DEPARTMENT OF THE NAVY
OFFICE OF THE SECRETARY
1000 NAVY PENTAGON
WASHINGTON DC 20350-1000

SECNAVINST 3052.2
DUSN
6 March 2009

SECNAV INSTRUCTION 3052.2

From: Secretary of the Navy

Subj: CYBERSPACE POLICY AND ADMINISTRATION WITHIN THE DEPARTMENT OF THE NAVY

Ref: (a) Joint Publication 1-02 of 12 April 2001
(b) DEPSECDEF Memo of 12 May 08, The Definition of Cyberspace (NOTAL)
(c) CJCS Memo of 10 Nov 08, Definition of Cyberspace Operations (NOTAL)
(d) DoD Instruction 5200.39 of 16 Jul 08
(e) SECNAV M-5210.1
(f) SECNAVINST 5430.7P
(g) SECNAVINST 5239.3A
(h) SECNAV M-5239.1 of Nov 05

Encl: (1) Glossary of Definitions

1. Purpose

a. To establish policies and responsibilities for the administration of cyberspace within the Department of the Navy (DON) consistent with references (a) through (h).

b. To designate the Under Secretary of the Navy as the DON Chief Cyberspace Officer.

2. Background

a. Cyberspace is an essential element to all military operations. DON reliance on cyberspace to conduct its missions and warfighting functions will continue to increase for the foreseeable future.

b. Cyberspace capabilities are critical to achieving DON objectives in every warfighting domain and enterprise business model. The Department of Defense (DoD) is undergoing a significant transformation in organization, structure, and alignment to enable the full range of operations in cyberspace.

Accordingly, the DON must enhance the way it is organized to man, train, and equip for its cyberspace missions and tasks.

c. Cyberspace operations will require intensive training and education for the total DON cyberspace workforce. DON workforce will be a single integrated resource that is carefully managed with a dedicated focus on continued training and education to meet emerging technical developments and employed to provide the highest level of cyberspace capabilities to meet naval and joint objectives. The associated mission areas of computer network operations, Network Operations (NETOPS), and Information Assurance (IA) will be enabled by common technologies, and, therefore, must be highly synchronized to maximize our limited resources.

3. Scope. This instruction:

a. Applies to the Offices of the Secretary of the Navy, the Chief of Naval Operations (CNO), the Commandant of the Marine Corps (CMC), and all Navy and Marine Corps activities, installations, and commands;

b. Does not alter command and control relationships for the employment of DON forces as directed by the Secretary of Defense, Unified Command Plan, “Forces For Unified Commands” or Navy Regulations; and

c. Applies to DON owned or controlled cyberspace systems that receive, process, store, display or transmit DoD information, regardless of classification or sensitivity.

4. Definitions. Definitions are provided in enclosure (1) and are per references (a), (b), and (c).

5. Policy

a. Cyberspace efforts within the DON will align with national and DoD efforts to ensure the Department’s capability and capacity to conduct cyberspace operations increases as cyberspace continues to evolve and grow in complexity. The DON requires unfettered access to, and assured capabilities in, cyberspace to execute the full range of naval missions and functions assigned. Horizontal protection across DoD activities is necessary to ensure the sustainment of secure DON cyberspace

systems for the warfighter. Therefore, the DON shall establish, institutionalize, fund, and sustain a robust capability in cyberspace, enabling the Department to:

(1) Acquire and apply capabilities to defend cyberspace assets and supply-chains against attack, exfiltration, corruption, and usurpation;

(2) Synchronize cyberspace protection capabilities across the DON during research, development, acquisition and sustainment of Command, Control, Communications, Computers, Intelligence (C4I), space and Information Technology (IT) enterprise systems. This will include definition of and support for DON supply-chain and Defense Industrial Base (DIB) partners;

(3) Develop warfighting capabilities for cyberspace operations. These capabilities will support objectives across joint mission areas to exploit and deny adversary freedom of maneuver in and through cyberspace, and cyberspace planning necessary to deliver increased warfighting capabilities available to Joint task force commanders; and

(4) Integrate Naval Criminal Investigative Service (NCIS) Law Enforcement (LE) and Counter Intelligence (CI) capabilities throughout the DON cyberspace domain and NETOPS centers. These capabilities will provide rapid, coordinated LE/CI pursuit and prosecution of the human elements associated with internal and external threats.

b. Speed of action in cyberspace demands real time situational awareness. DON investment objectives shall consider development of a true real time common operating picture of the cyberspace domain.

c. The DON will establish an organizational structure and processes that:

(1) Invest resources to recruit, train, retain, and equip personnel for cyberspace missions.

