DEPARTMENT OF THE NAVY

Enterprise Mobility 2008

Message From the CIO

The net-centric environment of the Global Information Grid (GIG) will provide our warfighters with Information Superiority, affording decision superiority, tactical advantages and enabling mission accomplishment. To maximize these benefits, information must be available where the warfighters and those who support them are located - even if no traditional, wired network infrastructure is in place. The ever advancing capabilities delivered in commercially available wireless technologies present the Department of the Navy (DON) with opportunities to expand secure information access to the warfighters in locations where previously, such access would have been impossible or impractical. This Enterprise Mobility 2008 report describes the process the DON will use to leverage the significant advantages these technologies can deliver while ensuring required levels of Information Assurance and performance. As this document highlights, the Department has already made great strides in making information available to those who need it, where they need it, and our enterprise mobility capability will continue to be enhanced on an ongoing basis.

I appreciate the efforts of the DON Wireless Working Group in forwarding this important work.

Robert J. Carey
Department of the Navy
Chief Information Officer

Overview

Enterprise mobility – the ability to provide Sailors and Marines with the information they require as they move between office, garrison, and battlefield or ad hoc locations – is a critical component of the Department of the Navy's (DON) efforts to support the warfighters and those who support them. Enterprise mobility represents the last link in the network that provides the warfighter with the "power to edge" component of net-centric warfare (NCW); indeed, without this capability NCW would be impossible.

In addition to customized military-specific solutions, the Department looks to a variety of commercially available wireless products to meet much of its enterprise mobility needs. There are significant advantages to this approach. Adopting commercial products:

- Assists in standardizing equipment;
- Provides interoperability across the Department as well as with Joint and coalition forces;
- Allows the DON to take advantage of the research and development (R&D) of the commercial sector;
- Provides a ready-made near-global network supporting voice and data;
- Preserves the increasingly precious spectrum assigned to the Department through the use of shared, unlicensed frequencies; and
- Is more cost effective than building customized wireless solutions.

At the same time, all wireless technologies have inherent drawbacks and resultant concerns. Chief among these concerns, of course, is the security of the signal as it traverses the airways. Another significant concern is the potential for a wireless platform to introduce new radio frequency emanations into a military environment where they might have an impact on weapons systems. Implementation of wireless technologies cannot go forward until these and other potential drawbacks are satisfactorily addressed.

Enterprise Mobility 2008 describes the strategy the Department is following in assessing and adopting commercially available wireless products to enhance its enterprise mobility capability. Specific program timelines and milestones will be developed as appropriate, by program managers as their projects progress.

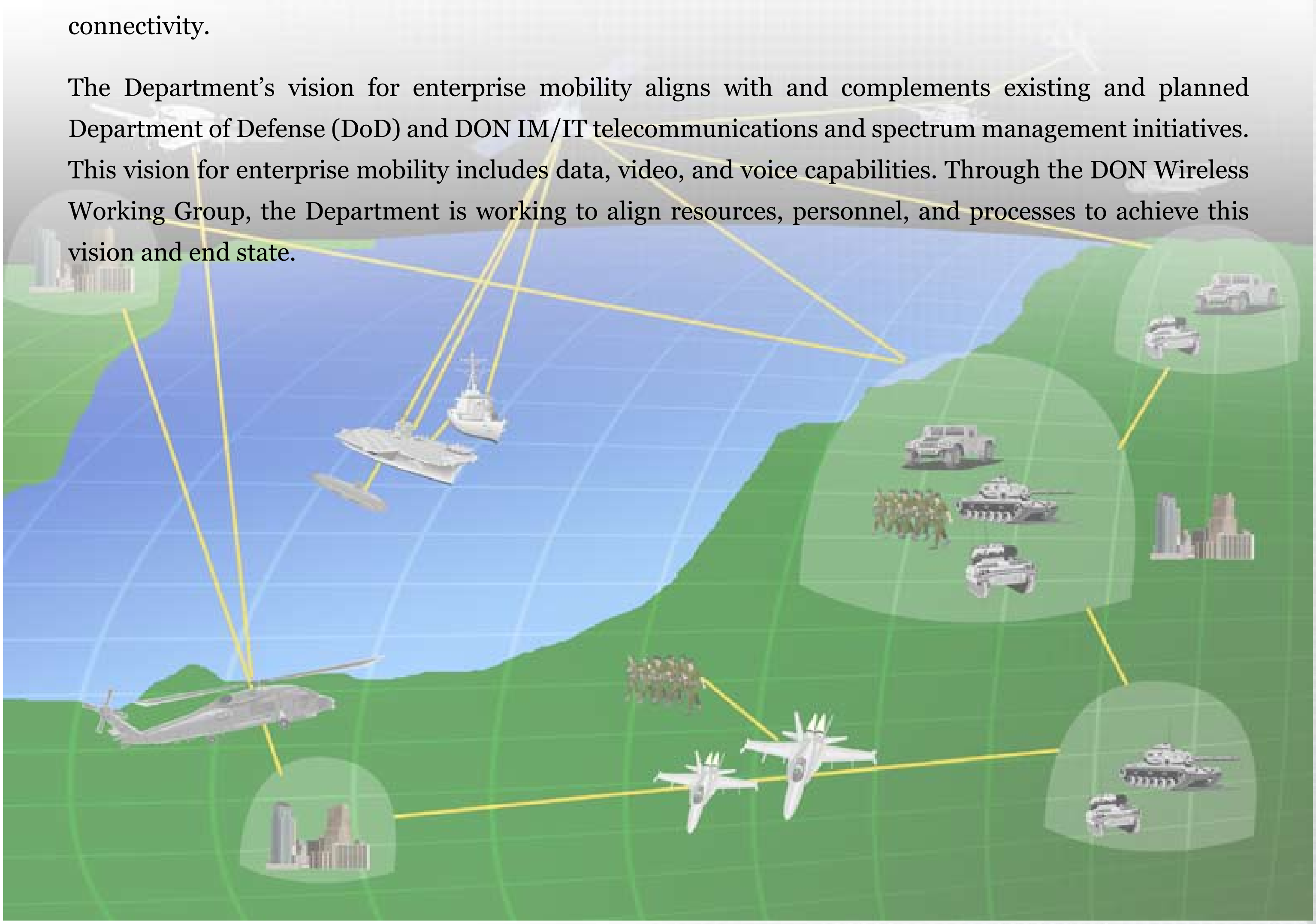
Vision

Provide robust, secure, and ubiquitous access to the required information through the development of an enterprise mobility capability that incorporates commercially available wireless products and solutions.

Provide robust, secure, and ubiquitous access to the required information through the development of an enterprise mobility capability that incorporates commercially available wireless products and solutions.

The end state capability to realize this vision will utilize "smart" devices in the field that automatically sense networks, devices and users and configure themselves to deliver the right information to the user through the best network option available, including, if necessary, connecting to other smart devices within range. Solutions will range from simple ones implementing one device and technology to more complex networks where a variety of devices and technologies will operate in concert under a "bubble" of wireless connectivity.

The Department's vision for enterprise mobility aligns with and complements existing and planned Department of Defense (DoD) and DON IM/IT telecommunications and spectrum management initiatives. This vision for enterprise mobility includes data, video, and voice capabilities. Through the DON Wireless Working Group, the Department is working to align resources, personnel, and processes to achieve this vision and end state.



Commercial Wireless Products

The DON looks to a variety of commercially available wireless products to meet much of its enterprise mobility needs. These include cell phones, personal digital assistants (PDAs), BlackBerrys®, smart phones combining multiple functions, laptops with wireless fidelity (WiFi) and/or air cards, sensors, and Radio Frequency Identification (RFID) systems. As technology convergence drives more power and functionality into smaller and smaller devices, such as smart phones, they become increasingly important in delivering enterprise mobility. Using commercial wireless products also enables standardization and interoperability across the Enterprise. Additionally, advantages are realized in spectrum utilization and cost efficiencies.

These benefits have great potential for the DON as it matures its net-centric warfare infrastructure. For example, Marines in the battle theater can quickly set up a wireless local area network in a temporary location and have access to the GIG and crucial tactical information such as live video provided by an Unmanned Aerial Vehicle (UAV). Onboard, ships' systems can be monitored in real time from a central location with the use of wireless sensors, thereby freeing up Sailors for other tasks.

