STATEMENT OF

DAVID M. WENNERGREN

DEPARTMENT OF THE NAVY CHIEF INFORMATION OFFICER

BEFORE THE

HOUSE ARMED SERVICES COMMITTEE

TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES

SUBCOMMITTEE

3 APRIL 2003

Mr. Chairman, distinguished members of the Terrorism, Unconventional Threats and Capabilities Subcommittee, thank you for inviting me to discuss the Department of the Navy's (DON's) vision for harnessing the power of emerging technologies to equip our forces to meet the demands of the warfighting environment today and in the future.

TRANSFORMATIONAL VISION

As the Navy-Marine Corps team moves forward to meet the challenges of the 21st Century, our Naval Power 21 vision defines new ways of deterring conflict, new capabilities for waging war and new technologies leading to major increases in operational effectiveness. The transformation will be enabled by interoperable, net-centric operations between Joint Service, Allied and Coalition forces to defend America's interests anywhere in the world. We are building a net-centric environment, integrating the Department's information management/information technology (IM/IT) capabilities across the Sea-Air-Land-Space domain to provide improved capabilities to our warfighters.

NET-CENTRIC OPERATIONS

Net-Centric Operations (NCO) will link sensors, shooters and commanders to provide the superior knowledge required for a more precise, agile, and responsive style of warfare that can sustain sealane access and decisively influence events ashore anytime, anywhere. NCO will provide future warriors superior knowledge from real-time netted sensors, enabling them to act at a faster pace than an adversary.

FORCEnet is the operational construct and architectural framework for naval warfare in the Information Age, integrating warriors, sensors, networks, command and control, platforms, and weapons into a networked, distributed combat force, scalable across the spectrum of conflict from seabed to space, from sea to land. It is crucial to Navy and Marine Corps transformation and is the Naval vehicle to make NCO an operational reality. Through FORCEnet we will link the Navy Marine Corps Intranet (NMCI), the Department's shore-based network; Information Technology 21 (IT-21), the Navy's afloat network; the Marine Air-Ground Task Force (MAGTF) Tactical Data Network (TDN), and the Base Level Information Infrastructure (BLII) program into a seamless enterprise network that forms our contribution to the Department of Defense (DoD) vision of a "trusted, dependable and ubiquitous" network.

The NMCI initiative provides the full range of state-of-the-art network-based information services through an innovative performance-based contract using state of the market equipment and industry leading service providers. NMCI replaces numerous independent and disparate networks ashore with a single secure network and is a vital part of the DoD Global Information Grid, interfacing with IT-21 and MAGTF TDN to enhance the flow of mission critical information to forward deployed forces. NMCI significantly improves the security of our IT enterprise; increases productivity by greater sharing of knowledge and improved interoperability, and gives the Navy and Marine Corps secure, universal access to integrated voice, video and data communications.

The transformational value of this revolutionary initiative has been demonstrated repeatedly. In addition to the tragic loss of life in the September 11, 2001 attack on the Pentagon, the Navy also lost the use of almost 70% of its Pentagon office space. Through the power of a single integrated service provider, the NMCI Information Strike Force was able to reconstitute service to the Navy, replacing hardware, reestablishing the network, and putting roughly 700 people back on line in a few short days, permitting the Navy staff to resume operations in record time. The enhanced security afforded by this enterprise network was demonstrated during the recent "SQL Slammer" attacks on networks. Strictly limiting our NMCI Internet exposure to three external gateways that the Defense Information Systems Agency provides, we exercised our robust firewall policy, intrusion detection systems, filtering and Information Assurance Bulletin/Alert implementation procedures to shield our systems and not a single network or user operating within NMCI was affected by the attack.

IT-21 is a systems approach to IT investment. It brings together software applications and improved shipboard local area networks (LANs) to support embarked staffs, aviation wings, Marines and Combined Forces. It also provides increased storage and distribution at multiple levels of classification to support Joint and allied/coalition operations and satellite communications systems with enough bandwidth to transport large volumes of data into a set of end-to-end capabilities for our forces afloat. Similarly, MAGTF TDN provides network connectivity to Marine Corps Forces as they move from their sea base to their objectives and while conducting sustained operations ashore. MAGTF TDN is an expeditionary capability that provides network connectivity to all components of the

MAGTF. This connectivity includes connections to the Combined/Joint Task Force headquarters and other Service components.

The BLII program modernizes existing IT facilities and installs capability where none exists at major fleet concentration bases and stations outside the United States, providing seamless interface from these locations to NMCI, IT-21 and the rest of the Global Information Grid.