(2) Synchronize the cyberspace-related capabilities of the Navy and Marine Corps to support the full range of cyberspace missions and functions assigned, creating mutually supportive kinetic and non-kinetic options and effects.

6. Action. The Offices of the Secretary of the Navy, CNO and CMC shall establish a capability that:

(1) To the extent authorized, supports national missions, through collaboration and cooperation with inter-agency partners, such as Department of Homeland Security and Department of Justice;

(2) As directed and as capable, supports strategic missions, including geographic and functional combatant commands. The DON's current priority for external support is to maintain the overall integrity and availability of DoD networks;

(3) Develops a cyberspace strategy and implementation plan that includes, but is not limited to: command and control; supply-chain management; intelligence; and other information system networks that the Services use to perform their functions and missions;

(4) Manages acquisition of DON cyberspace capabilities throughout the life-cycle to support offensive and defensive capabilities and systems, as well as our ability to support geographic and functional combatant commanders requirements; and

(5) Supports cyberspace operations with LE and CI mechanisms. Results from investigations, operations and related programs will be coordinated with NETOPS to include offensive and defensive cyberspace operations and supporting organizations to ensure continuity of effort.

7. Responsibilities

a. The Under Secretary of the Navy shall:

(1) Perform the duties, responsibilities and authorities of the Chief Cyberspace Officer for the DON.

(2) Serve as the single official and fiscal advocate responsible for advising the Secretary on the alignment of program of record and non-program of record resources for mature end-to-end cyberspace capabilities;

(3) Represent the Department of the Navy at DoD cyberspace related forums;

(4) Provide oversight to naval cyberspace policy, ensuring intelligence, CI, national security, foreign policy, LE, and counter-terrorism activities are consistent with applicable executive orders and national strategies;

(5) In consultation with the CNO and the CMC and other key Secretary of the Navy offices, advise the Secretary on DON cyberspace issues, to include:

(a) Intelligence and CI related activities;

(b) Research, development and acquisition;

(c) Alignment of DON financial priorities;

(d) Service and DON efforts to recruit, develop, assign and retain a professional cyberspace workforce; and

(e) DON LE, security and related investigative activities.

(6) Establish a governance framework and report the same to the Secretary on a regularly recurring basis; and

(7) Oversee cyberspace initiatives related to controlled unclassified data information damage assessments. In coordination with the Director of Naval Intelligence, Commander, Naval Network Warfare Command, and other offices, as required, the Office of the Under Secretary will manage DIB, as well as DON internal damage assessment recommendations and requirements, supported by the General Counsel and the Damage Assessment Management Office (DAMO).

b. The CNO and CMC shall:

(1) Develop organizational constructs necessary to ensure the exchange of information, tactics, techniques, and procedures between DON NETOPS, Computer Network Defense (CND), Computer Network Exploitation (CNE), and Computer Network Attack (CNA) activities, units and personnel to optimize synchronization between these related fields;

(2) Maximize efficiency between training and education of cyberspace specific occupational fields;

(3) Continue to provide Service specific NETOPS centers, computer incident response teams, and other cyberspace event and reporting activities to further situational awareness of cyberspace as well as inform emerging concepts of operation;

(4) Advocate for cyberspace capabilities, ensuring adequate resources are programmed to support geographic and functional combatant commanders' requirements;

(5) Develop and mandate cyberspace operational training programs, including Fleet training and exercises throughout the Navy and Marine Corps;

(6) Incorporate cyberspace into applicable Navy and Marine Corps doctrine, ensuring compliance with DON, DoD, Joint doctrine and national policies; and

(7) Provide to the Under Secretary of the Navy a plan for implementing and maintaining the objectives set forth in this instruction within the Navy and Marine Corps, respectively, and update this plan as necessary.

c. The General Counsel of the Navy shall oversee operations of the DAMO and adjudicate assessments of lost DON information. In so doing, the General Counsel will establish policy for the internal review and disposition of assessments, and receive the full support of appropriate organizations involved in DAMO assessments and investigations.