At the same time, all wireless technologies have inherent drawbacks and resultant concerns. Chief among these are:

- Information Assurance - can the traffic be intercepted and read by an adversary or easily jammed, thereby preventing information from getting through? This is particularly important as classified voice and Secure Internet Protocol Router Network (SIPRNET) communications will increasingly utilize wireless transport modes.
- Interference - will introducing new radio frequency emanations into a military environment negatively impact existing systems? Interference can hamper communications, degrade the performance of co-located electronics, or even cause ordnance to malfunction, an effect called Hazards of Electromagnetic Radiation to Ordnance (HERO) [1].
- Robustness - will the solution work across settings? For example, different frequencies have different propagation characteristics; what works well in a wide open environment may not work nearly so well in a shipboard environment with its numerous metallic enclosed spaces.
- Non-standard spectrum allocation - differing spectrum assignments in some countries mean that some equipment cannot be used globally without gaining permission to operate from the host nation.

Due to the special nature of the warfighters' mission, these concerns are critical. Weaknesses in a wireless network could easily lead to the compromise of operational details and put lives and mission accomplishment at risk. The challenge for the DON is implementing solutions that will maximize the benefits of these technologies while minimizing the risk inherent in them.

A number of working groups, project teams and experts from the DON, DoD, and other organizations collaborate to eliminate or significantly reduce these risks before a solution is approved for use. The DON Wireless Working Group plays a key role in facilitating these efforts.

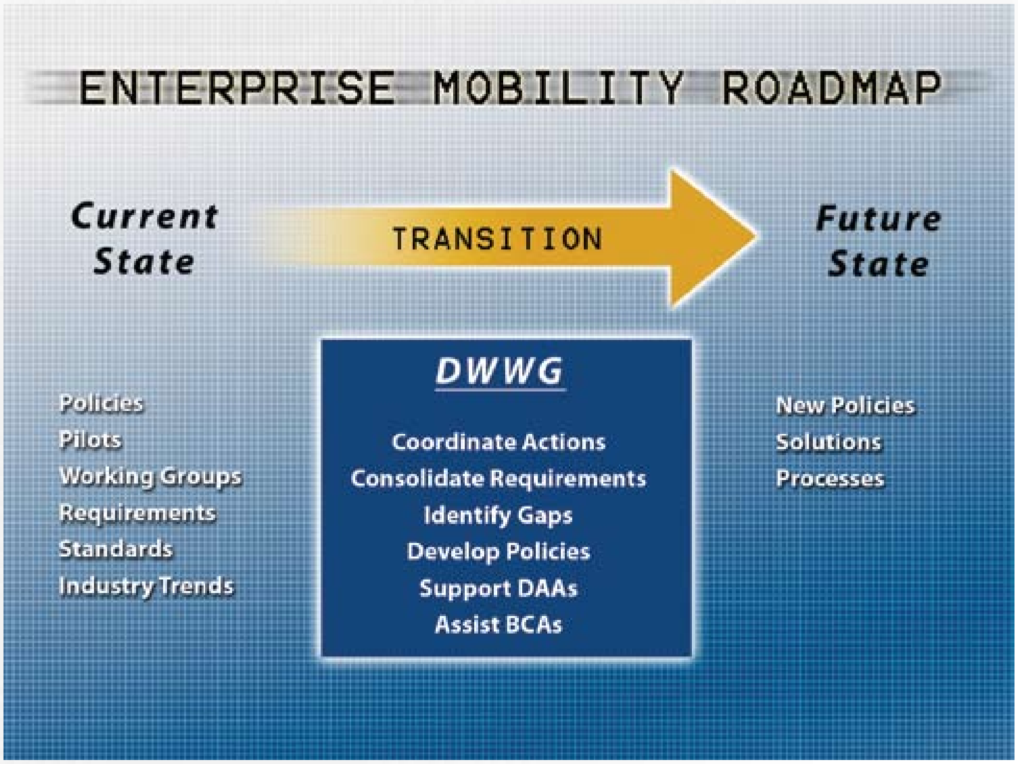
[1] Personnel and fuel may also be subject to hazards of electromagnetic radiation, referred to as HERP and HERF respectively.

DON Wireless Working Group

The DON Wireless Working Group (DWWG) was established by the DON Information Executive Committee (IEC) in 2005 to provide leadership in wireless solutions and coordinate the Department's efforts in attaining the vision for enterprise mobility. The DWWG operates under the aegis of the IEC, which is composed of the DON CIO, Chief of Naval Operations N6 (CNO N6) and Headquarters Marine Corps Command, Control, Communications and Computers (HQMC C4). The DWWG charter is included as Appendix A.

The work of the DWWG also has relevance to two related initiatives in the Department - Spectrum Management and Telecommunications. Components of these groups communicate and coordinate actions with the DWWG as needed to ensure an integrated approach to enterprise mobility.

The DWWG is a critical component of the Department's efforts to minimize and manage the risk involved in introducing new technologies to the DON technical architecture. By maintaining visibility into the Department's wireless environment – including baseline capabilities, requirements, Research and Development (R&D) activities, and policies – it serves as overseer and facilitator of DON enterprise mobility strategies and the Department's transition from the current state to the future state.



ENTERPRISE MOBILITY ROADMAP

Current State

TRANSITION

Future State

Policies
Pilots
Working Groups
Requirements
Standards
Industry Trends

DWWG

Coordinate Actions
Consolidate Requirements
Identify Gaps
Develop Policies
Support DAAs
Assist BCAs

New Policies
Solutions
Processes

The following summarizes the activities of the DWWG. Through these activities the DWWG fosters coordinated action and allows the Department to maintain a coherent and orderly approach to the introduction of new technologies and applications.

Policy Development. Traditional DoD and DON policies do not always adequately address new technologies such as commercial wireless devices. The DWWG actively works with DoD and DON personnel to continually refresh or develop new policies based on new requirements, technology trends, and feedback from trials. Interim guidance in the form of memos and messages make up part of the policy environment and help delineate the available solutions into R&D and operational capabilities[2].

Consolidation of Requirements. As different DON components develop their unique wireless requirements, the DWWG is in a position to identify and consolidate common requirements across the Department. This may lead to cost savings through combined acquisitions as well as improved project success. In some cases, existing solutions may not address identified requirements. The DWWG will forward these to the Office of Naval Research for potential inclusion in the Rapid Technology Transition program or other R&D efforts.

Knowledge Sharing. Personnel in different DON components recognize potential applications for new and emerging wireless technologies to meet mission requirements and conduct trials that can be viewed as part of the Department's wireless R&D activities. If allowed to remain stove-piped however, the Department as a whole would be deprived of the lessons learned from these trials. Data from both successful and unsuccessful experimentation are valuable for all interested parties and provide a feedback loop into the DWWG process. In this manner the DWWG fosters the exchange of information and experiences within and between the Services and serves as a clearinghouse of information.

Assist Business Case Analysis (BCA). Departmental components may envision useful applications for wireless technologies but lack the expertise to develop a compelling BCA to support them. The DWWG can assist DON units in developing BCAs that are comprehensive and that address costs, benefits, alternative solutions, business impacts, risks, and contingencies.

Support Designated Approving/Accrediting Authorities (DAAs). DAAs are responsible for approving the use of systems within the DoD and ensuring that DoD Information Assurance Certification and Accreditation Process (DIACAP) and other Information Assurance (IA) requirements are met. The characteristics of wireless transmissions and devices bring added complexity to IA. Data must be secure, not only when it is being transmitted, but also as it is stored on devices, should one become lost or otherwise compromised.

A key component of the DAA's analysis is identifying the level of residual risk in a system after all reasonable security precautions have been taken and whether that level is acceptable or not. This task becomes more difficult when rapidly evolving technology is involved. The DWWG's work and expertise support DAAs as they confront these issues with wireless solutions and will assist them in coordinating actions with DAAs across the DoD and Department of Homeland Security (DHS).

[2] Current overarching policy is included in Secretary of the Navy Instruction 2075.1, Department of the Navy Use of Commercial Wireless Local Area Network (WLAN) Devices, Services and Technologies, 30 November 2006.