By adapting existing Naval and other Service systems and commercial products in innovative ways, we have developed systems that will be essential elements of future Joint, Inter-Agency and Coalition operations. Beginning as the Naval Fires Network, the Joint Fires Network (JFN) is an architecture that addresses the need for near real time intelligence correlation, sensor control, target generation and development, mission planning, interfaces with engagement systems, and battle damage assessment in time critical strike planning. JFN is realized by interfacing the best elements of three existing systems into a converged architecture: Joint Service Imagery Processing System-Navy (JSIPS-N), derived from a system developed by the Air Force; an adapted Army system, Tactical Exploitation System-Navy (TES-N); and the Global Command and Control System-Maritime (GCCS-M).

Navy, Coast Guard, Allied and Coalition ships form an integrated battle force in current naval operations. Communications by secure email and web services have become the de facto standard for the command and control of this type of force, providing increased

situational awareness, better logistical support and increased information sharing. Access to email and battle group web sites is essential and our Combined Enterprise Regional Information Exchange Systems (CENTRIXS) allows us to configure ship networks and conforms to DoD and NATO architecture and standards. In the past year we have equipped all deploying warships, including two high-endurance Coast Guard cutters, with CENTRIXS capability and provided the architecture to our Allies to enable them to fit out their ships.

In response to Joint requirements, Deployable Joint Command Center (DJC2) is being developed with OSD and Joint Forces Command (JFCOM) oversight. Designed to support a Joint Task Force Commander and staff, DJC2 is Joint from its inception. Using lessons learned from current diverse transportable command centers fielded by the Services and Combatant Commanders, DJC2 will be based upon known Joint or Service systems that are already mature or maturing. DJC2 will be the material piece of the Standing Joint Force Headquarters (SJFHQ) JFCOM is tasked to develop.

KNOWLEDGE CENTRIC INITIATIVES

As we achieve a seamless enterprise network structure, we are simultaneously transforming the way in which information is shared to truly achieve knowledge superiority. Key to the success of our knowledge management efforts is the development and use of collaborative environments and communities of practice. Commands across the Navy – Marine Corps team are leveraging the tenets of knowledge management to create virtual collaboration environments for distance learning, telemaintenance and

telemedicine. In our Collaboration at Sea project, shared information and collaborative planning and decision-making were achieved through the use of a standardized website for non-real time collaboration, chat capability for real time collaboration, and customized website replication to minimize bandwidth requirements for deployed units.

Our use of Communities of Practice has allowed us to truly make knowledge "actionable." The Naval Education and Training Command (NETC) has structured thirteen separate learning centers and hundreds of communities of practice to enable the distributed sharing of targeted content and knowledge management. Naval facilities engineers have shared experiences and information to develop a new, more cost effective formulation for concrete used in pier building. Our submarine community at the Naval Submarine Base, Kings Bay, Georgia has initiated a collaboration and knowledge sharing initiative that will draw upon the experiences of the commands and individuals at Kings Bay to create enriched off-crew training using online, interactive and hands-on techniques.

Our goal is a web-enabled Navy-Marine Corps team, allowing our mobile workforce to have access to self-service transactions, via the web, around the world. Our movement to web services solutions will provide for the establishment of single authoritative data sources and eliminate "stand-alone" and "stove-piped" legacy systems. The cornerstone to this web-enabling effort is our development of the Navy Marine Corps Portal (NMCP). This enterprise portal will provide an integrated collaborative environment and personalized, role-tailored access to information in real time. This single integrated

portal structure will allow our organizations to focus on content delivery, and avoid the costs of individually developing portal features and functions. The NMCP will also reduce application costs, and improve information security, providing our Sailors, Marines and civilians with access to the intellectual capital of the entire Navy– Marine Corps team.

We have made significant progress in supporting the development and use of an Enterprise Architecture for the Department, and have developed policy and guidance in the areas of data, IT infrastructure, standards, applications, and warfighting and business processes. To effectively implement portfolio management, we have identified 23 Functional Areas and assigned responsibilities for managing processes, applications and databases within these areas to Functional Area Managers (FAMs). The FAMs and technical personnel are working to reduce the total number of applications used across our enterprise to eliminate redundant systems and achieve uniform standards and a consistent set of network tools throughout the Department. To date, by eliminating outdated and duplicative software, they have reduced the number of approved applications by over 89%, from 67,000 to 7,000. Our FAMs are identifying, aligning and improving business processes to maximize operational effectiveness and make sound investment decisions. Technical experts within functional areas are defining standards that will maximize information exchange through the use of the maturing commercial technology known as Extensible Markup Language, or XML. Our XML policy, which is the first published by a Federal Agency, is providing the means to facilitate data

exchange among diverse information systems, essential to establishing a net-centric environment.