d. The Assistant Secretary of the Navy for Research, Development and Acquisition (ASN (RDA)) shall:

(1) Issue acquisition policies and associated implementation details to support cyberspace capabilities. Assure compliance with reference (d) and related requirements. Streamlined acquisition authority will be addressed as appropriate to meet warfighter needs;

(2) Coordinate with the Under Secretary of Defense for Acquisition, Technology and Logistics, the Under Secretary of Defense for Intelligence (USD(I)), and the National Security Agency on key cyberspace operations related acquisition, as required;

(3) Ensure acquisition management policies and processes address cyberspace considerations during development and throughout the lifecycle of DON C4I, space and IT enterprise systems;

(4) Maintain robust cyberspace science and technology programs;

(5) Provide systems engineering support for naval cyberspace systems, to include offensive capabilities, in order to optimize integration;

(6) Establish, maintain and provide administrative support to the DAMO in order to assess the loss, through cyberspace, of DON Controlled Unclassified Information (CUI) from the DIB; and

(7) Coordinate DAMO policy, concept of operations, and assessment out briefs with the Under Secretary of the Navy, and others as applicable.

e. The Deputy Under Secretary of the Navy shall:

(1) Advise the Secretary and Under Secretary of the Navy and assist in the oversight and management responsibilities on all cyberspace related intelligence, CI, CNA, CNE, and CNA-operational preparation of the environment activities and

(2) Coordinate DON cyberspace issues with the USD(I) and the Under Secretary of Defense for Policy.

f. The Director, NCIS shall:

(1) Investigate terrorism, foreign intelligence, and major criminal offenses impacting the Department of the Navy from inside, on, and beyond the DON cyberspace perimeter.

(2) Conduct proactive cyberspace counter-terrorism, CI, and criminal operation programs related to DON and related DIB assets.

(3) Coordinate with ASN (RDA) to:

(a) Enhance LE/CI capabilities and solutions for the research, development, and/or acquisition efforts that support the DON cyberspace domain and

(b) Enable horizontal protection across the Department of the Navy of critical program information, CUI, and supply-chain risk management.

(4) Coordinate and deliver LE/CI cyberspace training to NETOPS and computer incident response teams to ensure responses are conducted in a manner that supports LE/CI pursuit and prosecution objectives;

(5) Establish information sharing programs between naval and other intelligence organizations to facilitate national and international collaboration on LE/CI related efforts involving naval cyberspace intelligence objectives; and

(6) Provide investigative and intelligence support for DAMO assessments to determine necessary follow-on actions.

g. The DON Chief Information Officer shall:

(1) Develop and promulgate IA and CND strategy and policy;

(2) Ensure compliance of DON and higher level IA and CND policies;

(3) Together with appropriate DoD and DON cyberspace workforce leadership, develop required cyberspace workforce policy and guidance. With the DoD Chief Information Officer and Assistant Secretary of the Navy (Manpower and Reserve Affairs), track and measure the effectiveness of DON cyberspace manpower, personnel, training, and education programs;

(4) Lead DIB initiatives to improve the protection of unclassified defense information processed on industry's unclassified networks and systems. When requested by DAMO, support assessments of compromised DIB data and review completed assessments for DON IT policy compliance. Adjust policy as necessary based on DAMO findings; and

(5) Participate in the development of the naval cyberspace architecture to ensure alignment and consistency with DON enterprise architecture. Review in accordance with established DON enterprise architecture governance processes and procedures.

8. Records Management. Records created as a result of this instruction, regardless of format and media, shall be managed in accordance with reference (e).

Donald C. Winter

Distribution:
Electronic only, via Department of the Navy Issuances Web site
http://doni.daps.dla.mil/

Glossary of Definitions

Computer Network Attack (CNA): Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. (Reference (a))

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

Computer Network Exploitation (CNE): Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks. (Reference (a))

Computer Network Operations: Comprised of CNA, CND, and related CNE enabling operations. (Reference (a))

Cyberspace: A global domain within the information environment consisting of the interdependent network of IT infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (Reference (b))

Cyberspace Operations: The employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid. (Reference (c))

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

Information Operations: The integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related

capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own. Also called "IO;" see also computer network operations; electronic warfare; military deception; operations security; psychological operations. (Reference (a))

Network Operations (NETOPS): Activities conducted to operate and defend the Global Information Grid. Also known as "NETOPS." (Reference (a))