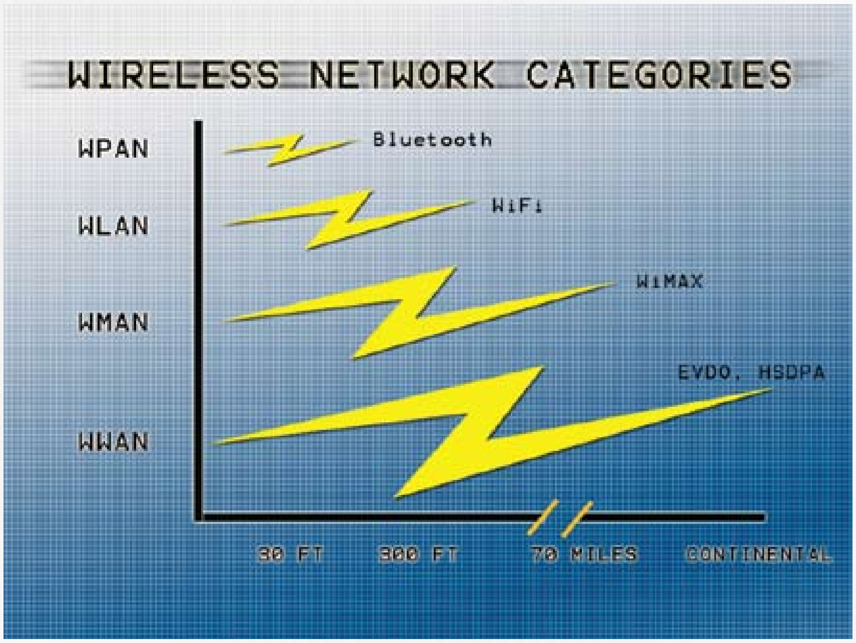
Wireless Technologies

The various wireless technologies that are available to serve the Navy-Marine Corps team can be sorted in a number of ways, but perhaps the most useful is by the typical range of coverage they provide. Solutions generally fall into the following categories: Wireless Personal Area Networks covering up to 10 meters/32 feet; Wireless Local Area Networks covering up to 100 meters/328 feet; Wireless Metropolitan Area Networks covering up to 112 kilometers/70 miles; and Wireless Wide Area Networks that can provide nationwide and continent-wide connectivity. Each of these solutions may connect to the GIG or other enterprise networks directly or indirectly.

Each of these technologies is based on specific technical and industry standards. Technical standards are generally promulgated by bodies such as the Institute of Electrical and Electronics Engineers (IEEE), which defines the underlying technical foundation and specifications. Industry groups, working through forums organized around a specification, then agree on implementation strategy to ensure interoperability among each vendor's products. An IEEE standard carries a numeric identifier, such as 802.11g, while the associated commercial products utilize more user-friendly nomenclature, *WiFi* in this case.

While these solutions primarily operate in portions of the spectrum that do not require a license, the parameters under which they can be operated are regulated to ensure minimal interference with licensed spectrum. In the United States, the Federal Communications Commission (FCC) provides the overarching regulatory environment for non-federal use of the unlicensed spectrum under Part 15 of its rules. Devices that are commercially available are said to be Part 15 compliant. Licensed spectrum, such as that utilized by cellular providers, is regulated under different FCC regulations. For federal spectrum users, the National Telecommunications and Information Administration within the Department of Commerce develops guidelines and rules to which the DON must adhere.

Any operator of a Part 15 device has no "right" to the spectrum and must accept interference from other authorized users. As a result, users of Part 15 devices assume the risk of interference by others using similar equipment in their vicinity. However, in actual practice, the devices' networking capabilities have advanced to the point where they are usually able to correct for any inadvertent interference emanating from another Part 15 device when used in a compliant manner. This is not necessarily true when a device is used in a noncompliant manner, such as by using more power than allowed under the specifications and/or regulations.



The following are typical applications for each wireless category:

Wireless Personal Area Networks (WPAN). A WPAN provides connectivity between devices within a radius typically limited to 32 feet. Designed with low power levels and relatively low data rates, WPAN devices may be limited in capacity but provide significant convenience and extensive benefits when used in certain applications.

Bluetooth (IEEE 802.15.1) is probably the most well known WPAN technology and is the technology behind your personal wireless cell phone headset. Other uses include wireless PC keyboards, mouse units, and game controllers. Bluetooth-enabled devices are easy to set up as they can identify other "trusted" devices and connect to them automatically. Up to eight devices may be connected in a *piconet*. Currently, the use of Bluetooth in the DON is restricted to approved Bluetooth smart card readers.

Ultrawideband (UW, IEEE 802.15.4) is another WPAN technology. UWB devices are used on sensors and automated home devices such as wireless motion and smoke detectors. UWB is also used for directly connecting digital cameras and printers.

Wireless Local Area Network (WLAN). WLANs are networks of computers, with or without servers, connected wirelessly instead of with traditional Ethernet cable. WLANs can be set up quickly and easily without the traditional overhead of network equipment; just one access point and wirelessly-enabled workstations are required. By being untethered to the network workstations, laptop computers can be portable and freely moved within the signal's range without loss of connectivity.

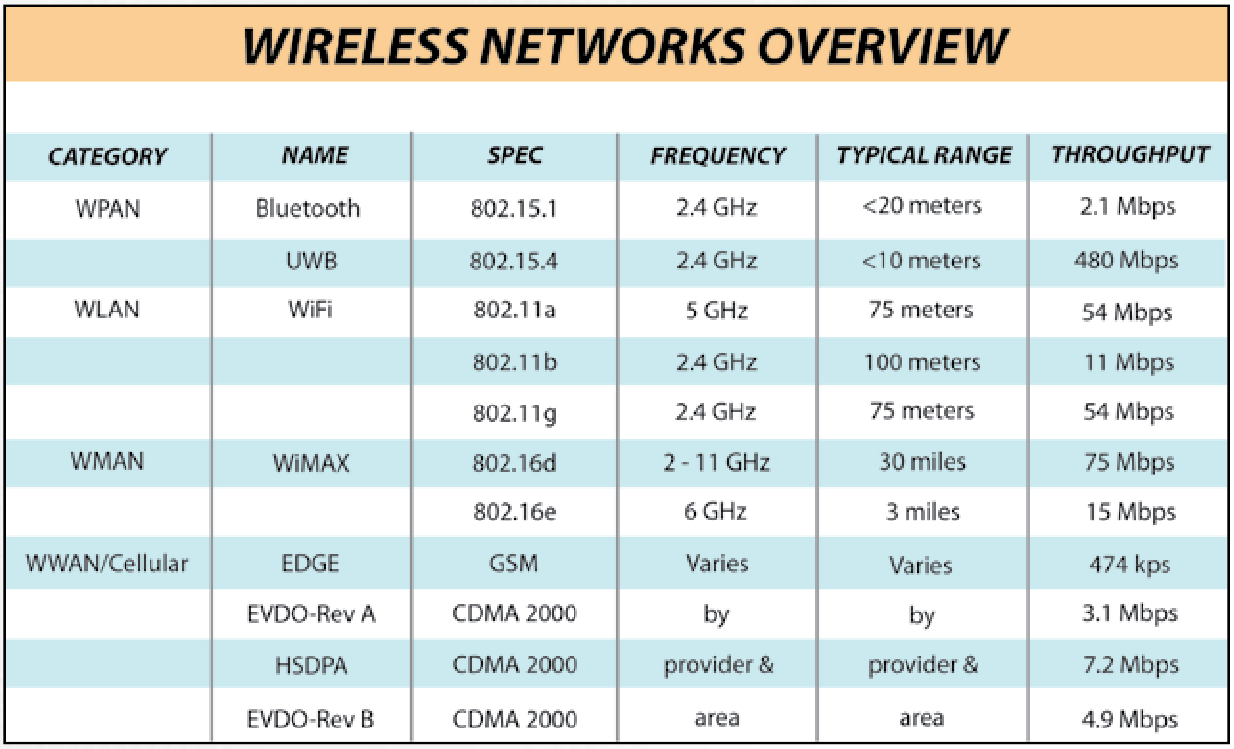
WiFi. By far the most prominent use of WLAN is WiFi, based on the IEEE 802.11 family of standards. WiFi has become synonymous with wireless computing to the general public and is built into almost every laptop sold today. WiFi is nearly ubiquitous from home networks to coffee shops and even to some citywide applications utilizing multiple access points.

Wireless Metropolitan Area Network (WMAN). WMANs provide connectivity at a much higher data rate and over considerably longer distances than WiFi. This makes them well suited to provide backhaul services for WiFi or wired networks in areas where direct, wired access to the Internet is not possible. At the same time, WMANs may operate as WLANs with extended reach and capacity.

