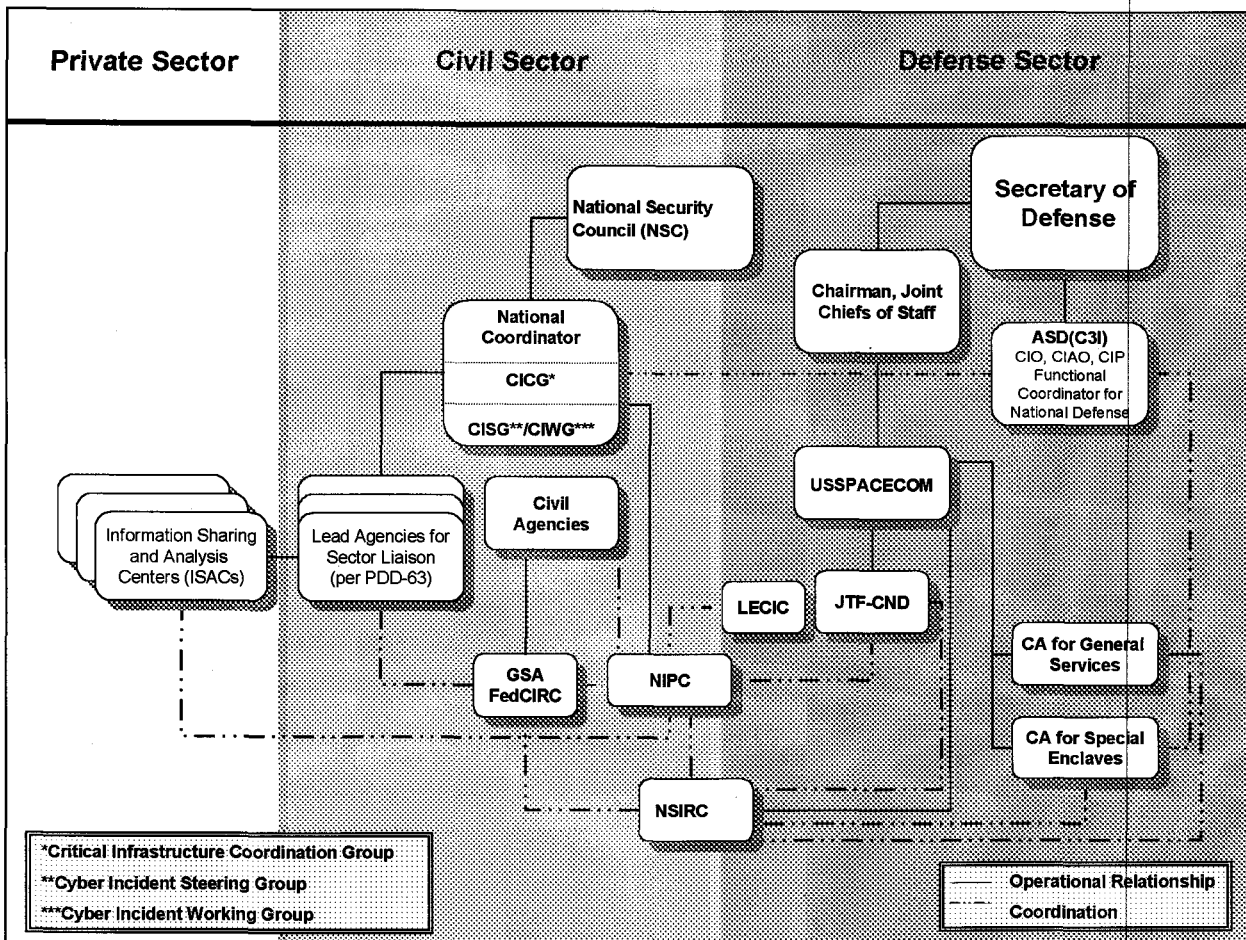


Figure E3.F5. The U.S. Government's Critical Infrastructure Protection Structure

E3.2.6. Critical Infrastructure Protection (CIP) is an overarching national policy (Presidential Decision Directive 63) which seeks to assure continuity and vitality in critical national infrastructures, including both physical and cyber-based systems, and their associated information and communications infrastructures. CIP is related to Information Assurance in that it applies to the entire life cycle of infrastructure systems and to Information Operations in that it provides an operational strategy for the protection of vital national and defense infrastructure. The DoD CND operational hierarchy, represented in the national plan for information systems protection (Defending America's Cyberspace: National Plan for Information System Protection (reference (h))), by the Joint Task Force - Computer Network Defense (JTF-CND), and described in section E3.3. of this enclosure, is an element of the U.S. Government's critical systems protection capabilities, as are the National Infrastructure Protection Center (NIPC), the Federal Computer Incident Response Center (FedCIRC) and the National Security Incident Response Center (NSIRC) (figure E3.F5.).

E3.2.7. Law Enforcement and Counterintelligence (LE&CI) are critical contributors to a viable CND capability, providing the mechanisms to establish attribution for and respond to illegal activity within DoD information systems and computer networks. The DoD Computer Forensics Laboratory and the DoD Computer Investigations Training Program support the LE&CI communities in all computer-related forensics and investigations. The

CND LE&CI Center provides Defense-wide coordination of CND related investigations and operations. The CND LE&CI Center supports operational decision making by coordinating CND related investigations and operations that cross the DoD Component or Federal Department/Agency bounds, and contributing law enforcement and counterintelligence generated information to a CND Common Operational Picture (COP). All of the Defense Criminal Investigative Organizations (DCIO) exchange CND related information with the LE&CI Center; the LE&CI Center maintains an information system to provide coordinated information input to the CND COP and to support the operational needs of the DCIOs.

### E3.3. THE DOD CND OPERATIONAL HIERARCHY

E3.3.1. The CND environment is characterized by escalating national and military requirements and increasing reliance on information and information systems, rapid technological change and a dynamic threat environment. 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 USCINCSpace, to conduct multi-Component and Defense-wide CND operations.

E3.3.2. To achieve such a capability, the DoD CND operational hierarchy integrates a traditional military command and control structure with a more dynamic and less formal coordination structure. This unique structure is organized into three tiers in order to:

E3.3.2.1. Ensure that all DoD information systems and computer networks are provided CND Services (CNDS). All information systems and computer networks must enter into a service relationship with a CNDS provider. Arranging for this service is the responsibility of the system or network owner.

