Department of Defense

DIRECTIVE

Canceled by: _____

January 8, 2001
NUMBER O-8530.1

ASD(C3I)

SUBJECT: Computer Network Defense (CND)

References: (a) 10 U.S.C. 2224, "Defense nformation Assurance Program."
(b) DoD Directive 5137.1, "Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C31))," February 12, 1992
(c) DoD 5025.1-M, "DoD Directives System Procedures," August 1994
(d) 18 U.S.C. 2511(2)(a)(1), "Wire and Electronic Communications Interception and Interception of Oral Communications."
(e) through (l), see Enclosure E1.

1. PURPOSE

This Directive:

1.1. Establishes, in accordance with references (a) and (b), the computer network defense (CND) policy, definition, and responsibilities necessary to provide the essential structure and support to the Commander in Chief, U.S. Space Command (USCINCSPACE) for Computer Network Defense (CND) within Department of Defense information systems and computer networks.

1.2. Authorizes the publication of DoD 8530.1-R and 8530.1-M, consistent with DoD 5025.1-M (reference (c)).

2. APPLICABILITY AND SCOPE

This Directive:

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

The terms used in this Directive are defined in enclosure 2.

4. POLICY

It is DoD policy that:

4.1. All DoD information systems and computer networks shall be monitored in accordance with 18 U.S.C. 2511 (reference (d)) and DoD Directive 4640.6 (reference (e)) order to detect, isolate, and react to intrusions, disruption of services, or other incidents that threaten the security or function of DoD operations, DoD information systems or computer networks.

4.2. CND activities shall be coordinated among multiple disciplines, including network operations, law enforcement, counterintelligence, and intelligence, as well as with the actions and responsibilities of DoD information systems and computer network owners and users.

4.3. The DoD shall organize, plan, train for, and conduct defense of DoD computer networks as part of a DoD-wide operational hierarchy, including a CND Common Operational Picture (COP), a sensor grid, and a capabilities accreditation and certification process.

4.4. CND operations that impact more than one DoD Component are centrally coordinated and directed by USCINCSPACE.

4.5. All DoD Components shall establish or provide for a CND Service (CNDS).

4.6. All DoD Components shall implement robust infrastructure and information assurance practices, including but not limited to:

4.6.1. Comprehensive configuration management and certification and accreditation in accordance with DoD Instruction 5200.40 (reference (f)) to ensure Information Assurance is applied throughout the life-cycle of information systems and computer networks.

4.6.2. Regular and proactive vulnerability analysis and assessment, including active penetration testing and Red Teaming, and implementation of identified improvements.

4.6.3. Adherence to a defense-in-depth strategy using risk management principles to defend against both external and internal threats by employing both technical and non-technical means and multiple protections at different layers within information systems and computer networks.

4.6.4. Information assurance training, awareness, and certification for all information system and computer network providers, managers, administrators, support personnel and users.

4.6.5. A dissemination and compliance process for information assurance advisories and alerts.

4.7. CND be supported by an integrated activity that monitors and coordinates criminal and counterintelligence investigations and provides releasable information concerning those

investigations to the DoD Components to counter threats to DoD information systems and computer net works.

4.8. All appropriate elements of national power (e.g., diplomatic, military, economic) will be considered to deter and defeat foreign based or sponsored threats to the security of DoD operations, DoD information systems, or computer networks.

5. RESPONSIBILITIES

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

5.1.1. Provide policy direction and guidance for the development and implementation of CND.

5.1.2. Develop and incorporate information assurance and CND requirements in the Command, Control, Communications and Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) Architectural Framework (reference (g)) and the Joint Technical Architecture (JTA) (reference (h)).

5.1.3. In coordination with the Chairman, Joint Chiefs of Staff (CJCS) and the Under Secretary of Defense for Acquisition, Technology and Logistics, ensure that CND requirements are fully integrated into C4ISR and information technology related architectures, plans and programs.

5.1.4. Establish and provide oversight of a certification process for CND capabilities.

5.1.5. Designate, as appropriate, DoD information systems and/or computer networks with special security requirements as Special Enclaves.

5.1.6. Oversee, in coordination with the Under Secretary of Defense for Personnel and Readiness, applicable training and career development policy to ensure personnel are trained, specifically designated and available to support and participate in CND.

5.1.7. In conjunction with the CJCS and the USCINCSPACE, establish requirements for the CND COP and the CND sensor grid.

5.1.8. Oversee development, deployment, configuration management and assurance of the CND COP and the sensor grid.

5.1.9. Coordinate with the General Counsel, DoD, the Inspector General, DoD and the Secretaries of the Military Departments on policy guidance for DoD CND counterintelligence and law enforcement investigations and operations.

