



Department of Defense
Defense Commissary Agency
DIRECTIVE

Network Enclave Security and Operations

DeCAD 35-12
February 6, 2008

Program Management
DeCA HQ/PMI

References: See Enclosure 1

1. REISSUANCE AND PURPOSE. This Directive:

a. Reissues Reference (a), establishes policy, and assigns responsibility for establishing and operating:

(1) A protected data network and computing environment enclave (DeCANet).

(2) Agency-wide telephone systems or voice networks and associated services.

(3) Converged networking services (voice, data, and/or video) as these capabilities are approved for inclusion in DeCANet.

b. Facilitates compliance with the commercial Payment Card Industry (PCI) Data Security Standard, available at <https://www.pcisecuritystandards.org>.

c. Facilitates compliance with federal law, Department of Defense (DoD) Global Information Grid (GIG), Information Assurance (IA), and Computer Network Defense (CND) directives and policies for operating DoD-certified and -approved networks.

d. Supports the protection and maintenance of the confidentiality, integrity, and availability of DeCANet as part of the DoD GIG.

e. Is established in compliance with Reference (b).

2. APPLICABILITY. This Directive applies to:

a. All Defense Commissary Agency (DeCA) personnel, contractor personnel, and activities that utilize:

(1) DeCANet enclave resources through either direct or indirect (remote) access, or that use any information technology (IT)-enabled technologies with networking capabilities.

(2) DeCA telephone systems or voice network.

(3) DeCA converged network services (data, voice, and/or video).

b. All IT-enabled services or technologies with networking capabilities, whether the networking capabilities are used or not.

3. POLICY. It is DeCA policy that:

a. A protected global network enclave, referred to as DeCANet, will be established and maintained. DeCANet will include all legacy voice and converged voice, data, and video network services.

(1) DeCANet will comply with relevant PCI standards, federal, DoD, and DeCA directives and policies, in accordance with the references listed in Enclosure 1, and all other applicable laws and regulations.

(2) DeCANet will be proactively managed and operated with a goal of maximizing net-centric enterprise strategies that encompass all network-connected systems and equipment, including but not limited to: network infrastructure assets, servers and their applications, workstations, printers, scanners, fax machines, wireless technologies, and other current and emerging technologies.

b. All IT-enabled technology requests and requirements for network services must be evaluated and approved for use in compliance with IA requirements and Agency policy, reference paragraph 3.c.

c. IT-enabled services or technologies with networking capabilities will be evaluated by the Chief Information Officer (CIO), and Directors of Program Management (PM) and System Engineering (SE), for possible integration into DeCANet in order to meet present and/or future mission support requirements. The integration decisions will establish policy for current and future acquisitions and implementations.

d. DeCA information systems and networks will be monitored in accordance with References (r), (aa), (ab), (ac), (ad), and all other relevant federal, DoD and DeCA regulations, in order to monitor threats to the security or function of operations, systems, or networks.

e. Consistent Agency-wide administrative remedies and/or penalties directed towards individuals not complying with this Directive and its subordinate manuals will be established and enforced.

4. RESPONSIBILITIES.

a. Chief Operating Officer (COO). The COO shall:

(1) Ensure implementation of this Directive, and the policies and procedures established under this Directive.

(2) Ensure establishment and enforcement of consistent Agency-wide administrative remedies and/or penalties directed towards individuals not complying with this Directive and its subordinate guidance.

b. Corporate Governance Board (CGB). The CGB shall:

(1) Enforce compliance with the policies outlined in this Directive, and the policies and procedures established under this Directive.

(2) Facilitate the establishment and enforcement of consistent Agency-wide administrative remedies and/or penalties directed towards individuals not complying with this Directive and its subordinate guidance.

c. CIO. The CIO shall:

(1) Ensure/monitor compliance with the policies outlined in this Directive, and the policies and procedures established under this Directive.

(2) Establish Agency policy, in consultation with the Directors of PM and SE, for acquisition and implementation of current and future IT-enabled technology with networking capabilities, whether the networking capabilities are used or not.

(a) Serve as the oversight and review authority for requests not in compliance with the policies outlined in this Directive.

(b) Seek to modify non-compliant acquisitions and programs to bring them into compliance, and/or recommend to the COO they be halted/terminated.

(3) As the Designated Accrediting Authority (DAA) shall:

(a) Ensure DeCANet, and all systems using DeCANet, obtain and maintain their DoD IA certification and accreditations.

(b) Ensure the certification and accreditation of CND service is in accordance with Reference (s).

(c) Ensure CND service support is a condition of system security certification and accreditation.

(d) Ensure compliance with DoD Ports, Protocols, and Services (PPS) program is a condition of system security certification and accreditation.

(e) Review and approve IA- and CND-related memorandums of agreement (MOA), reference paragraph 4.d.(7).

