DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

JUN 0 9 2014

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
COMMANDER, U.S. STRATEGIC COMMAND
COMMANDER, U.S. CYBER COMMAND
DIRECTOR, COST ASSESSMENT AND PROGRAM EVALUATION
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER
DIRECTOR, ADMINISTRATION AND MANAGEMENT

SUBJECT: Guidance Regarding Cyberspace Roles, Responsibilities, Functions, and Governance within the Department of Defense

The Secretary of Defense's December 4, 2013, memorandum, "Subject: Information Guidance from the 2013 Office of the Secretary of Defense Organization Review," signified the Department of Defense's (DoD) intent to strengthen the Chief Information Officer's (CIO) functions. At the same time, section 932(c) of the FY14 National Defense Authorization Act (NDAA) called for the designation of a Principal Cyber Advisor (PCA) in the Office of the Under Secretary of Defense for Policy and signaled the Congress's intent to consolidate cyber activities under the new PCA position.

In light of these developments, the purpose of this memorandum is to clarify the roles, responsibilities, and relationships for cyberspace matters in the Department; to streamline seemingly overlapping duties concerning information technology (IT) networks and cyber; and, to provide guidance on establishing a single governance structure for cyberspace going forward.[1] The appendix directs specific actions to be undertaken.

Roles, Responsibilities, and Functions

The Secretary of Defense's December 4, 2013, memorandum regarding the duties and responsibilities for the DoD CIO directed "discrete actions to add functions, expand authorities, and restore stature, with a priority focus on advancing the Joint Information Environment (JIE)." Concurrently, the FY14 NDAA assigned substantial oversight and managerial responsibilities for cybersecurity to the new PCA, to include serving as the principal civilian advisor to the Secretary of Defense on all "military cyber forces and activities," including defense of DoD networks.

Recognizing Congressional intent as well as the Department's desire to strengthen the DoD CIO position and to focus on advancing the JIE, the future roles, responsibilities, and functions for the DoD CIO and PCA shall be as follows:

[1]For the purpose of this memorandum, and as stated in Presidential Policy Directives, the term "cyberspace" means the interdependent network of information technology infrastructures that includes the Internet, telecommunications networks, computers, information or communication systems, networks, and embedded processors and controllers.

OSD006447-14

- DoD CIO: Shall serve as the principal staff assistant and senior advisor to the Secretary of Defense on matters related to IT systems and architecture, information resource management (IRM) and efficiencies, and cybersecurity standards, in coordination with the PCA. In these capacities, the DoD CIO shall:

    - Develop policy guidance and prescribe standards for: network operations, the secure configuration and maintenance of IT systems, interoperability of DoD systems and interface between non-DoD systems, and enterprise-wide architecture requirements.

    - Conduct oversight and manage implementation of: an integrated IT architecture, compliance with IT network policies and technical standards, IT programs and systems performance, the development and maintenance of network contingency and crisis response communications plans, and the IT budget.

    - Provide policy guidance and advice on: IT network security, cybersecurity standards, IT networks and IRM budget requests, and IT infrastructure procurement and investment decisions.

- PCA: Shall serve as the principal civilian advisor to the Secretary of Defense on offensive and defensive cyberspace operations and missions. The PCA shall advise the Secretary with respect to acquisitions related to cybersecurity and cyber offensive and defensive capabilities, but this advisory role shall not be construed to affect the authorities of the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD (AT&L)) or of the Acquisition Executives of the Military Departments. In addition, nothing in this Memorandum shall be construed to mean that the PCA has operational responsibilities for cyber defensive or offensive missions. The PCA shall:

    - Serve as the principal advisor within the senior management of the Department (after the Secretary and Deputy Secretary) on military cyber forces and activities.

    - Develop and oversee the implementation of DoD cyber policy and ensure that DoD activities support national cyber strategies and policies.

    - Oversee Department-wide cyber training programs, activities, resources, personnel, operations, acquisitions (in consultation with the USD (AT&L)), and technology (in consultation with USD (AT&L) and DoD CIO).