5.1.10. In conjunction with the Inspector General, DoD and the Secretaries of the Military Departments, establish aCND Law Enforcement and Counterintelligence (LE&CI) Center for coordination of LE&CI investigations and operations in support of CND.

5.1.11. Oversee DoD participation in the National Infrastructure Protection Center (NIPC) and ensure consideration of DoD interests and equities by the NIPC.

5.1.12. Develop and lead a process for periodic review of CND with the DoD Components that includes an assessment of Department effectiveness in meeting goals and objectives, an assessment of the performance of organizations in accomplishing their roles and responsibilities, and a review of threats and technologies impacting CND.

5.1.13. Approve, in accordance with DoD 5200.1-R (reference (i)), security classification guidance (SCG) and handling and release authority guidance for CND.

5.1.14. Require the Director, Defense Information Systems Agency (DISA)

5.1.14.1. Serve as the technical advisor to the ASD(C3I), the CJCS, and the USCINCSPACE for Defense-wide CND requirements.

5.1.14.2. Function as the Certification Authority for all General Service CNDS providers.

5.1.14.3. Provide CNDS support to DoD Component CNDS as required. Provide General Service CNDS on a subscription basis to any DoD Component that does not establish or otherwise subscribe to a General Service CNDS.

5.1.14.4. Establish advisory and alert procedures for General Service CNDS providers and technical alert support for USCINCSPACE release to network operators through established joint command and control channels. Provide CND trend and pattern analysis to USCINCSPACE and the DoD Components.

5.1.14.5. Serve as overall integrator for DoD CND-related systems.

5.1.15. Require the Director, Defense Intelligence Agency (DIA):

5.15.1. Oversee DoD intelligence requirements in support ofthe CND.

5.15.2. Manage Defense intelligence community production to support DoD CND.

5.15.3. Serve as the Defense intelligence community focal point for the design, development, and maintenance of information systems and databases that facilitate timely collection, processing, and dissemination of all-source, finished intelligence for CND and provide data to CND and the COP databases, as appropriate.

5.2. The Under Secretary of Defense for Acquisition, Technology and Logistics shall coordinate with the ASD(C3I) and the CJCS on matters of CND acquisition and acquisition policy to ensure that CND requirements are fully integrated into Command, Control, Communications, and Computer Systems (C4) and information technology related architectures, plans and programs.

5.3. The Under Secretary of Defense for Personnel and Readiness shall coordinate with the ASD(C3I) to develop applicable training and career development policy to ensure trained personnel are available to support and execute CND operations.

5.4. The General Counsel of the Department of Defense shall coordinate with the ASD(C3I) and the Inspector General, DoD to provide legal guidance on CND related counterintelligence and law enforcement investigations and operations.

5.5. The Inspector General of the Department of Defense shall:

5.5.1. In conjunction with ASD(C3I) and the Secretaries of the Military Departments, establish the CND LE&CI Center for coordination of law enforcement and counterintelligence activities in support of CND.

5.5.2. Coordinate with the General Counsel, DoD, the ASD(C3I), and the Secretaries of the Military Departments on policy guidance for law enforcement operations that support CND.

5.5.3. Require the Director, Defense Criminal Investigative Service (DCIS) to:

5.5.3.1. Provide administrative support to the CND LE&CI Center.

5.5.3.2. Serve, in coordination with the Secretaries of the Military Departments, as the Defense law enforcement community focal point for the design, development, and maintenance of information systems and databases that facilitate CND law enforcement operations and CND LE&CI Center requirements and provide data to CND and the COP databases, as appropriate.

5.6. The Chairman of the Joint Chiefs of Staff shall:

5.6.1. Serve as the principal military advisor to the Secretary of Defense on CND.

5.6.2. Coordinate with USCINCSPACE and other Commanders of the Combatant Commands to ensure effective planning and execution of CND.

5.6.3. Ensure plans and operations include and are consistent with CND policy, strategy, and doctrine.

5.6.4. Coordinate with USCINCSPACE to establish doctrine and instructions to facilitate the integration of CND into joint operations.

5.6.5. Ensure that exercises routinely test and refine CND operations, including the application of operational stress to information systems and computer networks. Exercises shall include Red Team activities directed against CNDS as well as DoD information systems and computer networks.

5.6.6. In conjunction with ASD(C3I) and USCINCSPACE, establish requirements for the CND COP and the sensor grid.

5.6.7. Ensure, in coordination with ASD(C3I), the validation of CND requirements through the Joint Requirements Oversight Council and as required by DoD Directive 5000.1 (reference (j)), and USD(AT&L), ASD(C3I), and DOT&E Memorandum, "Mandatory Procedures for Major Defense Acquisition Programs (MDAPS) and Major Automated Information System (MAIS) Acquisition Programs" (reference (k)).