(f) Review and approve/disapprove Enterprise Management Plan (EMP) compliance waiver requests, reference paragraph 4.d.(6).

(4) Facilitate the resolution of non-compliance issues.

d. Director of PM. The Director of PM shall:

(1) Implement the policies outlined in this Directive and establish subordinate policies and procedures as required.

- (2) Serve as the central management authority for the Agency-wide telephone systems (voice network) and associated services.
 - (3) Serve as the owner and central management authority for all converged network services.
 - (4) Ensure IT requirements are included in Agency major and minor facility construction programs.
 - (5) Approve and release for general use end-user and technical operations policies and procedures.
 - (6) Review and forward EMP compliance waiver requests, reference paragraph 4.g.(4)(b), and recommendations to the CIO/DAA for review.
 - (7) Review and forward MOAs, reference paragraphs 4.h.(3) and 4.h.(4) to the CIO/DAA for approval.
 - (8) Shall coordinate with the CIO and the Director of SE to:
 - (a) Review, evaluate, and approve/disapprove all requirements and requests for IT-enabled technology with networking capabilities for use within DeCANet.
 - (b) Complete the review and decision process for new requirements that do not fall within established and published policy not later than 60 calendar days after receiving notification of the requirement.
 - (c) Establish, maintain, and publish a current list of networking technology integration policy decisions.
 - (9) Identify and resolve non-compliance issues. Report non-compliance to the CIO, CGB, and responsible functional process owner(s) (FPO).
- e. FPO. The FPO shall:
- (1) Ensure compliance with the policies outlined in this Directive, and the policies and procedures established under this Directive.
 - (2) Ensure full coordination with and approval by the CIO, and the Directors of PM and SE, prior to any acquisition and implementation of technologies governed by this Directive.
 - (3) Facilitate the establishment of and enforce Agency-wide administrative remedies and/or penalties directed towards individuals not complying with this Directive and its subordinate guidance.
 - (4) Staff and budget for appropriate IA, CND, and proactive, centralized automated error and performance reporting, and security management reporting and related requirements, reference paragraphs 4.c.(3)(a), 4.g.(4)(b), and 4.g.(5)(a), in their areas of responsibility.
- f. CIO Office, Information Assurance Manager (IAM). The IAM shall:
- (1) Ensure/facilitate compliance with DoD and DeCA's certification and accreditation program.

(2) Provide and maintain policy and guidance on CND operations, to include vulnerability analysis and assessments scanning tools, information operations condition (INFOCON) policies, Blue Teaming, Red Teaming, network vulnerability scanning, and other areas of IA.

(3) Partner with the DeCA Network Manager to provide consultation and design/integration guidance and/or services for new and modified systems to ensure compliance with relevant federal, DoD, and DeCA directives and policies for network use.

(4) Identify and report non-compliance issues to the CIO, the Director of PM, the DeCA Network Manager, and the appropriate system/program managers.

(5) Seek to resolve non-compliance issues.

g. PM Infrastructure Division Chief. The PM Infrastructure Division Chief shall:

(1) Serve as the Network Manager for DeCANet.

(2) Implement and/or follow the policies outlined in this Directive.

(3) Publish end-user and technical operations policies and procedures for Director of PM approval, signature, and general release.

(4) Establish and maintain an EMP for DeCANet.

(a) Ensure proactive, centralized automated error and performance reporting, and security management reporting are elements of the EMP.

(b) Ensure the EMP requires all systems to report to and/or be monitored by a DeCANet Enterprise Management System (EMS). If system compliance is not possible, a justification and EMP compliance waiver request may be submitted to the CIO/DAA, with the concurrence of the Director of PM.

(c) Ensure the EMP provides for establishment of a user-defined operational picture (UDOP).

(d) Ensure DeCANet is operated within the bounds of the EMP.

(5) Establish and operate an appropriate combination of EMSs in accordance with the EMP.

(a) Ensure all systems connected to DeCANet report to, and/or are monitored by, the appropriate centralized EMS.

(b) Ensure at least one EMS, or component thereof, provides for a UDOP.

(6) Establish and operate a Telecommunications Expense Management program to ensure all networked assets and associated telecommunications transport services are centrally managed and life cycle costs are tracked.

(7) Staff and budget for all aspects of network operations and sustainment.

(8) Partner with the CIO Office IAM to provide consultation and design/integration guidance and/or services for new and modified systems to ensure compliance with relevant federal, DoD, and DeCA directives and policies for network use.

(9) Identify and report non-compliance issues to the CIO, the CIO Office IAM, the Director of PM, and the appropriate system/program managers.

(10) Facilitate the resolution of non-compliance issues.

h. Information Assurance Officer for the Network. The Information Assurance Officer for the Network shall:

(1) Serve as the Network Security Officer.