E3.3.2.2. Permit DoD Components organizational discretion in acquiring CND Services. Except where clearly impractical, the DoD Components must establish a Component-level CNDS capability. The DoD Components may also arrange for CND Services offered by other DoD Components when those CND Services can more effectively meet CNDS requirements (e.g., for activities collocated with another Component). Accordingly, CNDS for a given Component may be distributed among multiple providers. Whether Components opt to establish more than one CNDS or to acquire CNDS from other DoD Components, a primary CNDS provider must be designated and authorized to manage Component-wide situational awareness and coordinate Component-wide CND. CNDS providers that are not designated as the primary provider are considered to be support providers, and follow the direction of the primary provider in coordination and integration of Component CNDS.

E3.3.2.3. Ensure that all CNDS providers have continuous information exchange and work together in synchrony, i.e., simultaneously execute a single prescribed Course of Action (COA) and that at any given time, a new COA can override the existing one. Coordination among CNDS providers is primarily effected through the CNDS Certification Authorities (CNDS/CAs) on behalf and under the direction of the USCINCSpace. All CNDS providers are required to comply with the guidance and direction of the

USCINCSpace and enter into a service relationship with a CNDS/CA. The CNDS/CAs perform four interrelated functions:

E3.3.2.3.1. Technical and analytic support to the USCINCSpace.

E3.3.2.3.2. Technical and analytic support to the serviced CNDS providers.

E3.3.2.3.3. Dynamic information exchange among the serviced CNDS providers.

E3.3.2.3.4. Management and implementation of the CNDS certification and accreditation process (further described in enclosure 4 of this Instruction).

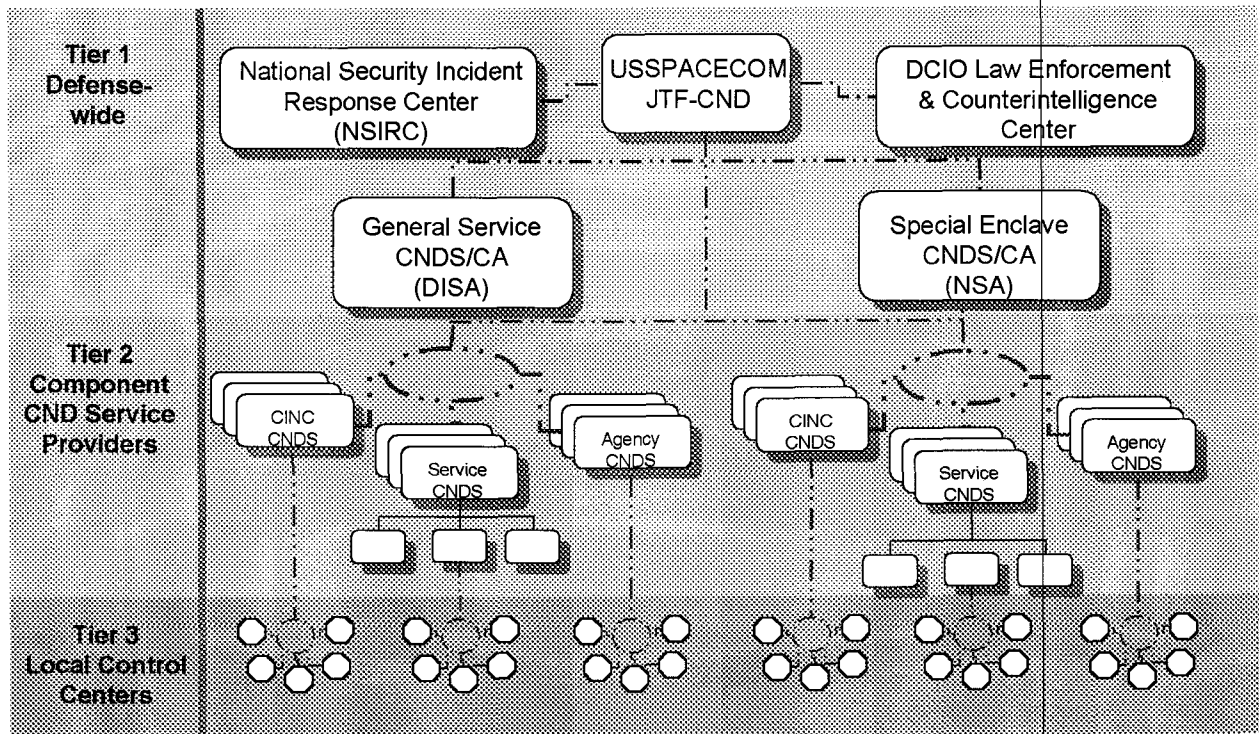
E3.3.2.4. Provide specialized Defense-wide services.

E3.3.2.4.1. The National Security Incident Response Center (NSIRC) provides overall focus and coordination for Attack Sensing and Warning and provides specialized analysis for discovery of Defense-wide and long term patterns.

E3.3.2.4.2. The CND LE&CI Center coordinates CND investigations and operations among the DoD Components, functions as integrated information exchange and operational interface between the DoD Components and USCINCSpace, and serves as the primary interface between DoD and the NIPC for CND related LE&CI issues.

E3.3.2.5. Permit the DoD Component CND elements to remain distributed, heterogeneous and autonomous, while providing for dynamic command and control.

E3.3.2. The USCINCSpace provides leadership and direction for the organization and evolution of the operational hierarchy, which is summarized in figure E3.F6.