5.6.8. In coordination with the ASD(C3I) and the Under Secretary of Defense for Acquisition, Technology and Logistics, ensure that CND requirements are fully integrated into C4ISR and information technology related architectures, plans and programs.

5.6.9. Ensure the compatibility, interoperability, integration and supportability of CND requirements for C4 in accordance with DoD Instruction 4630.8 (reference (l)).

5.6.10. Incorporate CND into joint military education curricula.

5.7. The Commander in Chief, United States Space Command (USCINCSPACE) shall:

5.7.1. Lead Defense-wide CND mission operations, to include:

5.7.1.1. Advocating the CND requirements of all Commanders-in-Chief (CINCs), conducting and planning for CND mission operations.

5.7.1.2. Executing operational authority to direct Defense-wide change in Information Operations Condition (INFOCON).

5.7.1.3. Coordinating release and distribution of CND advisories and alerts and monitoring compliance of issued Information Assurance Vulnerability Alerts (IAVA).

5.7.1.4. Developing national requirements for CND, defining intelligence support requirements, identifying intelligence resources, establishing intelligence support procedures, and supporting all CINCs for CND.

5.7.2. Provide the Secretary of Defense, through the CJCS, a periodic operational assessment of the readiness of the DoD Components to defend DoD computer networks.

5.7.3. In conjunction with the CJCS and the ASD(C3I), establish requirements for the CND COP and the CND sensor grid.

5.7.4. Execute combatant command authority to plan and execute operations to defend DoD computer networks or other vital national security interests as directed by the Secretary of Defense, against any unauthorized computer network intrusion or attack.

5.7.5. Provide defense-wide situational awareness and attack warning through fusion, analysis, and coordinated information flows through the CND COP.

5.7.6. Serve as the Accrediting Authority for the CND Certification Authorities.

5.8. The Secretaries of the Military Departments shall:

5.8.1. Coordinate with ASD(C3I) and the Inspector General, DoD, on policy guidance for law enforcement operations that support CND and establish the CND LE&CI Center for coordination of law enforcement and counterintelligence operations in support of CND.

5.8.2. Provide law enforcement and counterintelligence support to the CND LE&CI Center.

5.8.3. Ensure information sharing among the Defense law enforcement community in support of CND.

5.8.4. Ensure information sharing among the Defense counterintelligence community in support of CND.

5.9. The Secretary of the Air Force shall serve as the DoD Executive Agent for a DoD Computer Forensics Laboratory and a DoD Computer Investigations Training Program.

5.10. The Secretary of the Navy shall coordinate the design, development, and maintenance of information systems and databases that facilitate CND counterintelligence operations and CND LE&CI Center requirements, populate CND, and COP databases, as appropriate.

5.11. The Director, National Security Agency (NSA) shall:

5.11.1. Function as the Certification Authority for all DoD CNDS providers designated by ASD(C3I) as a Special Enclave.

5.11.2. Provide CNDS support for Special Enclaves to the DoD Component CNDS as required. Provide Special Enclave CNDS on a subscription basis to any DoD Component that does not establish or otherwise subscribe to a Special Enclave CNDS.

5.11.3. Establish advisory and alert procedures for Special Enclave CNDS providers.

5.11.4. Coordinate the design, development, and maintenance of Special Enclave information systems and databases that facilitate CND and populate CND and COP databases, as appropriate.

5.11.5. Coordinate incorporation of intelligence community (IC) network situational awareness information into the DoD CND COP.

5.11.6. Provide Attack Sensing and Warning (AS&W) (e.g., Defense-wide and long term CND trend and pattern analysis) support to USCINCSPACE and to the DoD Components. Populate CND and COP databases with AS&W analysis, as appropriate.

5.11.7. Establish and maintain a trusted agent network and procedures for the reporting of Information Assurance Red Teaming activities. Populate CND and COP databases with Red Team activities, as appropriate.

5.11.8. In support of ASD(C3I) CND architectural initiatives, serve as the CND Program Manager for research and technology in order to:

5.11.8.1. Develop and evaluate attack sensing and warning emerging technologies.

5.11.8.2. Coordinate development and evaluation of tools and techniques to support CND operations.

5.11.8.3. Support the CND procurement and logistics activities of the DoD Components.

5.12. The Heads of DoD Components shall:

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

5.12.2. Comply with the operational direction of the USCINCSPACE for the conduct of CND and the deconfliction of Information Assurance activities that may impact CND operations.

5.12.3. Require that all Component information systems and computer networks are assigned to a certified CNDS.

5.12.4. 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).