(2) Ensure compliance with DoD and DeCA IA, CND, and PPS policies.

(3) Establish and maintain MOAs between DeCA and non-DeCA information system service providers in compliance with Reference (p), and subsequent versions.

(4) Establish and maintain MOAs between DeCA's primary computer network defense service provider and other organizations.

(5) Ensure compliance with the policies outlined in this Directive.

(6) Facilitate the establishment of and ensure compliance with approved policies and procedures established under this Directive.

(7) Identify and report non-compliance issues to the CIO, the CIO Office IAM, the Director of PM, the DeCA Network Manager (PM Infrastructure Division Chief), and the appropriate system/program managers.

(8) Facilitate the resolution of non-compliance issues.

i. Division and Branch Chiefs, Supervisory Personnel, System/Program Managers, and Implementers. Division and branch chiefs, supervisory personnel, system/program managers, and implementers shall:

(1) Ensure compliance with the policies outlined in this Directive, and the policies and procedures established under this Directive.

(2) Consult with the CIO Office IAM and DeCA Network Manager (PM Infrastructure Division Chief) at the earliest time allowable when developing new or modifying existing system requirements to ensure compliance with relevant federal, DoD, and DeCA directives and policies for network use.

(3) Ensure full coordination with and approval by the CIO and the Directors of PM and SE prior to any acquisition and implementation of technologies governed by this Directive.

(4) Identify and report non-compliance issues to the CIO, the CIO Office IAM, the Director of PM, the DeCA Network Manager (PM Infrastructure Division Chief), and the appropriate system/program managers.

(5) Seek to resolve non-compliance issues.

j. User Community, Including System Developers. The user community, including system developers, shall:

(1) Ensure compliance with the policies outlined in this Directive, and policies and procedures established under this Directive.

(2) Facilitate compliance efforts and report suspected non-compliance to the DeCA Network Manager and CIO Office IAM.

(3) Consult with the CIO Office IAM and DeCA Network Manager at the earliest time allowable when developing new or modifying existing system requirements to ensure compliance with relevant federal, DoD, and DeCA directives and policies for network use.

5. RELEASABILITY - UNLIMITED. This Directive is approved for public release. The DoD Components, other Federal agencies, and the public may obtain copies of this Directive through the Internet from the DeCA Web site at <http://www.commissaries.com>.

6. EFFECTIVE DATE. By order of the Director, this Directive is effective immediately.



Bonita M. Moffett
Chief, Corporate Operations Group

Enclosures

1. References
- Glossary

ENCLOSURE 1

REFERENCES

- (a) DeCA Directive 35-12, "Network Security and Firewall Policy," February 18, 2000, (hereby canceled)
- (b) DoD Directive 5105.55, "Defense Commissary Agency (DeCA)," November 9, 1990
- (c) Public Law 105-261, October 17, 1998, Section 368, Defense Commissary Agency Telecommunications
- (d) DoD Directive 8100.1, "Global Information Grid (GIG) Overarching Policy," September 19, 2002
- (e) Assistant Secretary of Defense (C3I) Memorandum, "Global Information Grid Waiver Charter," July 4, 2002
- (f) DoD Directive 8100.2, "Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)," April 14, 2004
- (g) DoD Instruction 8100.3, "Department of Defense Voice Networks," January 16, 2004
- (h) DoD Directive 5200.1, "DoD Information Security Program," December 13, 1996
- (i) DoD Directive 8500.01E, "Information Assurance (IA)," October 24, 2002
- (j) DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003
- (k) DoD Instruction 8551.1, "Ports, Protocols, and Services Management (PPSM)," August 13, 2004
- (l) Department of Defense Ports, Protocols, and Services (PPS) Assurance Category Assignment List (CAL), current release available at <https://powhatan.iiee.disa.mil/ports/index.html>
- (m) DoD Instruction 8552.01, "Use of Mobile Code Technologies in DoD Information Systems," October 23, 2006
- (n) DoD Directive 8570.01, "Information Assurance (IA) Training, Certification, and Workforce Management," August 15, 2004
- (o) DoD Manual 8570.01-M, "Information Assurance Workforce Improvement Program," December 19, 2005
- (p) Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6510.01E, "Information Assurance (IA) and Computer Network Defense (CND)," August 15, 2007
- (q) DoD Chief Information Officer Memorandum, "Interim Department of Defense Information Assurance (IA) Certification and Accreditation (C&A) Process Guidance," July 6, 2006
- (r) DoD Instruction 8560.01, "Communications Security (COMSEC) Monitoring and Information Assurance Readiness Testing," October 9, 2007
- (s) DoD O-8530.1-M, "Department of Defense Computer Network Defense (CND) Service Provider Certification and Accreditation Program," December 17, 2003
- (t) Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGS)
- (u) Strategic Command Directive SD-527, "Department of Defense Information Operations Condition (INFOCON) System Procedures," January 27, 2006
- (v) OMB Circular No. A-130, "Management of Federal Information Resources," current revision
- (w) Federal Information Security Management Act (FISMA) of 2002, various dates
- (x) Public Law 93-579, Privacy Act of 1974
- (y) Public Law 100-235, Computer Security Act of 1987
- (z) Public Law 104-106, Division E, Clinger-Cohen Act of 1996
- (aa) 18 U.S.C. 1030, Computer Fraud and Abuse Act
- (ab) 18 U.S.C. 2510-22, Federal Wiretap Act
- (ac) 18 U.S.C. 3121-27, Pen/Trap Statute
- (ad) 18 U.S.C. 2511, Wire and Electronic Communications Interception and Interception of Oral Communications
- (ae) DeCAD 35-31, "DeCA Automated Information Systems Security (INFOSEC) Program," August 11, 1996