WiMAX (Worldwide Interoperability for Microwave Access). WiMAX (IEEE 802.16d/e) has increasingly become the de facto WMAN standard over all others. Its reach can cover tens of miles and users can be truly mobile. WiMAX has been designed with enhanced security over WiFi. As Quality of Service has also been designed into WiMAX, it can carry voice traffic (Voice over Internet Protocol or VoIP) much more effectively than WiFi.

Wireless Wide Area Networks (WWAN). Wireless WANs are offered commercially by cellular phone companies. Due to the build-out of their networks, national and even continental-wide seamless access to the network is often available. Subscribers can access the network through their smart phones or via air cards inserted into a laptop's PCMCIA/USB slot or through a laptop with a built-in WWAN capability. There are three primary access routes to these networks, EDGE, EVDO, and HSDPA, in increasing order of bandwidth. Carriers are expected to continue to increase the reach and capacity of their WWAN offerings. Additionally, new providers are expected to enter the marketplace under impending FCC rules.

Access to a WWAN network may take the form of one person/device communicating with the carrier network, as when one accesses the Internet on a smart phone, or through the implementation of a Virtual Private Network (VPN), which allows an organization to extend its internal network over the commercial network and provide access to field and mobile workers. Common VPN applications include sales force automation, support for field technicians, and mobile public safety networks providing vehicular access to common databases and systems.



WIRELESS NETWORKS OVERVIEW

CATEGORY	NAME	SPEC	FREQUENCY	TYPICAL RANGE	THROUGHPUT
WPAN	Bluetooth	802.15.1	2.4 GHz	<20 meters	2.1 Mbps
	UWB	802.15.4	2.4 GHz	<10 meters	480 Mbps
WLAN	WiFi	802.11a	5 GHz	75 meters	54 Mbps
		802.11b	2.4 GHz	100 meters	11 Mbps
		802.11g	2.4 GHz	75 meters	54 Mbps
WMAN	WiMAX	802.16d	2 - 11 GHz	30 miles	75 Mbps
		802.16e	6 GHz	3 miles	15 Mbps
WWAN/Cellular	EDGE	GSM	Varies by provider & area	Varies by provider & area	474 kps
	EVDO-Rev A	CDMA 2000			3.1 Mbps
	HSDPA	CDMA 2000			7.2 Mbps
	EVDO-Rev B	CDMA 2000			4.9 Mbps

Voice – Land Mobile Radio (LMR) and VoIP. The majority of the technologies discussed so far are primarily used for the transmission of data encapsulated in packets on an IP-based network. However, enterprise mobility also includes supporting voice – a capability that today is normally provided via legacy radio systems. Wireless voice communications are often provided by LMRs, which are commercial off-the-shelf (COTS) or government off-the-shelf (GOTS) systems consisting of base stations and mobile/handheld radios. Critical components of LMR functionality include the ability to communicate and coordinate with state and local first responders and support the Anti-Terrorist/Force Protection mission, as well as support shipboard flight deck safety and ship damage control survivability operations. Advances in Software-Defined Radio systems and antennas allow greater operating flexibility, providing Sailors and Marines with new communications capabilities to support a variety of missions.

The ability to provide VoIP can deliver significant benefits in streamlining the entire communications network infrastructure and increasing the return on investment of building that infrastructure. While VoIP is increasingly being implemented within wired networks, the wireless environment presents special challenges in reliability, quality of service, interference, spectrum use, and security.

At the same time, early VoIP trials have shown great promise. There is little doubt that as the convergence of analog and digital IP-based communications technologies advances, wireless VoIP will play an increasingly prominent role within the DON.

Automated Identification Technology (AIT). AIT enables and facilitates the accurate capture and rapid transmission of machine-readable data to information systems. AIT enhances the readiness of deploying forces, with accurate knowledge of their equipment, personnel, and capabilities in support of their respective missions. For example, through AIT the contents of a shipping container can be automatically and accurately inventoried as it passes through the logistics chain. AIT solutions often rely on wireless technologies such as WiFi or WiMAX, using RFID tags or portable data terminals that communicate wirelessly with the primary logistics application.

The DON has used AIT for a number of different applications and the results have been significant savings in personnel time, reduced costs, and enhanced end-to-end visibility in the value chain. The DON AIT program office works with the DWWG and other relevant DoD entities as they broaden the scope and capabilities of the AIT solutions being deployed.