Tier	Description	Organizational Entities
1	<p>Provides DoD-wide CND operational direction or support to all DoD Components</p> <p>Centrally coordinates and/or directs CND operations that impact more than one DoD Component</p> <p>Provides Defense-wide situational awareness and attack sensing and warning through fusion, analysis and coordinated information flows</p> <p>Supports Component situational awareness and attack sensing and warning</p> <p>Coordinates CND related LE&amp;CI investigations and operations that cross DoD Component or Federal Department/Agency bounds</p> <p>Coordinates development of baseline CND (and supporting IA)</p> <p>Education, Training and Awareness curriculum and products</p>	<p>USCINCSpace</p> <p>CND Service Certification Authorities (CNDS/CA)</p> <p>NSIRC</p> <p>CND LE&amp;CI Center</p>
2	<p>Responds to direction from Tier One</p> <p>Provides DoD Component-wide operational direction or support</p> <p>Provides DoD Component situational awareness and attack sensing and warning and supports Tier 1 situational awareness and attack sensing and warning through coordinated reporting and information flows</p>	<p>CNDS providers designated by Heads of Components to coordinate Component-wide CND</p>
3	<p>Responds to direction from servicing Tier Two CNDS</p> <p>Supports Tier 2 situational awareness and attack sensing and warning through coordinated reporting and information flows</p>	<p>Local control centers that manage and control information systems, networks and services, either deployed or fixed at DoD Installations</p>

Figure E3.F6. DoD CND Operational Hierarchy

E4. ENCLOSURE 4COMPUTER NETWORK DEFENSE (CND) SERVICESE4.1. INTRODUCTION

E4.1.1. This Enclosure describes CND Services, their composition and the functions of the tiers in the DoD CND Operational Hierarchy (see Enclosure 3) that provide those Services.

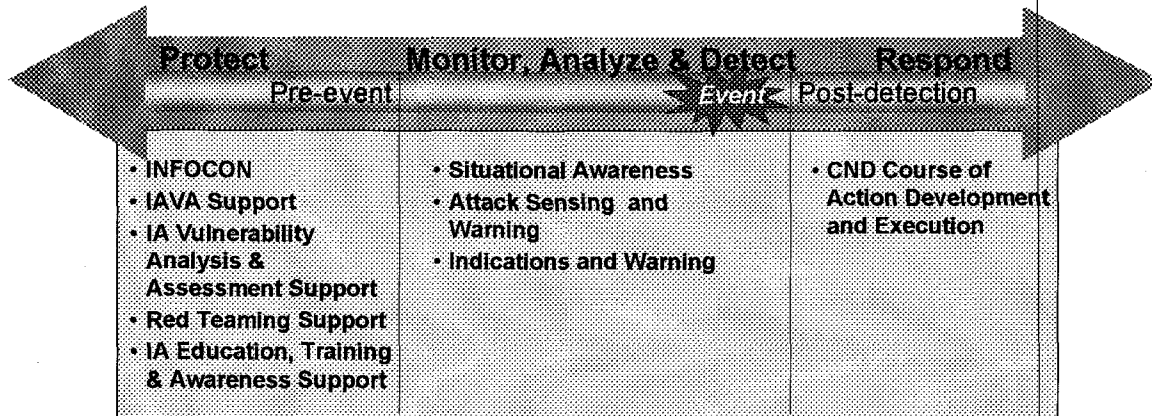


Figure E4.F1. CND Services

E4.1.2. CND Services are a standard, certified, continuously measured suite of services that are organized along the Protect; Monitor, Analyze & Detect; and Respond paradigm, as illustrated in figure E4.F1. Defense-wide services are planned, coordinated, and directed by Tier 1. Component-wide services are planned, coordinated, directed, and implemented by Tier 2. Local services are planned and implemented by Tier 3. See enclosure 3 for a discussion of the CND tiers.

E4.2. CND PROTECT SERVICES

E4.2.1. Information Operations Conditions (INFOCON) are intended to uniformly raise or lower defensive posture, to respond to unauthorized activity (e.g., computer network attacks, computer network exploitation, system misuse), and to mitigate potential damage to DoD information systems and computer networks.

E4.2.1.1. Tier 1: The USCINCSpace is the authority for changes in the DoD INFOCON level, and is the administrator of the INFOCON system. INFOCON levels can be changed by Tier 2 or Tier 3 level authorities to a level more restrictive than the level established by USCINCSpace.

E4.2.1.2. Tier 2: CNDS providers support the INFOCON system by:

E4.2.1.2.1. Maintaining INFOCON, implementing INFOCON changes and complying with USCINCSpace reporting requirements.

E4.2.1.2.2. Monitoring the current INFOCON and providing information and recommendations to the USCINCSpace and serviced Components.

E4.2.1.2.3. Monitoring Tier 3 compliance with changes in INFOCON and advising the USCINCSpace and serviced Components regarding compliance status and issues related to compliance.

E4.2.1.2.4. Supporting serviced Components in assessing the impact of INFOCON changes on missions and operations.

E4.2.1.2.5. In coordination with the USCINCSpace, serviced Components, and serviced Tier 3 entities, continuously improving the INFOCON definitions and system.

E4.2.1.2.6. Supporting Component INFOCON system extensions as required.

E4.2.1.3. Tier 3 entities support INFOCON by implementing INFOCON changes and complying with INFOCON reporting requirements.

E4.2.2. The Information Assurance Vulnerability Alert (IAVA) process is a positive control system that provides a Defense-wide mechanism to ensure all entities are informed of newly identified system vulnerabilities and deficiencies, and receive and implement appropriate corrective measures. While IAVA is a traditional Information Assurance (IA) activity, it is essential to CND as a primary means of improving the CND posture of DoD information systems and computer networks. DoD Components may establish a similar capability for further disseminating this type of information as long as there is clear linkage to the appropriate IAVA notification ("IAVA" is a reserved term used for Defense-wide alerts only). Enclosure 6 provides policy and guidance for the DoD IAVA process.

E4.2.2.1. Tier 1: The USCINCSpace is the DoD monitor for IAVA compliance and assessing impact on defense of DoD computer networks. USCINCSpace may coordinate and direct actions in response to IAVA non-compliance that impacts defense of DoD computer networks. The IAVA system is managed by the Defense Information Systems Agency (DISA); IAVAs are initiated by DISA and monitored by the CNDS/CAs.

E4.2.2.2. Tier 2: CNDS providers support the IAVA process by:

E4.2.2.2.1. Monitoring the implementation of all IAVAs and providing technical assistance to Tier 3 as required.

E4.2.2.2.2. Deconflicting Component-specific and information system-specific guidance with IAVAs as required.

E4.2.2.2.3. Providing technical support to serviced Components in the development, dissemination, and management of Component vulnerability guidance.