- (af) DeCAD 50-1, "Employee Processing and the Common Access Card (CAC)," September 2003
- (ag) Public Law 107-314, Bob Stump National Defense Authorization Act for Fiscal Year 2003, Section 353, Installation and Connection Policy and Procedures, regarding Defense Switch Network, December 2, 2002
- (ah) Commercial Payment Card Industry (PCI) Data Security Standard (DSS) available at <https://www.pcisecuritystandards.org>.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

CGB	Corporate Governance Board
CIO	Chief Information Officer
CND	Computer Network Defense
COO	Chief Operating Officer
DAA	Designated Accrediting Authority
DeCA	Defense Commissary Agency
DeCANet	Defense Commissary Agency Network
DoD	Department of Defense
EMP	Enterprise Management Plan
EMS	Enterprise Management System
FPO	functional process owner
GIG	Global Information Grid
IA	Information Assurance
IAM	Information Assurance Manager
IT	information technology
MOA	memorandum of agreement
PCI	Payment Card Industry
PM	Program Management
PPS	Ports, Protocols, and Services
INFOCON	information operations condition
SE	Systems Engineering
UDOP	user-defined operational picture

PART II. DEFINITIONS

common operational picture. A distributed capability that provides local, intermediate, and DoD-wide visual situational awareness of Computer Network Defense activities and operations.

Computer Network Defense (CND). Actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within DoD systems and computer networks.

CND architect. Provides oversight and direction for the Computer Network Defense service provider certification and accreditation process. Oversees and coordinates Defense-wide CND activities related to the design and development of systems supporting the CND common operational picture, sensor grid, de-confliction, and integration activities of the CND Research and Technology Program Manager.

CND service (CNDS). A DoD service provided or subscribed to by owners of DoD systems or networks in order to maintain and provide CND situational awareness, implement CND protection measures, monitor and analyze in order to detect unauthorized activity, and implement CND operational direction.

CND Service Certification Authority (CNDS/CA). An entity responsible for certifying CNDS providers, coordinating among assigned CNDS providers, and managing information dissemination supporting CND operations. The Commander in Chief, U.S. Space Command is the accrediting authority for CNDS.

CND 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 communication protocols established by the CNDS Certification Authority (CNDS/CA).

CND service providers (CNDSP). Those individuals responsible for delivering protection, detection, and response services for protected enclaves or networks. CNDSPs must provide for the coordination service support of a CNDS/CA.

Designated Accrediting Authority (DAA). Official with the authority to formally assume responsibility for operating a system or network at an acceptable level of risk.

enclave. An environment that is under the control of a single authority or DAA.

incident. An attempted entry, unauthorized entry, and/or an information attack having actual or potentially adverse effects on a system.

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

Net-centric (also spelled “netcentric”). Wikipedi says, “network-centric” refers to “Participating as a part of a continuously-evolving, complex community of people, devices, information, and services interconnected by a communications network to achieve optimal benefit of resources and better synchronization of events and their consequences.” “Network Centric Enterprise Architecture” has been defined in lay terms as a massively distributed architecture with components and/or services available across and throughout an enterprise’s entire lines-of-business.

A net-centric network ensures that information gets where it is needed when it is needed. This concept is a part of the NetCentric Enterprise Solution for Interoperability (NESI). NESI is a body of architectural

and engineering knowledge that guides the design, implementation, maintenance, evolution, and use of the IT portion of net-centric solutions for military application. Similar interoperability concepts and operational requirements make NetCentricity a critical component for DeCA's mission success.

sensor grid. A coordinated constellation of decentrally owned and implemented intrusion and anomaly detection systems deployed throughout DoD systems and networks.

special enclave. DoD systems and/or networks with special security requirements and designated as a special enclave by the Assistant Secretary of Defense.