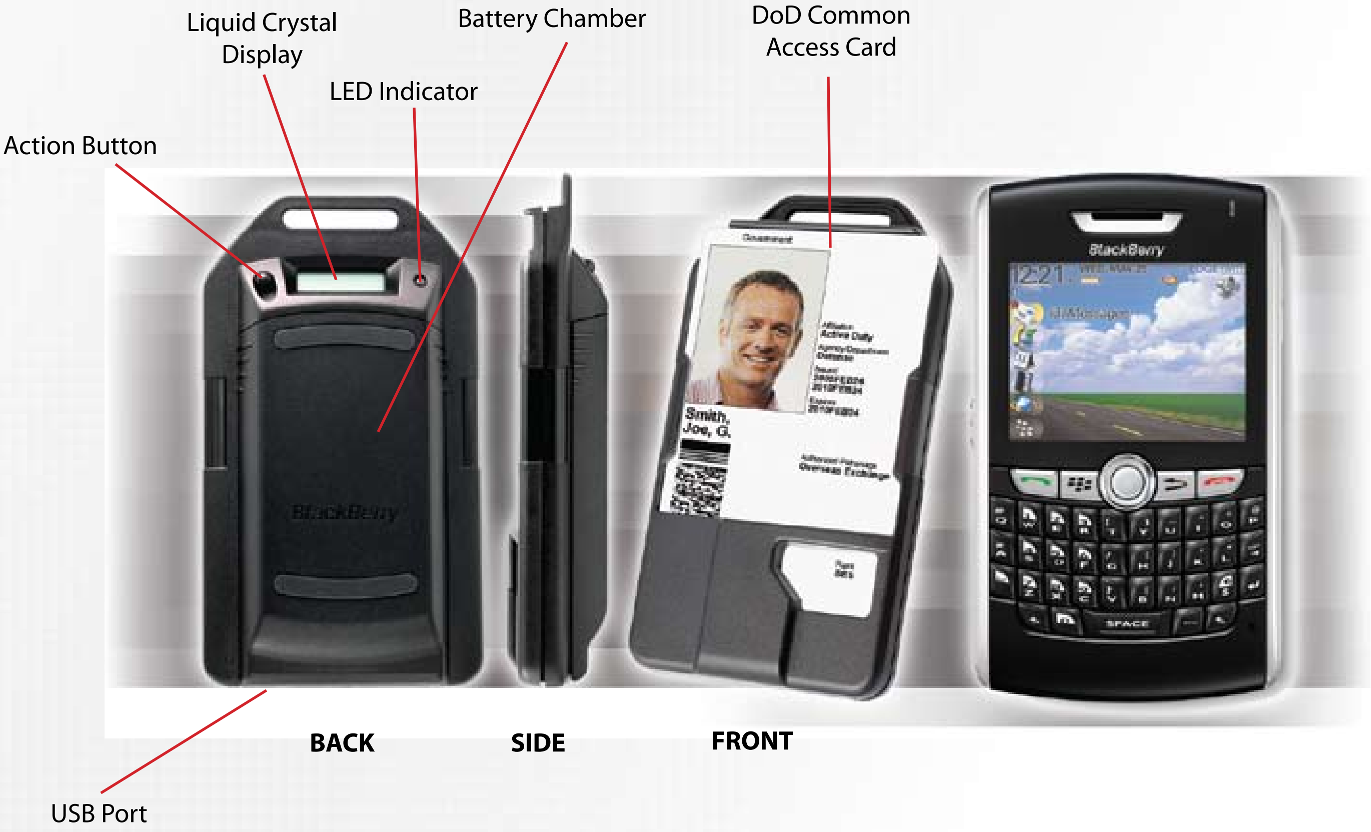
Activities Underway

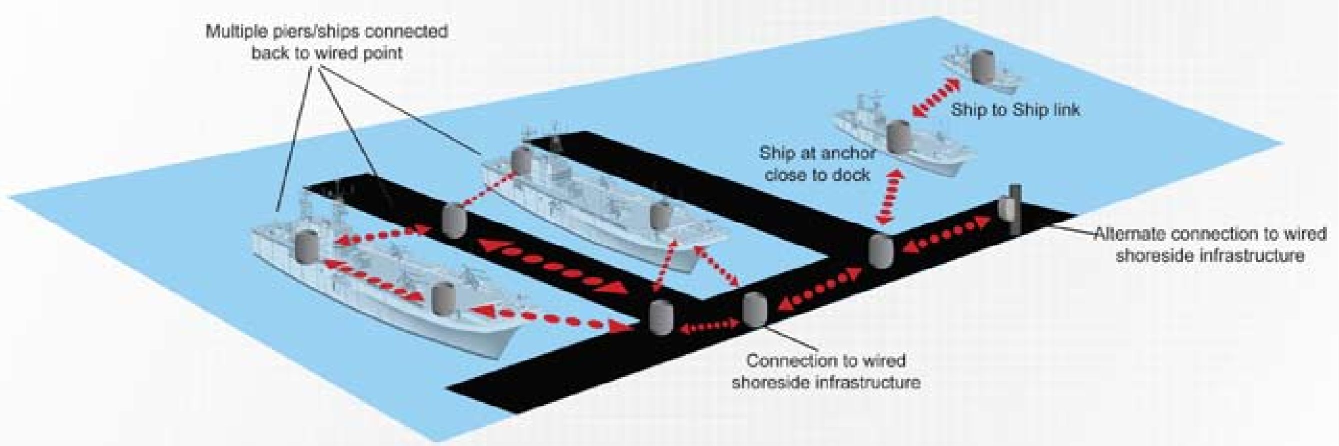
WPAN – Wireless Common Access Card (CAC) Reader for BlackBerry

Like many organizations, the DON utilizes *smart phones*, in this case RIM BlackBerrys, combining mobile voice and data access to DON email services. However, these smart phones or personal electronic devices (PED) must be able to interface with the public key infrastructure (PKI) certificates stored on a user's DoD Common Access Card (CAC) through a Designated Accrediting Authority (DAA) approved device and/or connection - either a physical connection or a secured Bluetooth communications link configured in accordance with DoD and DON wireless security standards.

Integrating network security principles into enterprise mobility, the Department is deploying a BlackBerry Bluetooth CAC reader solution that enables NMCI users to send and receive digitally signed, encrypted, and decrypted email messages on BlackBerry devices using DoD-issued PKI certificates on their CAC. With a 10 foot range, the user can carry the CAC reader, providing CAC-based security without interfering with normal use of the Blackberry device itself.

Additional devices will be evaluated as security implementations mature.




Multiple piers/ships connected back to wired point
Ship to Ship link
Ship at anchor close to dock
Alternate connection to wired shoreside infrastructure
Connection to wired shoreside infrastructure

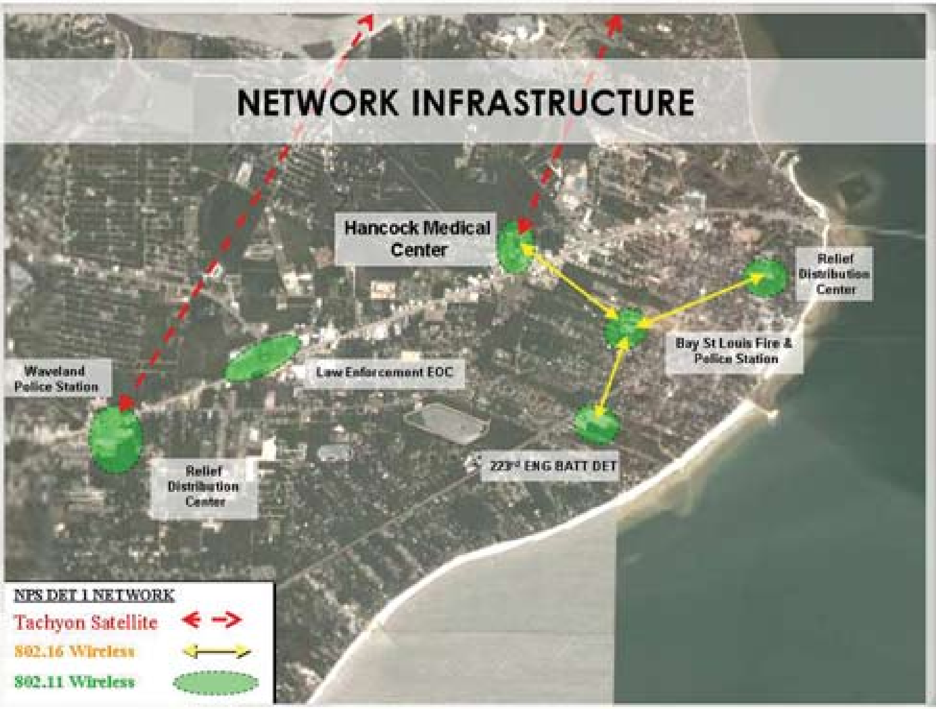
WLAN- Wireless Piers Connectivity System (WPCS)

Traditionally, when a ship was in port, numerous cables were run to provide connectivity to the shore network to support ongoing work aboard the ship. Particularly at larger ports where many ships could be docked for varying lengths of time, this was an arduous task for the network managers and complicated their ability to effectively manage the network.

Among the alternatives being examined to address this issue is WPCS. The WPCS uses a standard WiFi solution to provide wireless connectivity. Ships close to shore may also take advantage of this connectivity as well as create a ship-to-ship connection. The end result is that WPCS provides an enhanced level of connectivity with less labor and complications for the shore IT staff. In 2005 a new WPCS platform was successfully implemented within days to provide connectivity for three frigates that were temporarily berthed at Naval Air Station (NAS) Pensacola after Hurricane Katrina destroyed their docks at NAS Pascagoula, MS.

AIT – USMC in Iraq

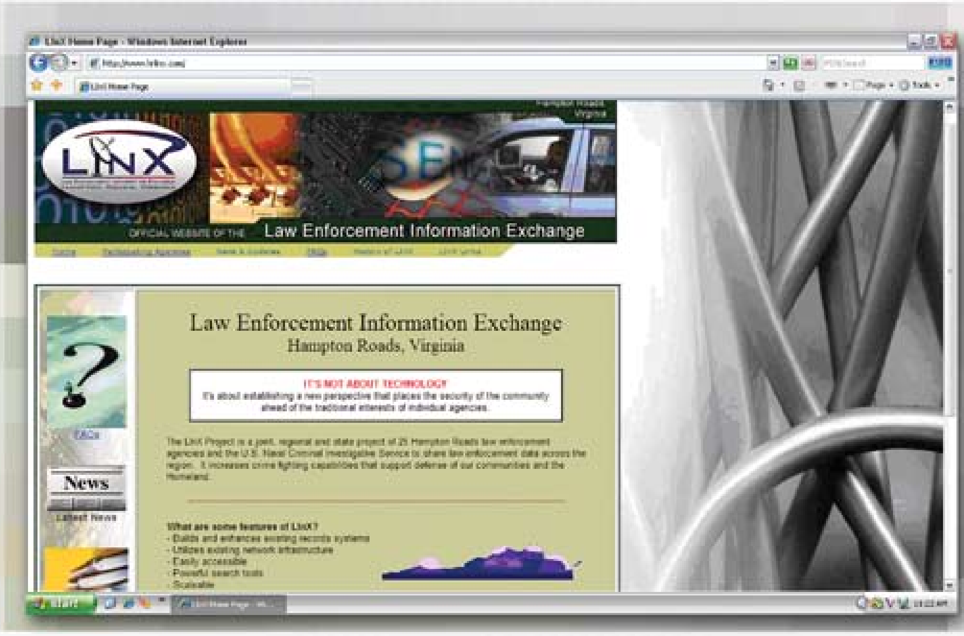
The Marines implemented a WiFi-based wireless LAN in Iraq to manage the receipt and assignment of every critical support item from boots to bombs. The system consisted of some 2,000 components including access points, handheld bar code scanners, and servers. The scanners interpreted the bar codes and automatically entered the information into the inventory database via a wireless link. The system allowed the Marines to dramatically reduce inventory errors introduced by manual data entry and delivered enhanced control and visibility into the logistics chain. The solution is entirely portable and can be easily moved and set up in a new location as requirements dictate.