E4.2.2.2.4. Identifying system vulnerabilities or threats to the CNDS/CAs for inclusion in IAVAs.

E4.2.2.2.5. Providing feedback to the CNDS/CAs for improvement of the IAVA system and process.

E4.2.2.3. Tier 3 entities support IAVAs by implementing all IAVAs and complying with IAVA reporting requirements.

E4.2.3. Vulnerability Analysis and Assessments (VAA) for DoD information systems and computer networks originate from a number of programs, systems, and organizations. They typically differ according to the systems and networks included; the VAA objectives; the duration and the methodologies employed; the targeted recipients of the outputs and the outputs themselves. While VAA is a traditional IA activity, it is essential to CND as a primary means of measuring the CND posture of DoD information systems and computer networks. Achieving a comprehensive view of VAA activity within the CND serviced area is essential and challenging.

E4.2.3.1. Tier 1: The USCINCSpace is the authority for the deconfliction of VAAs and Red Teaming (see succeeding paragraph) with CND operations, and may direct changes to in-progress or planned VAAs that may negatively impact CND operations. The CNDS/CAs support VAAs by:

E4.2.3.1.1. Establishing and implementing a Defense-wide process for VAA notification, reporting and coordination.

E4.2.3.1.2. Identifying Defense-wide VAA programs and schedules and assessing their impact to CND operations.

E4.2.3.1.3. Coordinating with VAA providers to incorporate CND issues and requirements.

E4.2.3.1.4. Incorporating VAA results into the CND certification and accreditation process and other CND support activities.

E4.2.3.2. Tier 2 CNDS providers support VAAs by:

E4.2.3.2.1. Supporting serviced Components and Tier 3 entities in identifying and cataloging VAAs that may be performed within the serviced area and by whom. This includes related programs such as Critical Infrastructure Protection, Information Operations, Law Enforcement, and Counterintelligence VAAs as well as IA VAAs.

E4.2.3.2.2. Assessing the potential impact of VAAs to CND situational awareness and operations and coordinating or directing changes to in-progress or planned VAAs that may negatively impact CND operations.

E4.2.3.2.3. Supporting serviced Components and Tier 3 entities in the implementation of Defense-wide VAA notification and reporting requirements.

E4.2.3.2.4. Supporting serviced Components in the establishment and implementation of Component-specific VAA notification, reporting, and coordination requirements.

E4.2.3.2.5. Supporting serviced Components and Tier 3 entities in an assessment of the potential impact of each VAA to military or support operations.



E4.2.3.2.6. Working with VAA providers to incorporate CND related requirements for information collection and performance measurement.

E4.2.3.2.7. In coordination with the USCINCSpace, identifying requirements for and supporting VAAs directed at CND-related systems.

E4.2.3.2.8. Providing feedback to and incorporating VAA lessons learned into the INFOCON system, the IAVA system, IA Education, Training, and Awareness (ETA) programs, the certification and accreditation process, and the Information Assurance programs of serviced Components.

E4.2.3.3. Tier 3 entities support VAAs by complying with Tier 1 and Tier 2 direction regarding the deconfliction of VAAs with CND and by complying with VAA notification, reporting, and coordination requirements.

E4.2.4. Red Teaming is essential to gauge the state of CND operational readiness of the DoD Components and the networks that sustain their operations. This activity is fundamentally different than the VAA in that it is an independent and threat based activity that simulates an opposing force and is focused on readiness improvements. Red Team support is available from NSA and may be available at the DoD Component level. Red Teams emulate the capabilities and methods of an adversarial force against DoD information systems, including systems under development. Red Teams are requested at the system owner's (or developer's) request and based on a defined scenario, Red Teams become knowledgeable of the target system(s), match their approach to the adversary threat environment for the target, gather appropriate tools to attack the system, and train to effect the attack. The Red Team then deploys to launch the assault, documenting the vulnerabilities and suggesting countermeasures. Red Teams work closely with system owners, demonstrating how the attacks were run, and how owners can protect their systems. Red Teams provide an accurate assessment on which system owners and developers can make coherent risk management decisions concerning their information systems, networks, and supporting infrastructure.

E4.2.4.1. Red Teaming activities, like VAAs, originate from a number of programs, systems, and organizations while conforming to a DoD standard methodology. Because they may originate from a number of sources, impact situational awareness, negatively impact the defensive posture of the targeted information systems and computer networks during conduct, and inform the improvement of information assurance and computer network defense capabilities, they are an item of interest to CND operations.

E4.2.4.2. Tier 1: The USCINCSpace is the authority for deconflicting Red Teaming activity with CND operations, and may direct changes to in-progress or planned Red Teaming activities that may negatively impact CND operations. The National Security Agency is responsible for the establishment and maintenance of a trusted agent network and procedures for the reporting of Red Teaming activities and for tracking Red Team and VAA activities in support of Special Enclaves. DISA is responsible for tracking Red Team and VAA activities in support of General Service Enclaves. The DoD Component initiating Red Team activity is responsible for coordination with affected parties and obtaining necessary authorization for the activity.

E4.2.4.3. Tier 2: CNDS providers support Red Teaming much the same way they support VAAs:

E4.2.4.3.1. Supporting serviced Components and Tier 3 entities in the implementation of Defense-wide Red Teaming notification and reporting requirements.

E4.2.4.3.2. Assessing the potential impact of Red Teaming activities to CND situational awareness and operations and coordinating or directing changes to in-progress or planned activities that may negatively impact CND operations.

E4.2.4.3.3. Supporting serviced Components in the establishment and implementation of Component-specific Red Teaming notification, reporting, and coordination requirements.

E4.2.4.3.4. Supporting serviced Components and Tier 3 entities in an assessment of the potential impact of each Red Teaming activity to military or support operations.

E4.2.4.3.5. Working with Red Teams to incorporate CND related requirements for information collection and performance measurement.

E4.2.4.3.6. In coordination with the USCINCSpace, identifying requirements for and supporting Red Teaming activities directed at CND operations.

E4.2.4.3.7. Providing feedback to and incorporating Red Teaming lessons learned into the INFOCON system, the IAVA system, IA Education, Training, and Awareness programs, the certification and accreditation process, and the Information Assurance programs of serviced Components.

