

NOT FOR PUBLICATION UNTIL  
RELEASED BY THE  
HOUSE ARMED  
SERVICES COMMITTEE

STATEMENT OF  
ROBERT J. CAREY  
DEPARTMENT OF THE NAVY CHIEF INFORMATION OFFICER  
BEFORE THE  
HOUSE ARMED SERVICES COMMITTEE  
TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES  
SUBCOMMITTEE  
HEARING ON  
CYBERSPACE AS A WARFIGHTING DOMAIN:  
POLICY, MANAGEMENT AND TECHNICAL

5 MAY 2009

NOT FOR PUBLICATION UNTIL  
RELEASED BY THE  
HOUSE ARMED  
SERVICES COMMITTEE

Chairman Smith and members of the Committee, I am pleased to appear before you today to provide you with an overview of the Navy and Marine Corps team's views on Cyberspace as a Warfighting Capability, especially those affecting Navy and Marine Corps missions at home and abroad. In a 12 May 2008 policy memorandum, the Deputy Secretary of Defense directed the Department of Defense to use a definition of cyberspace consistent with that provided in National Security Presidential Directive 54 / Homeland Security Presidential Directive 23, which defines cyberspace as a global domain within the information environment consisting of the interdependent network of Information Technology (IT) infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. This emerging battlefield space presents new challenges to our Information Management (IM) and Information Technology (IT) systems, practices and management.

Information management and information technology have become the crucial elements supporting our warfighters. The Navy and Marine Corps rely upon our networks to deliver combat power, provide intelligence and support business operations. Internet protocol based communications permeate the battlefield. Cyberspace has become inextricably linked to the success of kinetic forces and our ability to accomplish the broad mission set of the Navy and Marine Corps. The Department of the Navy's (DON) reliance on cyberspace to conduct its missions and warfighting functions will continue to increase for the foreseeable future. A challenge we face in this domain is that information technology changes rapidly due to market forces and Naval systems change at a vastly slower pace. The need to remain current with technology and the ability to provide information to the warfighter is inconsistent with the

system development cycle times. Our effort must be directed at modernizing our approach to development in order to meet these needs.

### Policy Challenges

Some challenges the Department of the Navy is focusing on are governance, policy, acquisition, role clarification and our relations with the Defense Industrial Base.

To ensure success in cyberspace, effective governance is critical. Current authorities and processes for making decisions affecting security, the design of our systems, and our portfolio of investments require adjustment to fully support cyberspace as a warfighting domain. These adjustments will improve our DON Enterprise Architecture standards and processes to better enable the exchange of information, the integration of systems and the operational management of technology resources. We also recognize the need to refine our IT asset management approach and policy to better ensure our security posture.

As the Defense Science Board (DSB) stated in their recent report on Acquisition of Information Technologies, “a new acquisition approach is needed that is consistent with rapid IT development cycles and software-dominated acquisitions.” Specifically, the DSB stated the DoD needs to “develop new acquisition and requirements (capabilities) development processes for information technology systems.” These must include a holistic view of our “business systems, information infrastructure, command and control, ISR (intelligence, surveillance, and reconnaissance) systems, embedded IT in weapons systems, and IT upgrades to fielded systems.”

To address a portion of this new acquisition approach, the Department of the Navy is currently in the process of implementing a more proactive approach to Clinger-Cohen Act Certification. This approach will be closely aligned with our formal requirements and acquisition review and approval processes. It will ensure that Department of the Navy cyberspace investments and capabilities comply with the overarching tenets of the Clinger-Cohen Act, to:

- a. implement effective information systems;
- b. identify and track improvements to mission performance;
- c. deploy business process improvements before investing in information technology and national security systems; and
- d. accommodate the fast-paced nature of the IT industry in order to avoid outdated procurement approaches that do not take advantage of competition.

Cyberspace operations present unique and uncertain operational environments. Clearly defining the rules of engagement for cyberspace within both the uniformed and civilian domains will require careful deliberation. Law enforcement and criminal investigations, operations and related efforts, and military and intelligence functions must be well synchronized to ensure unity of effort.

Further, the implementations of the statutorily defined roles within the military departments are challenged in adequately addressing the growing cyber threat. Traditional command and control, management and acquisition all must become seamless within the IT space. Policies that control fighting, defending, information assurance and operations in cyberspace must be synchronized and consistent since all these functions occur in the same domain. Our policies need to be

synchronized to de-conflict fighting and defending operations in cyberspace. At present, the Department of the Navy faces challenges meeting the various statutory obligations while maintaining an agile posture to respond to emerging threats. In addition, the implementation of any statutory construct must be informed by a new understanding that our network environment, up to our desktops and personal electronic devices, is the new battlefield.

A final topic to address in this area is security threats to the Defense Industrial Base (DIB) who manufacture our weapons and information systems. Our networks have been under attack for more than a decade, and we must acknowledge that cyberspace is a contested domain. While we employ resources to offer a comprehensive multi-disciplinary approach to protecting our networks, we need to do more. The threat to our infrastructure and information is advanced, persistent, sophisticated, always changing, and well resourced. The challenge to the DIB is to be as vigilant and secure as the DoD and be able to maintain a security posture that enables seamless information sharing. Sustainment of this goal is impacted by the extent to which policy enables organizations to engage in an active defense of the DIB.