5.12.5. Comply with USCINCSPACE alerts and directives (e.g., INFOCON and IAVA) and report CND activities in accordance with DoD and USCINCSPACE guidance.

5.12.6. Ensure, in coordination with Director, DISA, that the DoD Component information systems and computer networks are instrumented according to CND sensor grid requirements.

5.12.7. Ensure that the DoD Component information systems and computer networks are monitored to detect CND-related activity and that detected activity is reported in accordance with USCINCSPACE guidance.

5.12.8. Coordinate CND related research development and evaluation with the Director, National Security Agency.

5.12.9 Coordinate with Director, DIA on intelligence collection and reporting requirements.

5.12.10. Provide training and education programs to support CND personnel, to include system administrators and network managers, and ensure that CND personnel are trained, designated, equipped and certified in accordance with established DoD standards.

6. EFFECTIVE DATE

This Directive is effective immediately.

Rudy de Leon
Deputy Secretary of Defense

Enclosures – 2
E1. References
E2. Definitions

E1. ENCLOSURE 1

REFERENCES (Cont)

(e) DoD Directive 4640.6, "Communications Security Telephone Monitoring and Recording," June 26, 1981.
(f) DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process," December 30, 1997.
(g) "DoD C4ISR Architecture Framework," Version 2.0, December 18, 1997
(h) DoD Joint Technical Architecture (JTA), Version 3.0, November 29, 1999
(i) DoD 5200.1-R, "Information Security Program," January 1997
(j) DoD Directive 5000.1, "The Defense Acquisition System," October 23, 2000
(k) USD(AT&L), ASD(C3I), and DOT&E Memorandum, "Mandatory Procedures for Major Defense Acquisition Programs (MDAPS) and Major Automated Information System (MAIS) Acquisition Programs," October 23, 2000.
(l) DoD Instruction 4630.8, "Procedures for Compatibility, Interoperability, and Integration of Command, Control, Communications and Intelligence (C3I) Systems," November 18, 1992

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 Network Defense Service (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 .

E2.1.5. CNDS Certification Authority (CNDS/CA). An entity responsible for certifying CNDS providers, coordinating among assigned CNDS providers, and managing information dissemination supporting CND operations.

E2.1.6. CND Common Operational Picture (COP). A distributed capability that provides local, intermediate, and DoD-wide visual situational awareness of CND activities and operations and their impact; collaboration; and decision support. The CND COP is a view on the Network Operations (NETOPS) Common Operational Picture (NETOPS COP).

E2.1.7. CND Sensor Grid. A coordinated constellation of decentrally owned and implemented intrusion and anomaly detection systems (i.e., instrumentation) deployed throughout DoD information systems and computer networks. The CND sensor grid is a component of the NETOPS sensor grid.

E2.1.8. CND Service (CNDS). A DoD service provided or subscribed to by owners of DoD information systems or computer network 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.

E2.1.9. 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/CA. 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).

E2.1.10. 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.

E2.1.11. Computer Network Attack (CNA). Operations to disrupt, deny, degrade, or destroy information resident on computers and computer networks or the computers and networks themselves.

E2.1.12. 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.

E2.1.13. CND Law Enforcement and Counterintelligence Center (CND LE&CI 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.

E2.1.14. DoD Executive Agent. For the purpose of this Directive, a DoD Executive Agency is the individual designated by position to have and to exercise the assigned responsibility and delegated authority of the Secretary of Defense, as specified in this Directive.

E2.1.15. Enclave. An environment that is under the control of a single authority and has a homogeneous security policy, including personnel and physical security. Local and remote elements that access resources within an enclave must satisfy the policy of the enclave. Enclaves can be specific to an organization or a mission and may also contain multiple networks. They may be logical, such as an operational area network (OAN), or be based on physical location and proximity. The enclave encompasses both the network layer and the host and applications layer.

E2.1.16. General Services. Any DoD information system or computer network (e.g. NIPRNET & SIPRNET) not otherwise specifically designated by the ASD(C3I) as a Special Enclave because of special security requirements.

E2.1.17. 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.

E2.1.18. Information Assurance. Information operations (IO) 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.

E2.1.19. Information Assurance Red Team. 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.

E2.1.20. 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.

E2.1.21. 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 (e)).

E2.1.22. 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 attack. The NIPC is an interagency activity hosted by the Federal Bureau of Investigation.

E2.1.23. 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. Note: CND employs NETOPS capabilities, specifically information assurance mission area, in concert with law enforcement, intelligence, and other military activities to defend and protect DoD computer networks.

E2.1.24. 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)

E2.1.25. Sensor Grid. See CND Sensor Grid

E2.1.26. 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 ASD(C3I).

E2.1.27. 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 deficiencie , provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.