E4.2.4.4. Tier 3 entities support Red Teaming by complying with Tier 1 and Tier 2 direction regarding the deconfliction of Red Teaming activities with CND and by complying with Red Teaming notification, reporting, and coordination requirements.

E4.2.5. Information Assurance Education, Training, and Awareness (IA ETA) forms the basis for a robust CND capability. IA ETA also provides the means to coordinate a consistent level of knowledge across DoD Components. IA ETA, like the VAA process, is highly decentralized.

E4.2.5.1. Tier 1: The USCINCSpace is the DoD advocate for IA ETA as it relates to CND. The Certification Authorities must develop a coordinated curriculum for CND education training, awareness, professionalization, and ensure the implementation of the curriculum throughout the CNDS certification and accreditation process.

E4.2.5.2. Tier 2 CNDS providers support IA ETA by:

E4.2.5.2.1. Working with Tier 3 serviced entities and serviced Components to identify their CND-specific IA ETA requirements.

E4.2.5.2.2. Supporting the serviced Components as required in the establishment and management of IA ETA tracking systems.

E4.2.5.2.3. Working within the CND operational hierarchy and with the program managers of the DoD Computer Forensics Laboratory and DoD Computer Investigations Training Program to identify CND specific education, training, and awareness requirements for CNDS providers and with the CNDS Certification Authorities to ensure that they are incorporated into the CNDS Certification and Accreditation Program.

E4.2.5.2.4. Working with ETA providers to incorporate CND requirements and objectives into ETA curricula and courseware and providing technical support in course development.

E4.2.5.2.5. Working within the CND operational hierarchy and with serviced Components to determine requirements for a shared synthetic training and rehearsal environment.

E4.2.5.2.6. Provide CND ETA requirements to Tier 1 to insure a coordinated CND curriculum is developed.

E4.2.5.3. Tier 3 entities support IA ETA by:

E4.2.5.3.1. Identifying Component level IA ETA requirements.

E4.2.5.3.2. Complying with Tier 1 and Tier 2 requirements and guidance.

#### E4.3. CND MONITOR, ANALYZE and DETECT SERVICES

E4.3.1. Situational awareness is the key to effective CND. A robust situational awareness capability is mandated by the highly interconnected nature of the DoD information systems and computer networks; the degree to which they share risk; and the coordination and synchronization requirements of response efforts. Situational awareness is enabled by an interoperable suite of information systems that collectively support and comprise a Common Operational Picture (COP).

E4.3.1.1. Constructing a COP is a top down and a bottom up endeavor. A common operational picture is required that is both Defense-wide and tailored to a hierarchy of decision-makers in a dynamic command and control construct. Managing and collecting information in and for a dynamic environment is inherently complex. Many factors contribute to that complexity, for example:

E4.3.1.1.1. The optimum set of data elements is inherently dynamic, changing as the computer network environment, the DoD operational environment and the threat change, as the DoD CND capability matures, and as technology evolves to support CND. Additionally, the optimum subset for decision support changes as control shifts up and down the operational hierarchy.

E4.3.1.1.2. Both the optimal and the obtainable refresh rates for the required data elements are inherently dynamic. Each rate is continuously moving toward real time but is

constrained by the rates of the set itself in that extremely disparate refresh rates among individual data elements can distort or falsify the resulting fused picture.

E4.3.1.2. The major Components of the CND COP are:

E4.3.1.2.1. A shared picture of the DoD global information and computing networks and the military and business operations they supports, to include notice of any impending changes in configuration, capacity, utilization, assurance posture, user priorities, or criticality of support for military operations. An understanding and visualization of these global systems is required for all Network Operations elements – network management, information dissemination management, and information assurance – therefore, the development and maintenance of the network operational picture is not the exclusive responsibility of CND. Rather, the CND COP incorporates and builds upon the operational picture of the DoD global network COP that is common to all Network Operations elements.

E4.3.1.2.2. A shared picture of the threat developed from all sources. These sources include foreign intelligence; Federal law enforcement; National counterintelligence; Defense law enforcement, Defense counterintelligence, other security sources; private sector infrastructure service and computer emergency response providers and, and other open sources. E.O. 12333 (reference (i)) applies to both DoD and non-DoD intelligence and counterintelligence units. DoD Directive 5240.1 (reference (j)) and DoD 5240.1-R (reference (k)) govern the activities of all DoD intelligence units and non-intelligence units performing intelligence activities.

E4.3.1.2.3. A shared picture of CND operations, e.g., effective INFOCON levels and status of compliance, status and compliance of IAVAs, schedule and status of VAAs, status of CND COA development and execution, as well as impending changes to CND services.

E4.3.1.3. In addition to a Defense-wide shared picture, the COP seeks to enable contributing communities by promoting "community specific COPs." Communities may be organizational, e.g., DoD Component, or functional, e.g., the Defense Law Enforcement community. The community specific COPs are intended to:

E4.3.1.3.1. Provide the ability to collect, organize, process, manage and disseminate CND related information within the community at a level of detail greater than the CND COP.

E4.3.1.3.2. Support the development and improvement of standard processes for community support to CND.

E4.3.1.3.3. Support the standardization and availability of information required for the DoD CND COP.

E4.3.1.4. Tier 1: The USCINCSpace establishes CND requirements for the CND COP. The certification authorities maintain common Defense-wide aspects of the COP by:

E4.3.1.4.1. Contributing Component and relevant functional CND information to the COP.

E4.3.1.4.2. Coordinating informational needs with Tier 2 entities to ensure a Defense-wide CND COP.

E4.3.1.4.3. Assisting Tier 2 entities to meet reporting and information input requirements.

E4.3.1.5. Tier 2 CNDS providers support situational awareness by:

E4.3.1.5.1. Working with and supporting the CND Architect and the CND Systems Integrator to identify requirements, and to develop, deploy and maintain information systems.

E4.3.1.5.2. Working with serviced Tier 3 entities and Components to ensure that CND COP information is timely and accurate.

E4.3.1.5.3. Working with serviced Components to identify Component-unique requirements and support their development, deployment and maintenance.

E4.3.1.5.4. Assisting Tier 3 entities to meet reporting and information input requirements.

E4.3.1.6. Tier 3 supports situational awareness by complying with reporting requirements and providing information inputs to the COP.