WMAN – Disaster Assistance

When Hurricane Katrina hit the Mississippi shore in 2005, it brought about significant damage to the commercial and private telecommunications infrastructure. The lack of data connectivity hampered efforts by federal, state, and local officials to effectively coordinate relief and recovery efforts.

As illustrated in the above figure, Navy engineers quickly erected a hybrid terrestrial and satellite wireless network, connecting local law enforcement, fire departments, the relief center, and the main medical center. This network facilitated relief efforts and enhanced and streamlined communications.



Law Enforcement Information Exchange
Hampton Roads, Virginia

IT'S NOT ABOUT TECHNOLOGY
It's about establishing a new perspective that places the security of the community ahead of the traditional interests of individual agencies.

The LInX Project is a joint, regional and state project of 25 Hampton Roads law enforcement agencies and the U.S. Naval Criminal Investigative Service to share law enforcement data across the region. It increases crime fighting capabilities that support defense of our communities and the Homeland.

What are some features of LInX?
- Builds and enhances existing records systems
- Utilizes existing network infrastructure
- Easily accessible
- Powerful search tools
- Scalable

WWAN – Law Enforcement Information Exchange (LInX)

The Naval Criminal Investigative Service (NCIS) is the DON's primary law enforcement agency responsible for, among other things, investigating major crimes committed on Department property or by Department personnel. As the DON's larger locations are often adjacent to, or in the vicinity of, multiple local jurisdictions, critical information regarding incidents and suspects often ends up in multiple stove-piped systems, providing a barrier to successfully investigating and solving crimes.

To eliminate this barrier NCIS created partnerships with state and local law enforcement agencies in key DON locations. Each participant contributes data to a shared data warehouse that is accessible to each agency. The LInX application is accessible via laptop computers in most local law enforcement agency cruisers via commercial services such as EDGE or EVDO. LInX systems are currently operational in Hawaii; Puget Sound, WA; the gulf coast of Texas; northeast Florida/southeast Georgia; and Hampton Roads, VA. The LInX system homepage for Hampton Roads, VA is shown above. Additional systems are being developed in New Mexico and the National Capital Region. Over 200 agencies currently participate in the LInX project.

Voice

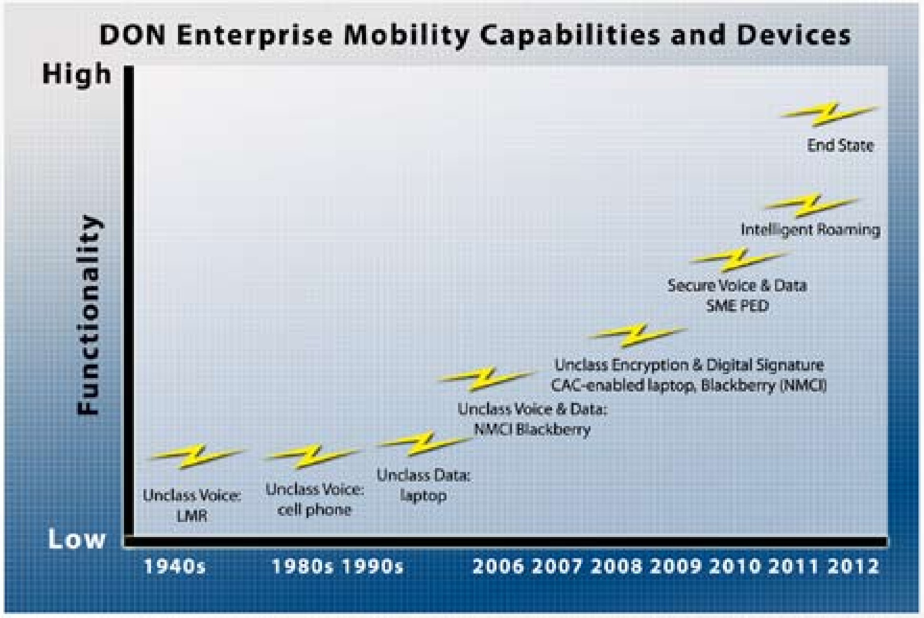
Integrated Voice Communications Network (IVCN). Onboard voice communications on a ship support vital operations such as flight deck, damage control, safety, and security operations, as well as non-vital operations, such as routine maintenance work on ship systems. Traditionally, these services were supplied by wired systems with little flexibility in adding coverage where it might be needed or by analog land mobile radios or PCS cellular systems. A number of successful trials have been conducted recently that implement wireless voice solutions utilizing 802.11 WLAN technology, which dramatically improve the IVCN environment. The goal of these ongoing efforts is to develop a converged vital/non-vital wireless IVCN environment for all shipboard communications that leverages COTS IP-based solutions.

Enterprise Land Mobile Radio (ELMR)

ELMR is a Navy and Marine Corps solution that will replace the entire inventory of LMR devices with new radios capable of operating in a digitized, trunking manner with support for VoIP. ELMR will provide the DON with enhanced communications capabilities with state and local first responders as it employs COTS devices that adhere to the Association of Public Safety Communications Officials Project 25 (APCO P25) interoperability standard. ELMR is currently in the process of being implemented with completion targeted for 2008.

Moving Forward

The dramatic impact of technology convergence and wireless advances is witnessed in the rapid growth of available capabilities to the mobile user and the speed with which they are delivered. As seen in the chart below, early capabilities in enterprise mobility grew slowly over time. Land mobile radios, for example, remained much the same for decades in the capability they delivered, as did, to a lesser extent, cell phones. However, more recently, with the introduction of software defined radios and the emergence of multi-function cellular devices, significantly new or enhanced capabilities are being delivered on an annual basis.



It is expected that this trend will continue over the next few years (if not longer) until the targeted end state is achieved. This dynamic environment presents great opportunities to quickly improve the DON's enterprise mobility with new capabilities in the next years. However, it also presents DON IM/IT leadership with a management challenge in identifying and developing the technologies and solutions that will best forward the strategic goals of the DON and deliver direct warfighter advantages.

The activities of the DWWG as described herein will help DON leadership meet that challenge by:

- Moving successful trials to fielded, enterprise capabilities;
- Integrating emerging technologies quickly, yet deliberately;
- Ensuring DON requirements are considered as future specifications are defined; and
- Maintaining a responsive wireless policy environment.

From Trials to Enterprise

The primary objective of the DWWG is to facilitate the introduction of proven solutions throughout the Enterprise wherever they can provide value. Pilot implementations and trials, that demonstrate value to the Enterprise, need to be fielded as quickly as possible to obtain maximum benefits. The DWWG's clearinghouse function allows full visibility throughout the DON so that all entities that could benefit from a solution may do so at an accelerated rate.

Trident Warrior (TW) exercises are a primary example of the value of trials in developing new capabilities. A past TW exercise proved the utility of a WiFi-based solution supporting Expanded Maritime Interdiction Operations (EMIO), which is now operational. The solution connects the boarding party on the interdicted vessel with the host Navy ship. Through the wireless link, biometric data from the interdicted crew is relayed back to the host Navy ship for identification of potential threats. TW 2008 will further develop this capability by providing access to a more extensive range of networks to better support Maritime Domain Awareness.

- To support accelerating trials to fielded solutions, the DWWG will canvass DON components to identify technology development, commercialization, and resource opportunities.

Emerging Technologies

The suite of commercial wireless technologies currently available will change. The industry is highly competitive and offerings will continue to leapfrog each other in available bandwidth and coverage. For example, some vendors have already announced their migration paths to enhanced versions of the current EVDO and HSDPA technologies to provide expanded data capabilities.

- A key emerging technology that provides increased Information Assurance is the 802.11i WLAN standard. DoD has identified this WiFi version as a critical requirement for future WLAN implementations. This must be integrated as quickly as possible throughout the DON's WLAN environment, but with assurances that the introduction of this new wireless solution does not compromise any network's security or performance.

The Secure Mobile Environment – Portable Electronic Device (SME-PED) represents another new and advanced capability on the horizon. A National Security Agency-sponsored development effort, the SME-PED device is the handheld portion of a system that will allow mobile users access to classified email, unclassified email, clear voice calls (via circuit switched data networks), as well as clear and secure web browsing. The converged device is able to provide both classified and unclassified operation through the use of what is called red/black separation. With introduction into the DON environment targeted for 2008, the SME-PED offers the opportunity to dramatically enhance enterprise mobility.