FULL DIMENSIONAL PROTECTION

The 21st Century presents new challenges for continued maritime dominance and our national security. The security of our information, systems, personnel and critical infrastructure assets is fundamental to our continued success. We have crafted an approach we call "Full Dimensional Protection." Joint Vision 2020 states that Full Dimensional Protection is achieved "through the tailored selection and application of multi-layered active and passive measures." For the Department of the Navy, that protection takes three forms: (1) protecting Knowledge pathways through Information Assurance (IA) and Defense-in-Depth, (2) protecting our Centers of Knowledge through Critical Infrastructure Protection (CIP), and (3) protecting our Knowledge Workers through efforts to protect individual privacy. These protection efforts will ensure the reliability, availability, and integrity of DON information and information systems; protect our people, and protect the critical infrastructure needed to defend and secure our mission-critical capabilities.

IA is essential for warfighting and homeland defense. It is required operationally in the Department of the Navy to protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. Recent denial of service and malicious code attacks; combined with the inability of any one specific defense to stop these attacks, dictate the necessity for a multifaceted,

integrated system, network security defense. The Department has adopted the defense-in-depth strategy to mitigate the risk associated with a single point of failure. Available protection technologies are employed in a layered system of defenses. To this end, attacks directed against systems within defined network boundaries are met by a series of protection mechanisms including, but not limited to, encryption, intrusion detection systems, access control, user identification and authentication, malicious content detection, audit, and physical and environmental controls. Use of these mechanisms will mitigate inherent system vulnerabilities and counter potential threats. The number and type of defense mechanisms used in each boundary layer is a consequence of the protective qualities of the device and the assigned value of the information within the protected enclave. Without appropriate information assurance, reduction or denial of information resources would have a major detrimental effect on the ability of the Navy and Marine Corps to fulfill critical operational missions.

We have established an Information Assurance Policy and are developing an overall Department of the Navy IA Strategy and a Federal Information Security Management Act (FISMA) Action Plan to ensure the Department as a whole is working together to improve and carry out effective IA programs. We are also developing policies for wireless security and remote access to information systems for our reservists and personnel away from their workplace. With these policies in place, and the development of an effective metrics system, our oversight programs will enable us to continually monitor the state of information assurance within the Department. We test the effectiveness of our information assurance posture by conducting annual assessments and

audits of information security, reviews by the Inspector General, and through Red Team operations. The Navy and Marine Corps have infrastructure and personnel in place for ensuring detection, notification, and remedial action of deficiencies and security incidents.

We have put into place an aggressive Critical Infrastructure Protection (CIP) initiative to (1) identify infrastructures, both cyber and physical, essential to warfighting readiness and achievement of operations plans; (2) assess their vulnerability to loss from terrorist actions, natural disaster, or human error; (3) develop a coordinated physical and cyber indications and warnings capability, and (4) take necessary action to ensure the achievement of Navy and Marine Corps objectives in the event of the loss of critical infrastructures.

In my role as Critical Infrastructure Assurance Officer (CIAO), I have worked with organizations across the DON to develop a plan that identifies and protects our critical infrastructure and oversees implementation efforts across the Navy and Marine Corps. A senior council guides the overall direction of this enterprise-wide effort. We have developed a groundbreaking CIP self-assessment tool and reference guide on CD-ROM that provides our base commanders with the capability to identify and assess infrastructure vulnerabilities and strengthen their critical asset protection postures. We built upon existing best practices in force protection, anti-terrorism and systems security; adding new initiatives that promote understanding of mission dependence on commercial, state and local infrastructures. This expanded vulnerability assessment process not only

identifies mission critical vulnerabilities, but also recommends appropriate corrective action.

We have partnered with state and local governments, as well as private industry in meeting CIP challenges. For example, we have pursued regional Integrated Vulnerability Assessments with Homeland Security officials. In 2002, we conducted Naval Vulnerability Assessments of the National Capitol Region and Hampton Roads area, working closely with the Secure Virginia Panel. We also conducted the first multi-jurisdictional, cross-border tabletop CIP exercise in June 2002. Entitled "Blue Cascades," the event was attended by over 150 representatives from 70 public and private sector organizations. The exercise was hosted by the Pacific Northwest Economic Region (PNWER) and cosponsored by the Navy, the Federal Emergency Management Agency (FEMA Region 10) and the Canadian Office of CIP and Emergency Preparedness (OCIPEP).