E4.3.2. Indications and Warning (I&W) is defined as 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/coalition military, political, or economic interests or to U.S. citizens abroad. It includes forewarning of enemy actions or intentions; the imminence of hostilities; insurgency; nuclear/non-nuclear attack on the United States, its overseas forces, or allied/coalition nations; hostile reactions to U.S. reconnaissance activities; terrorists' attacks; and other similar events.

E4.3.2.1. Tier 1: The USCINCSpace provides the Intelligence Community (IC) with priority intelligence requirements (PIR) and indications and warning requirements for potential attacks against DoD information systems and computer networks. The Defense Intelligence Agency (DIA) coordinates IC support to the USCINCSpace.

E4.3.2.2. Tier 2: DoD Components provide PIR input to the USCINCSpace, and in coordination with the USCINCSpace and DIA, determine direct intelligence support to the CNDS providers.

E4.3.2.3. Tier 3 implements Tier 1 and Tier 2 direction.

E4.3.3. Attack sensing and warning (AS&W) is defined as 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. Attack sensing and warning also includes attack/intrusion related intelligence collection tasking and dissemination; limited immediate response recommendations; and limited potential impact assessments.

E4.3.3.1. AS&W focuses not only on actual intrusions or misuse, but also preparatory actions or preliminary network conditions that signify that an incident is likely, is planned, or is under way. This service is supported by both intelligence and counterintelligence indications and warning of foreign or foreign-sponsored developments, and law enforcement products regarding domestic criminal activity. Information system and computer network owners and operators are the most likely detectors of changes in network state, and must therefore be considered full partners in the AS&W process.

E4.3.3.2. Attack sensing and warning and situational awareness are inextricably linked. The complexity of constructing a COP is complicated by the requirement to optimize COP data collection and exchange requirements with AS&W requirements. Like the COP, an integrated AS&W system must conform to the construct and operating principles of the CND operational hierarchy. It must permit control to dynamically shift from tier to tier, be supported by a robust common repository of information, and enable the establishment of community or function-specific supporting repositories.

E4.3.3.3. AS&W requires an in-depth understanding of vulnerabilities in information technologies and of intrusion or computer attack strategies that can exploit these vulnerabilities. The innovative fusion of traditional intelligence information with systems and network monitoring and reporting information is essential for effective AS&W. Analysis of intrusion data using specially developed exploitation tools can uncover intrusion, exploitation or attack techniques that may be overlooked by other analysis. Operational analysis for AS&W requires an understanding of network mapping and net reconstruction, the analysis of system intrusion data, and protocol and bit stream analysis.

E4.3.3.4. The results of time-sensitive CND and the correlation, fusion and technical analysis of incidents, intrusions and events requires automatic transfer of alerts, advisories, threat reports, and response recommendations. Formal reporting procedures and formats are necessary to exchange raw and processed information on detected intrusions, and to deliver timely and effective warning and response coordination products. AS&W is comprised of the following:

E4.3.3.4.1. The CND Sensor Grid, a coordinated constellation of intrusion, misuse and anomaly detection systems deployed throughout the DoD global networks.

E4.3.3.4.2. Data repositories or warehouses that archive data from the Sensor Grid and other sources in order to support long term analysis, diagnostics and pattern discovery plus supporting tools and techniques.

E4.3.3.4.3. AS&W analysts.

E4.3.3.4.4. Procedures and communication channels for warning.

E4.3.3.4.5. A research and engineering Component for continuous technological and analytical advancement.

E4.3.3.5. The CND Sensor Grid and the Tier 3 entities comprise the foundation of the Department's AS&W capability and are key contributors to situational awareness, although

neither is dedicated to CND. As technologies converge and the Sensor Grid matures, it will continue to expand in functionality toward a true Network Operations Sensor Grid, enabling, for example, Network Management capacity and performance management functions and Security Management identification and authentication functions. For CND, the Sensor Grid provides the ability to:

E4.3.3.5.1. Enable an operational capability throughout the DoD global networks.

E4.3.3.5.2. View network and system activity in real-time.

E4.3.3.5.3. Discover, detect and guide further investigation.

E4.3.3.5.4. Identify unauthorized activity and engage and control it in real-time, to include some near-real-time automated response.

E4.3.3.5.5. Analyze current activity in view of past activity in order to identify larger trends and problems.

E4.3.3.5.6. Collect information to support AS&W, an analytic service that builds upon intrusion, misuse and anomaly detection.

E4.3.3.5.7. Collect information to support continued intrusion, misuse, and anomaly detection and AS&W research.

E4.3.3.6. Tier 1: The USCINCSpace establishes requirements and direction for AS&W as part of its responsibilities for the National Security Incident Program as defined in NSTISSD 503 (reference (1)). The NSIRC facilitates AS&W cooperation and coordination within the DoD CND operational hierarchy, and it provides additional support to the Department of Defense to:

E4.3.3.6.1. Provide direct support to the USCINCSpace for AS&W.

E4.3.3.6.2. Provide specialized analysis for discovery of Defense-wide and long term patterns.

E4.3.3.6.3. Provide overall focus and coordination for the AS&W service.

E4.3.3.7. Tier 2 CND providers support AS&W by:

E4.3.3.7.1. Working with and supporting the CND Architect and the CND Systems Integrator to identify requirements and to develop, deploy, and maintain information systems.

E4.3.3.7.2. Working with the CND Research and Technology Program Manager to develop and evaluate emerging AS&W technologies.

E4.3.3.7.3. Conducting or supporting AS&W in accordance with Tier 1 established agreements, standards, and protocols.

E4.3.3.7.4. Working with serviced Tier 3 entities and Components to ensure that CND AS&W information is timely and accurate.

E4.3.3.7.5. Working with Serviced Components to identify Component-unique requirements and support their development, deployment and maintenance.

#### E4.4. CND RESPONSE SERVICES

E4.4.1. The USCINCSpace is responsible for managing the DoD process for CND Course of Action (COA) development and execution, and developing supporting documentation (e.g., doctrine; tactics, techniques and procedures; OPLANs and CONPLANs).

E4.4.2. Tier 2 CNDS providers support CND COA development and execution by:

E4.4.2.1. Supporting Tier 1 in COA development.