As a SIPRnet device, the SME-PED must be implemented through a deliberate process. In conjunction with Navy and Marine Corps leadership, DON CIO will leverage the DON Wireless Working Group to support SME-PED policy and planning.

Future Technologies

The specifications and characteristics of existing and emerging technologies are known and therefore must be accepted as-is by the DON. However, for future technologies the DON has an opportunity to influence the specifications as they are being developed by standards-setting organizations. The DWWG accomplishes this by engaging these organizations on an ongoing basis through meetings and forwarding the Department's viewpoint as appropriate.

One such technology is the 802.16m implementation of WiMAX. This implementation is envisioned to deliver significant enhancements, including increased throughput to 100 Mb for mobile users and 1GB for users that are stationary or moving on foot, an increase in coverage to a 500 km (310 miles) cell size, mobility speeds of up to 350 kmh (217 mph), and enhanced security and battery life. These advances clearly show potential to be highly beneficial to the DON mission. By being involved in the early stages of development, the DON significantly improves the chances of having its requirements addressed in the ultimate standard definition, targeted to be completed by the end of 2009. A related, though less mature, initiative is underway to define an 802.20 variant of WiMAX.

- To support this effort the DWWG, in concert with DoD, will continue providing input to the standards body developing the specifications for the 802.16m and 802.20 WiMAX implementations.

Maintaining a Responsive Policy Environment

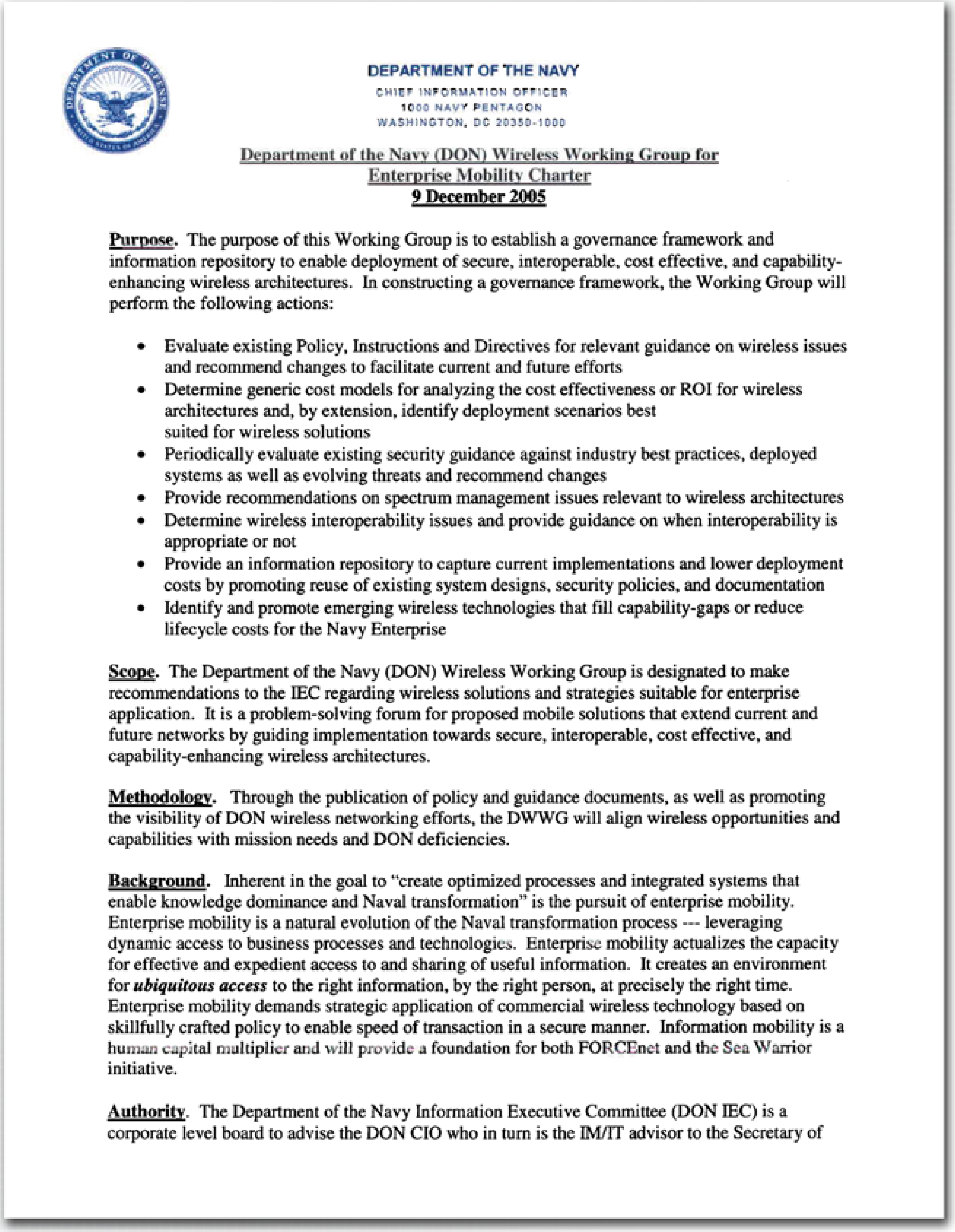
In the midst of quickly changing technological advances, the policy environment must be agile and responsive to the realities of the capabilities and risks of new solutions. The DWWG will not only develop recommended Secretary of the Navy instructions but will also develop interim DON CIO policy memoranda and other guidance as appropriate. The DWWG will work closely with the DoD Commercial Wireless Working Group and other entities to assist in the development of DoD-wide policies.

- To support this work, the DWWG will develop policy and guidance in concert with DoD to ensure the proper integration of solutions into the classified and non-classified environments.

Summary

Enterprise Mobility describes the ability to expand access to information wherever the warfighters are located, regardless of the existence of a wired infrastructure. Commercially available wireless technologies will be used increasingly to provide that access and the last link in the net-centric environment. As these technologies have potential vulnerabilities in addition to their advantages, they must be introduced in an orderly, planned manner. The DON CIO coordinates the Department's efforts in this area and facilitates the advancement of commercially available wireless technologies.

Appendix A: DWWG Enterprise Mobility Charter



DEPARTMENT OF THE NAVY
CHIEF INFORMATION OFFICER
1000 NAVY PENTAGON
WASHINGTON, DC 20350-1000

Department of the Navy (DON) Wireless Working Group for Enterprise Mobility Charter

9 December 2005

Purpose. The purpose of this Working Group is to establish a governance framework and information repository to enable deployment of secure, interoperable, cost effective, and capability-enhancing wireless architectures. In constructing a governance framework, the Working Group will perform the following actions:

- Evaluate existing Policy, Instructions and Directives for relevant guidance on wireless issues and recommend changes to facilitate current and future efforts
- Determine generic cost models for analyzing the cost effectiveness or ROI for wireless architectures and, by extension, identify deployment scenarios best suited for wireless solutions
- Periodically evaluate existing security guidance against industry best practices, deployed systems as well as evolving threats and recommend changes
- Provide recommendations on spectrum management issues relevant to wireless architectures
- Determine wireless interoperability issues and provide guidance on when interoperability is appropriate or not
- Provide an information repository to capture current implementations and lower deployment costs by promoting reuse of existing system designs, security policies, and documentation
- Identify and promote emerging wireless technologies that fill capability-gaps or reduce lifecycle costs for the Navy Enterprise