Strengthening the Governance of Cyberspace

Creating an integrated cyberspace governance process will streamline IT network decisions, specify coordination lines, reduce duplicative or overlapping systems, enhance network security, and encourage innovation. Going forward, the primary roles and responsibilities governing cyberspace should be aligned according to the following guidance:

- DoD CIO: In coordination with the PCA, USD(AT&L), the Director, National Security Agency, and others, as appropriate, the DoD CIO shall identify common standards and system requirements to facilitate interoperability and to protect DoD networks.

- PCA: Shall provide strategic oversight of DoD's cybersecurity policies and activities.

- The Deputy Chief Management Officer: In coordination with DoD CIO, shall identify business requirements for DoD systems, including requirements for systems to interact with each other in the enterprise business architecture, and shall work with the DoD CIO to translate these requirements into technical standards.

- USD(AT&L): Shall have final decision authority for all IT and cyber infrastructure acquisition matters, including IT-intensive software systems such as business systems, but can delegate such authority, including to the DoD CIO, Military Departments, and other components, as appropriate. All IT and cyber infrastructure investment decisions shall be informed by the DoD CIO, the PCA, and the Cyber Investment Management Board.

- Chairman, Joint Chiefs of Staff: Through the Joint Requirements Oversight Council, will identify, assess, and approve military capability requirements in all warfighting domains, including cyber.

- USSTRATCOM: Under the authority of USSTRATCOM, USCYBERCOM shall serve as the principal DoD entity responsible for operationally defending DoD networks and ensuring the execution of Secretary of Defense orders.

- DoD Components: All DoD components, particularly the Defense Information Systems Agency, shall operate DoD networks in accordance with DoD CIO standards and USCYBERCOM orders.

At a time when IT capabilities can provide the warfighter with critical advantages over adversaries on land, at sea, and in space, it is more important than ever to improve how the Department governs its cyberspace enterprise. Collectively, these guidelines will enhance the Department's management of cyberspace issues, streamline coordination, and ensure that the warfighter and all DoD employees can depend on secure, reliable, and efficient cyberspace services in the future.

cc:
Vice Chairman of the Joint Chiefs of Staff
Chiefs of the Military Services
Assistant Secretary of Defense for Legislative Affairs
Assistant to the Secretary of Defense for Public Affairs

Appendix

Upon further review of the Secretary of Defense's December 4, 2013, memorandum ("Subject: Information Guidance from the 2013 Office of the Secretary of Defense Organization Review") and section 932(c) of the FY14 National Defense Authorization Act (NDAA) requiring the designation of a Principal Cyber Advisor to the Secretary of Defense, I hereby direct the following actions to clarify the future roles, responsibilities, and functions for cyberspace governance in the Department.

First, the Under Secretary of Defense (USD) for Acquisition, Technology, and Logistics (AT&L), shall, in coordination with the DoD Chief Information Officer (DoD CIO), ensure that acquisition associated with Joint Information Environment (JIE) is planned and managed as a coherent Department-wide effort, although the JIE shall not be a formal joint program of record. The JIE is an integrated DoD-wide effort to modernize computer networks and associated software, and includes a mix of policies, standards, projects, and programs. The JIE consists of both centralized and decentralized components. The JIE design and standards shall be led by the DoD CIO and acquired and managed by the Military Departments and other components, including the Defense Information Systems Agency, with acquisition oversight provided by the USD(AT&L).

Second, in coordination with the DoD General Counsel, the USDs for Policy, Intelligence, and AT&L, the Deputy Chief Management Officer (DCMO), the Joint Staff, Military Departments, and the Deputy Secretary of Defense, DoDD 5144.02 shall be revised according to the guidance set forth in this Memorandum, by July 11, 2014.

Finally, the DoD CIO's March 10, 2014, memorandum, "Subject: Department of Defense Information Technology Governance Process," now retracted, shall be reissued to realign the governance structure with the guidance set forth in this memorandum. The revised DoD CIO memorandum shall be coordinated with the Joint Staff, DCMO, the USD's for Policy, Intelligence, and AT&L, CAPE, GC, and approved by the Deputy Secretary of Defense, by August 1, 2014.