E4.4.2.2. Following the operational direction of Tier 1 for COA execution and executing CND COAs in accordance with Tier 1 established doctrine; tactics, techniques and procedures.

E4.4.2.3. Working with serviced Tier 3 entities and Components to ensure effective lines of command, control, communication, and coordination.

E4.4.2.4. Working with serviced Tier 3 entities and Components to ensure that information supporting COA development and execution is timely and accurate.

E4.4.2.5. Working with serviced Components to identify Component requirements and ensure their incorporation in COAs.

E4.4.3. Tier 3 entities follow the operational direction of Tier 2 for COA development and execution.



## E5. ENCLOSURE 5

### COMPUTER NETWORK DEFENSE (CND) SUPPORT FUNCTIONS

#### E5.1. INTRODUCTION

E5.1.1. This Enclosure describes the activities that provided essential support to the DoD CND Operational Hierarchy (see enclosure 3) and CND Services (see enclosure 4).

E5.1.2. CND Support Functions assist in managing special services and capabilities under development within the CND community. The CND Support Functions aid in the administration, program management, and oversight of CND capabilities on a Defense-wide basis. CND Support Functions program management is established through certification and accreditation of CND Services, standardization of common security practices, development of a CND architectural framework, and oversight of CND research and technology (R&T) initiatives.

#### E5.2. SPECIAL ENCLAVE/GENERAL SERVICE DESIGNATION

For the purposes of CND, all DoD information systems and computer networks are labeled as either General Service or Special Enclave. CND Services (CNDS) must be certified and provided at one of these two security levels. Special Enclave systems and networks are those designated by the ASD(C3I) as requiring special security. Any information system or computer network not designated as Special Enclave is considered General Service. Special Enclave systems and networks shall be assigned to CNDS Providers that are certified for Special Enclave Services. The CND Architect manages the Special Enclave designation process.

#### E5.3. CND ARCHITECT

E5.3.1. The CND Architect 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 insures CND requirements are incorporated into the DoD C4ISR Architectural Framework (reference (b)) and Joint Technical Architecture (reference (c)).

E5.3.2. The CND Architect facilitates the development of the CND aspects of the operational, systems and technical architecture views. Heads of Components have a responsibility to ensure that ALL their information systems and computer networks are provided support by certified CNDS providers and that ALL Component-established CND Services are certified and accredited. The CND Architect interacts with all Components to ensure that these responsibilities are met. Components ensure compliance by:

E5.3.2.1. Maintaining a master inventory of Component information systems and computer networks (defined as those systems and networks separately accredited by a DAA in accordance with DoD Instruction 5200.40 (reference (d))).

E5.3.2.2. Developing a CND architecture to both facilitate CND policy, CND requirements generation and development, acquisition, Planning, Programming and Budgeting System activities, force structure and force management activities, and operational process improvement.

E5.3.2.3. Ensuring that Special Enclave systems and networks are so designated.

E5.3.2.4. Ensuring that all Component information systems and computer networks are supported by an certified CNDS provider, and that support is established as a condition of system accreditation in accordance with DoD Instruction 5200.40 (reference (d)).

E5.3.2.5. Tracking the certification and accreditation of all Component-established CNDS providers.

E5.3.2.6. Providing guidance and oversight regarding arrangements with non-Component CNDS providers.

E5.3.3. In addition to maintaining an operational view of CND for Component assets in compliance with the DoD C4ISR Architecture Framework (reference (b)), the CND Architect works with the Components to coordinate CND-related system requirements and ensure Component compliance with the Joint Technical Architecture (reference (c)). Specifically, the CND Architect works with Components to ensure that they:

E5.3.3.1. Establish Component requirements for COP.

E5.3.3.2. Track and comply with Component responsibilities and efforts toward development of information systems or databases supporting Defense-wide CND.

E5.3.3.3. Track Component sensor grid requirements and implementation.

E5.3.3.4. Respond to requests for information from the CND Architect and support CND Architect-sponsored activities.

E5.3.3.5. Support Defense-wide Information Assurance Program (DIAP) planning and programming integration activities relative to CND.

E5.3.4. The CND Architect provides oversight and direction for the certification and accreditation process.

#### E5.4. CNDS CERTIFICATION AND ACCREDITATION Process

E5.4.1. The CNDS/CAs work together and in conjunction with the CND Architect to establish and implement the certification and accreditation process. The certification and accreditation process will include a CNDS capability maturity model, CNDS best practices, and self-assessment and independent assessment methods, service performance metrics, individual capability maturity models, and models to determine optimum staffing and workload levels. The capability maturity models will link education, training, and certification standards and requirements to organizational capabilities.

E5.4.2. The CNDS/CAs, in conjunction with Heads of Components, will develop a coordinated Defense-wide CND educational curriculum integrated with DoD's IA educational curriculum and continuously improve it through the incorporation of best practices and needs.

E5.4.3. The CNDS/CAs, in conjunction with the CND R&T Program Manager and Heads of Components, will identify CNDS requirements and ensure that new technology is transitioned into acceptable DoD CNDS practices.

E5.4.4. The CNDS capability maturity model will address all CND Services described in Enclosure 4 as well as subscription and reporting requirements, service level agreements, and any additional process areas identified by the CND Architect or the USCINCSpace.

E5.4.5. In addition to managing certification and process improvement, the CNDS/CAs will provide an active and ongoing coordination service for all associated Tier 2 CNDS providers. This includes dynamic information exchange among the CNDS providers and management of the exchange protocols and technical and analytic support. The CNDS/CAs also provide technical and analytic support to the USCINCSpace and to Component CNDS providers as required.

#### E5.5 CND RESEARCH AND TECHNOLOGY PROGRAM MANAGEMENT

E5.5.1. The CND Research and Technology Program Manager coordinates development and evaluation of tools and techniques to support CND operations; develops and evaluates attack sensing and warning emerging technologies; and supports the CND procurement and logistics activities of the DoD Components, to include enterprise-wide licensing of CND tools.

E5.5.2. To support these efforts, the Program Manager chairs a CND technology transition steering group whose members include USCINCSpace, the Joint Staff, the CND Architect, the DIAP, the CNDS/CAs and the DoD Components. The CND technology transition steering group shall host regular reviews of DoD and Component requirements and technology transition efforts.