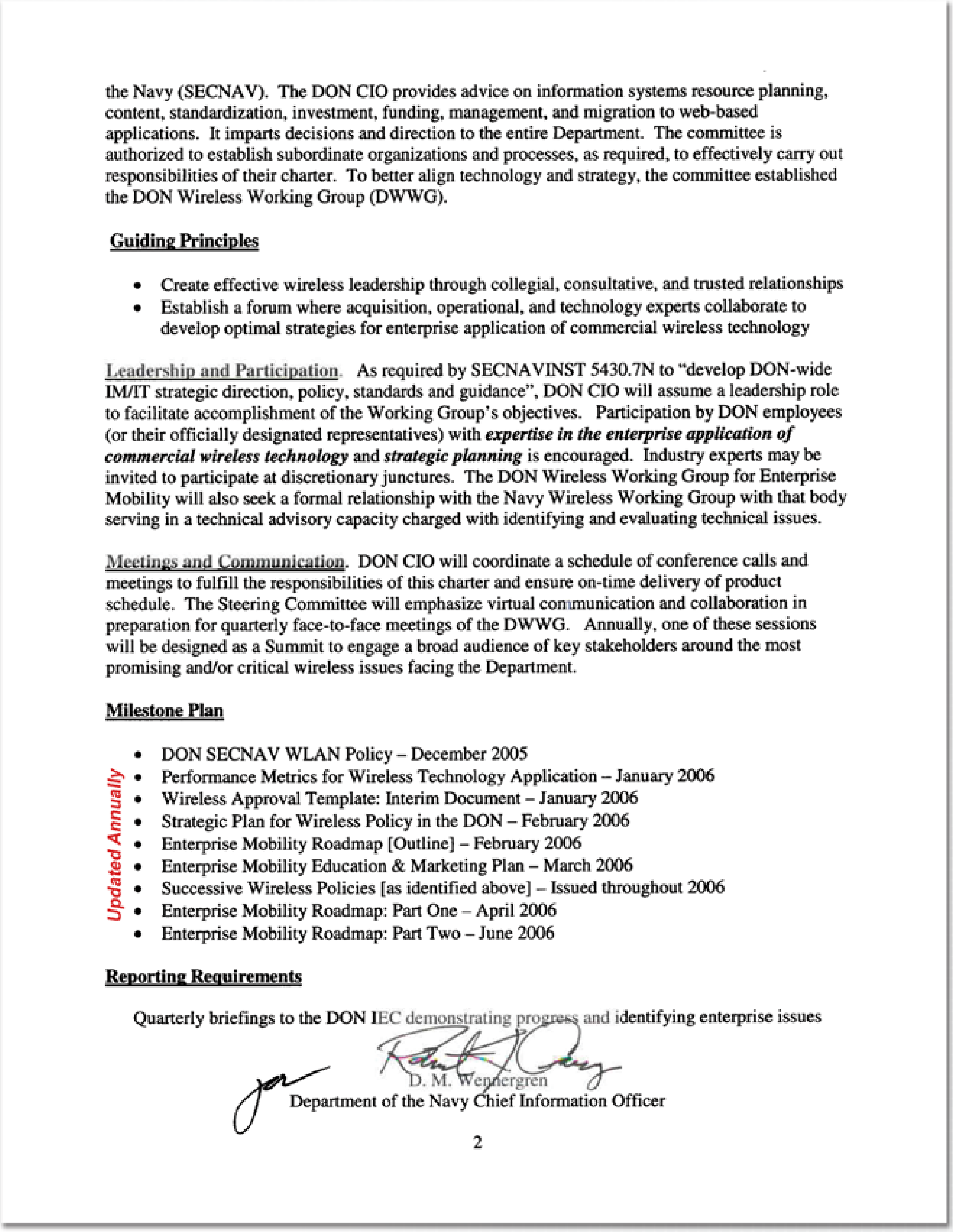
Scope. The Department of the Navy (DON) Wireless Working Group is designated to make recommendations to the IEC regarding wireless solutions and strategies suitable for enterprise application. It is a problem-solving forum for proposed mobile solutions that extend current and future networks by guiding implementation towards secure, interoperable, cost effective, and capability-enhancing wireless architectures.

Methodology. Through the publication of policy and guidance documents, as well as promoting the visibility of DON wireless networking efforts, the DWWG will align wireless opportunities and capabilities with mission needs and DON deficiencies.

Background. Inherent in the goal to "create optimized processes and integrated systems that enable knowledge dominance and Naval transformation" is the pursuit of enterprise mobility. Enterprise mobility is a natural evolution of the Naval transformation process --- leveraging dynamic access to business processes and technologies. Enterprise mobility actualizes the capacity for effective and expedient access to and sharing of useful information. It creates an environment for ***ubiquitous access*** to the right information, by the right person, at precisely the right time. Enterprise mobility demands strategic application of commercial wireless technology based on skillfully crafted policy to enable speed of transaction in a secure manner. Information mobility is a human capital multiplier and will provide a foundation for both FORCEnet and the Sea Warrior initiative.

Authority. The Department of the Navy Information Executive Committee (DON IEC) is a corporate level board to advise the DON CIO who in turn is the IM/IT advisor to the Secretary of

Appendix A: (Cont.)



the Navy (SECNAV). The DON CIO provides advice on information systems resource planning, content, standardization, investment, funding, management, and migration to web-based applications. It imparts decisions and direction to the entire Department. The committee is authorized to establish subordinate organizations and processes, as required, to effectively carry out responsibilities of their charter. To better align technology and strategy, the committee established the DON Wireless Working Group (DWWG).

Guiding Principles

- Create effective wireless leadership through collegial, consultative, and trusted relationships
- Establish a forum where acquisition, operational, and technology experts collaborate to develop optimal strategies for enterprise application of commercial wireless technology

Leadership and Participation. As required by SECNAVINST 5430.7N to "develop DON-wide IM/IT strategic direction, policy, standards and guidance", DON CIO will assume a leadership role to facilitate accomplishment of the Working Group's objectives. Participation by DON employees (or their officially designated representatives) with ***expertise in the enterprise application of commercial wireless technology*** and ***strategic planning*** is encouraged. Industry experts may be invited to participate at discretionary junctures. The DON Wireless Working Group for Enterprise Mobility will also seek a formal relationship with the Navy Wireless Working Group with that body serving in a technical advisory capacity charged with identifying and evaluating technical issues.

Meetings and Communication. DON CIO will coordinate a schedule of conference calls and meetings to fulfill the responsibilities of this charter and ensure on-time delivery of product schedule. The Steering Committee will emphasize virtual communication and collaboration in preparation for quarterly face-to-face meetings of the DWWG. Annually, one of these sessions will be designed as a Summit to engage a broad audience of key stakeholders around the most promising and/or critical wireless issues facing the Department.

Milestone Plan

Updated Annually

- DON SECNAV WLAN Policy – December 2005
- Performance Metrics for Wireless Technology Application – January 2006
- Wireless Approval Template: Interim Document – January 2006
- Strategic Plan for Wireless Policy in the DON – February 2006
- Enterprise Mobility Roadmap [Outline] – February 2006
- Enterprise Mobility Education & Marketing Plan – March 2006
- Successive Wireless Policies [as identified above] – Issued throughout 2006
- Enterprise Mobility Roadmap: Part One – April 2006
- Enterprise Mobility Roadmap: Part Two – June 2006

Reporting Requirements

Quarterly briefings to the DON IEC demonstrating progress and identifying enterprise issues

D. M. Wennergren
Department of the Navy Chief Information Officer

Appendix B: Resources

Bluetooth Special Interest Group	**https://www.bluetooth.org/**
DoD Logistics AIT Office	**http://www.dla.mil/j-6/AIT/**
DON AIT Program	**http://www.nko.navy.mil**
DON CIO	**http://www.doncio.navy.mil**
IEEE	**http://www.ieee.org**
Near Field Communications Forum	**http://www.nfc-forum.org/home**
WiFi Alliance	**http://www.wifialliance.com/**
WiMAX Forum	**http://www.wimaxforum.org/home**
ZigBee Alliance	**http://www.zigbee.org**

DISA
JFCOM
HQMC
NG
SWNWG
DWWG
USMC NWWG
Policy
Shipboard
USMC
RFID
BAR CODES
Requirements

Bringing Enterprise Mobility to the Warfighter

The following groups work collaboratively to implement the visions and capabilities described in this document:

Carrier Network Working Group

Charleston Communications Working Group

CANES Voice Community of Interest

DoD Commercial Wireless Working Group

DON Wireless Working Group

Electronic Special Weapons Ordnance Working Group

Federal Partnership for Interoperable Communications

Joint Wireless Working Group

Joint Forces Wireless Working Group

Naval Expeditionary Overwatch Communications Working Group

National Institute of Standards and Technology

National Security Agency

Navy Automated Identification Technology Office

NETWARCOM Wireless Working Group

Shipboard Wireless Networks Working Group

SPAWAR Wireless Working Group

Tactical/Non-Tactical Radio IPT

Marine Corps Wireless Working Group

Voice Migration to IP Working Group

Wireless Discovery Working Group

DEPARTMENT OF THE NAVY

DEPARTMENT OF THE NAVY
CHIEF INFORMATION OFFICER

1000 NAVY PENTAGON
WASHINGTON, DC 20350 - 1000

WWW.DONCIO.NAVY.MIL

APRIL 2008