### Management Challenges

Some challenges the Department of the Navy is focusing on are total workforce training and education, improving acquisition agility, critical infrastructure protection, and budget agility.

The Department of Defense is undergoing a significant transformation in culture, organization, structure and alignment to enable the full range of operations in cyberspace that will have broad

implications for the DON. Cyberspace management must be consistent and seamlessly linked with joint and national efforts. The DON is engaged in an intensive and comprehensive effort to improve its cyberspace governance, workforce capabilities and management approach in response.

Historically, we are oriented to acknowledge the contribution of weapons platform investments such as planes and ships to our security. Cyberspace resources must be controlled independently of the platforms they reside upon to ensure compatibility and common architectures to reduce security vulnerabilities and training cost. However, the principal management challenge arising from the emergence of cyberspace are policies governing the planning, programming and execution of our resources. Consequently, we are challenged to balance competing demands for limited resources between cyber-oriented and more traditional weapons platform investments. The cycle time associated with IM/IT moves far faster than our ability to plan, budget, and acquire, forcing potentially poor investment decisions. Further, a tighter integration of enterprise architecture, cyberspace warfighting requirements and our investment decision making process characterize the focus of our efforts.

A highly skilled workforce, trained to common DON, DoD and Federal standards is essential to meeting cyberspace requirements. The effective operation and governance of our IT will be grounded in the abilities of our workforce. Cyberspace spans multiple occupational fields, and the workforce communities must be highly synchronized to be effective. Identifying, attracting and retaining a highly qualified total workforce is an ongoing challenge which the DON is aggressively attacking through multiple strategies. The DON must also address the ability of our

current education and training development model to integrate lessons learned and the requirements of a rapidly changing IT domain. We must create a more responsive process of training development. We are investigating and leveraging all available education and training sources and processes to streamline, improve and align our training development and delivery.

Further, we must establish a culture within the Department wherein our members' understanding of their responsibilities for network security is ingrained in every single member. They must understand the ramifications of their actions on the information environment. Every action affects the security and operation of our networks which in turn affects every aspect of our warfighting environment as evidenced by our recent thumb drive issue which would have been reduced through proper adherence to network security policies. This cannot be stressed enough; the manner in which we engage every day on the network must be secure and conscientious.

Achieving and sustaining the goal of information superiority requires that we establish, maintain, and defend a secure and interoperable infrastructure. The Navy and Marine Corps rely upon the nation's infrastructure to perform their mission. Strikes against critical infrastructure can damage the economy, terrorize the population, and degrade or neutralize our Naval capability.

### Technical Challenges

Some challenges the Department of the Navy is focusing on are ensuring secure access to information across the Global Information Grid, integrating Open Architected solutions, and protecting our critical infrastructure.

The DON is leveraging many technologies to improve security and lower cost. However, technical solutions delivered by industry to meet general market needs are often inadequate to meet military use in high threat environments wherein adversarial attack is presumed. Further, industry produces software products at rates sufficient to meet the needs of most users but, some software producers cannot react rapidly enough to security vulnerabilities to ensure security of our information. Investments in technology must be made to ensure we maintain the capabilities to be proactive vice reactive to security concerns. Open architecture technologies must be integrated, but security of our networks must remain the deciding factor when integrating these technologies. The Department must cooperate with industry to improve our life cycle management of our hardware and software.

In addition, there has been much discussion of using industry software to solve military problems. However, when these applications are put into military use, they have, among other issues, exploitable vulnerabilities. The DON must team with industry to ensure these applications are secure. Through activities such as vulnerability assessments and experimenting with designs, industry can engineer more secure systems that better withstand adversarial attempts to exploit them.

The size and scope of the Department presents technical challenges for networking our systems that few other organizations face. Nearly half of the Navy's ships are deployed at any given moment, making timely technology upgrades across the fleet difficult. Similarly, deployed Marine ground forces cannot be upgraded until they return to CONUS bases with robust

communications infrastructures. Multiple Information Technology architectures impact our security posture, are expensive to maintain and require separate training tracks for our cyber workforce. Addressing challenges such as security and cost containment, the Department is evolving its networking environment into a consistent, integrated naval networking environment allowing Sailors and Marines highly secure and reliable access to necessary information and services.

The DON must significantly reduce the number of points of presence (places the DON GIG connects to the DoD GIG or the Internet) and increase network security and defense resources. Additionally, asset management is essential to obtain the situational awareness necessary for network command and control and security compliance, in conjunction with consistent network architectures to facilitate cyber defense and warfighter success.

A critical emerging technical challenge is to exchange information securely with federal, state, and local departments and agencies, as well as our allies and partners. To enable information sharing across the enterprise and achieve the vision of network centric operations, data must be visible, accessible, and trusted. At present, information is locally owned and managed, which is not conducive to mission success. Additionally, providing the bandwidth necessary to facilitate sharing must be considered at the initial planning stages of any program or system.

Thank you for the opportunity to report to you the DON's views and positions on this vital issue. The Department will continue to exploit the power of information in order to transform the way

the Navy and Marine Corps fight. The assured use and protection of cyberspace is essential to our ability to deliver the Naval component of National Security.