E5.5.3. The Program Manager:

E5.5.3.1. Has program coordination responsibility for Defense-wide issues related to CND technology transition.

E5.5.3.2. Develops, in coordination with the DoD Components, a comprehensive view of all CND R&D requirements and technology transition programs.

E5.5.3.3. Reports to the Director Defense Research and Engineering (DDR&E) and the DIAP on these R&D requirements and technology transition plans and activities.

E5.5.4. The Program Manager provides support to the CND Architect, OSD and the Joint Staff in the identification and resolution of CND technology transition program issues.

## E5.6. CND INTEGRATION INTO DOD INFORMATION SYSTEMS

E5.6.1. The Systems Integrator coordinates Sensor Grid systems engineering, implementation and integration; coordinates COP requirements, design and integration; and develops and maintains COP common databases and utilities.

E5.6.2. To support these efforts, Systems Integrator chairs a regular CND systems working group under the Military Communications and Electronics Board (MCEB) Information Assurance Panel (IAP) to address COP and Sensor Grid architecture, engineering, and deployment. Membership includes but is not limited to those Components responsible for development of the COP system. Figure E5.F1. details a listing of member agency and CND COP development responsibilities.

DoD Component	CND COP Development Responsibility
DISA	CND Systems Integrator General Service Network Operations COP Common databases and utilities Systems support for USCINCSpace requirements General Service CNDS Education and Training
USCINCSpace	CINC input
Navy	Counterintelligence input and community view
DoD IG	Law Enforcement input and community view
DIA	Intelligence input and community view
NSA	Special Enclave Network Operations COP Special Enclave CNDS
DoD Component	Component view (optional)

Figure E5.F1. Component Responsibilities for CND Common Operational Picture.

## E6. ENCLOSURE 6

### INFORMATION ASSURANCE VULNERABILITY ALERT (IAVA)

#### E6.1. INTRODUCTION

E6.1.1. This enclosure provides policy and guidance for the DoD information assurance vulnerability alert (IAVA) process. The IAVA process supports the protection of DoD systems against known or identified vulnerabilities. IAVA also provides a positive control mechanism to ensure system administrators receive, acknowledge, and comply with vulnerability alert notification and to ensure that corrective actions were taken against new and critical vulnerabilities. The IAVA process assists in mitigating vulnerabilities that may impact mission effectiveness or operational readiness.

E6.1.2. Requirements and Responsibilities. Within DoD the IAVA provides the means to incorporate positive control of vulnerability notification and corresponding corrective action. The IAVA process is managed by the Defense Information systems Agency (DISA). In coordination with USCINCSpace through the Joint Task Force - Computer Network Defense (JTF-CND), DISA processes and distributes IAVA alerts to all Component points of contact. The IAVA is an Internet Web-based process that is pre-coordinated with CNDS providers for action to ensure corrective measures have been implemented. The CNDS/CAs monitor IAVA activity, to include compliance.

E6.1.3. IAVA Notification. IAVAs are generated whenever a critical vulnerability exists that poses an immediate threat to DoD and where acknowledgement and corrective action compliance must be tracked. Not all identified vulnerabilities and threats will warrant an IAVA. After an initial evaluation, a request for comments is sent to a coordination team consisting of JTF-CND, Component CNDS providers, and joint system program managers. This team provides input in determining the type of notification to be generated. IAVAs are promulgated via organizational messaging. The message is for notification only and directs recipients to check the DoD Computer Emergency Response Team's (CERT) Internet web site ([HTTP://WWW.CERT.MIL](http://www.cert.mil)) for technical specifications and corrective action. IAVAs will expire after three years unless otherwise specified and may be modified or superceded, as more technical information becomes available.

E6.1.4. IAVA Acknowledgement Procedures. All Heads of the DoD Components shall designate a primary and secondary point of contact (POC) responsible for IAVA acknowledgement and reporting. Acknowledgement of receipt of the IAVA notifications is required within five days of the date of the AUTODIN/DMS message or with the timeframe specified in the message itself. Dissemination of the IAVA within Component channels is conducted by all program managers, system administrators, and or other personnel responsible for the implementation and managing of technical responses to IAVAs.

E6.1.5. The DoD Components will report compliance with an IAVA notification via appropriate (unclassified or classified) IAVA web site within 30 days of the date of the message, or as specified in the individual message. Component program manager reports will be included

in the overall compliance report. For reporting purposes, assets include all components (i.e., hardware and software) of information systems comprising or assessing a networked environment. Compliance information shall include at a minimum: the number of assets affected; the number of assets in compliance; and the number of assets with waivers.

E6.1.6. Configuration Management. Maintaining positive configuration control of all information systems/assets under a component's purview supports the integrity of the IAVA process.

E6.1.6.1. The DoD Components will maintain configuration documentation that identifies specific system/asset owners and system administrator(s), including applicable electronic addresses.

E6.1.6.2. Networked assets will be managed and administered in a manner allowing for both chain-of-command and authorized independent verification of corrective actions.

E6.1.6.3. The DoD Components will modify contracts for DoD information system asset management to reflect the above performance requirements (i.e., paragraphs E6.1.4 and E6.1.5) for IAVA acknowledgement and reporting. This includes contracts being developed that will affect Defense Information Infrastructure (DII) assets (utilize, administer, or integrate IT or communication assets into the DII).

E6.1.6.4. The DoD Components will also establish a process to periodically review any waivers prior to their expiration date.

E6.1.7. In support of the IAVA process, the DoD Components will register with the DISA for assignment of a web-site user-ID and password. On receipt of an IAVA notification Component POC's must enter their organization's acknowledgment and compliance data into the IAVA database.

E6.1.8. Waivers. Designated Approving/Accrediting Authorities (DAA's) have the authority to waive compliance with a specific IAVA notification, if appropriate, following a risk assessment and determination of other risk mitigating actions. Waivers shall be for the minimum length of time required to achieve compliance with the IAVA notification. The DAA must consider the risks involved, to both the local network and the greater DII when granting a waiver. Specific technical questions regarding individual IAVAs should be addressed to the DoD CERT via e-mail at ([cert@cert.mil](mailto:cert@cert.mil)).