Privacy is the third leg of our Full Dimensional Protection program. Now, more than ever, striking the delicate balance between personal privacy and national security is a challenge faced by the entire nation. The strengthening of security controls throughout the country has heightened America's sensitivity to the protection of civil liberties. The Department of the Navy recognizes this fact and has taken proper steps to ensure privacy protection by creating tools and policies to aid in the protection of personal information in DON systems. To support these efforts, we developed and distributed within the

Department a privacy education and awareness tool CD-ROM, and are developing a Privacy Impact Assessment for use by our program managers.

eBUSINESS/eGOVERNMENT INITIATIVES

Our eBusiness efforts are transforming labor-intensive paper processes into reengineered, efficient, and effective web-based solutions. Aligning with the tenets of the President's Management Agenda, our efforts have achieved, and will continue to produce, substantial efficiencies and significant resource savings and cost avoidance across every mission area of the Department – providing the force multipliers of value and improved services to the warfighter. We established the DON eBusiness Operations Office as an innovation center to encourage commands to adopt eGovernment solutions. The efforts of this office, in particular its pilot initiatives, have resulted in significant achievements. For example, a $100K investment in a web-based medical appointment initiative at the Naval Medical Center, San Diego will eventually yield a cost avoidance for DoD of about $18M and provides markedly improved customer service. The DON received a 2002 eGovernment Performance Leader Award for this initiative.

I chair the DoD Smart Card Senior Coordinating Group (SCSCG), a DoD-wide alliance for rollout of a single smart card across the Department of Defense. The result of this group's efforts is the successful rollout of the Common Access Card (CAC) that is being issued to all active duty military, Selected Reserve, government civilian and selected contractor personnel – a total population of approximately four million. It serves as the new Geneva Convention identification card for military members and is our cyber

identification and physical access card. To date, the DoD has issued over 2.2 million CACs and the DON has been a leader in this effort with over 890,000 CACs issued to Navy and Marine Corps personnel. The value of the CAC is multi-dimensional, but one of its greatest attributes is as the carrier of our Public Key Infrastructure (PKI) digital certificates, providing the ability for cryptographic logon to networks, secure authentication to protected websites and the ability to digitally sign electronic transactions, which are key to the success of our eGovernment transformation. We will continue to expand and improve the Common Access Card, and are currently developing and testing the next generation CAC platform that will incorporate contactless and biometric technologies to further enhance and strengthen our physical security and force protection efforts.

IM/IT WORKFORCE

People are the heart of our organization. We know our real power comes through our people - what they know, how they bring their knowledge together and how they translate that knowledge into action. As a result, we are always looking for ways to provide our personnel with opportunities to develop professional skills aligned to mission requirements. We are identifying specific ways to recruit and develop employees who have the knowledge, skills, abilities and behaviors needed to support current and emerging mission requirements; and are strongly committed to provide both our military and civilian IM/IT personnel the opportunities they need to stay current in an increasingly complex technology-based environment. To meet our people's career development needs, and thereby achieve our broader goal of a highly skilled workforce, we have been

developing guidance, tools, and programs that focus on career development. As an example, the establishment of the Navy Information Professional officer community assures the growth and development of individuals who will be critical to our IT future.

Under the Information Assurance (IA) Scholarship Program, we have provided graduate level IA education to Navy and Marine Corps personnel serving in critical security billets. To ensure our Sailors returning from sea duty keep their skills current, we are capitalizing on the training opportunities afforded by NMCI, assigning them to work in our network operations centers alongside -- and training with -- our support contractors in a world class environment. For civilians, we have defined the competencies that we believe are key to our future and provided a tool for career planning. The Federal CIO Council has adapted the tool for use across the Federal Government as the IT Roadmap career development tool for over 66,000 IT professionals. Given the diverse challenges that we continue to face, we recognize that we must stay vigilant to the needs of our people, which will continue to evolve and require resourcing to enable us to stay responsive to mission requirements.

DON IM/IT GOVERNANCE

We have embarked upon a significant restructuring of information management/information technology governance across the Department. This restructuring will strengthen, align, and integrate our IM/IT efforts across the Navy and Marine Corps; strengthen the tie between the Secretariat and the Services; and ensure Department-wide alignment of IM/IT efforts with warfighter priorities. A key element of

the restructuring was the designation of RADM Thomas E. Zelibor, Director, Space, Information Warfare, Command and Control Division (CNO N61) to be dual hatted as the Department of the Navy Deputy Chief Information Officer (Navy) and BGEN John R. Thomas, Director for Command, Control, Communications, and Computers (C4) to be dual hatted as the Department of the Navy Deputy Chief Information Officer (Marine Corps). These designations as DON Deputy CIOs are in addition to their C4 responsibilities in the operational chain of command and are separate and distinct from their CIO responsibilities. However, this dual hatted organizational structure enables a close alignment between C4 and CIO responsibilities. Another essential element of the restructuring is the development of a DON IM/IT Enterprise Implementation Plan. This plan will link our vision and strategy to programmatic and budgeting guidance and serve as the basis for approving and funding IM/IT investments.

Mr. Chairman, members of the Subcommittee, I thank you again for allowing me the opportunity to speak to you today. We greatly appreciate your support of our information technology initiatives to meet the challenges we face and I look forward to working with you on these important initiatives.

I will gladly answer any questions that you may have about the Department of the Navy's information management/information technology initiatives.