STATEMENT BY

VICE ADMIRAL TED N. BRANCH
DEPUTY CHIEF OF NAVAL OPERATIONS
FOR INFORMATION DOMINANCE (N2/N6),
DEPUTY DEPARTMENT OF THE NAVY (DON)
CHIEF INFORMATION OFFICER - NAVY,
DIRECTOR OF NAVAL INTELLIGENCE,
AND HEAD OF THE NAVY'S INFORMATION DOMINANCE CORPS

BEFORE THE

HOUSE ARMED SERVICES COMMITTEE

SUBCOMMITTEE ON

EMERGING THREATS & CAPABILITIES

ON

"Information Technology Investments and Programs: Supporting Current Operations and Planning for the Future Threat Environment"

FEBRUARY 25, 2015

Introduction

Good afternoon Mr. Chairman and distinguished Members of the Subcommittee. Thank you for this opportunity to provide written testimony for the record to the Subcommittee on information technology (IT) modernization and policy. I would also like to thank Dr. John Zangardi, the Department of the Navy's (DON) acting Chief Information Officer (CIO) and Deputy Assistant Secretary of the Navy for Command, Control, Communications, Intelligence and Space (DASN C4I & Space) for his testimony. My intent is to provide remarks complementary to his testimony.

I am Vice Admiral Ted Branch, Deputy Chief of Naval Operations for Information Dominance (N2/N6), Deputy DONCIO - Navy, Director of Naval Intelligence, and Head of the Navy's Information Dominance Corps. For this testimony and Subcommittee's interest, my written comments focus largely on my role as the Navy service's CIO. Like the Marine Corps, we have a uniformed service CIO below the Secretariat (DONCIO) level.

Before going too much further, it occurs to me that you may not be familiar with the term Information Dominance. We define Information Dominance as the operational advantage gained from fully integrating the Navy's information functions, capabilities and resources to optimize decision making and maximize warfighting effects.

In other words, it is about warfighting in the Information Age.

To accomplish our goals, we focus on three core capabilities: Assuring Command and Control, maintaining persistent Battlespace Awareness, and Integrating kinetic (missiles, warheads, etc.) and non-kinetic (cyber, electromagnetic spectrum) Fires.

With that as the basis for what we do, I will discuss five specific areas: The challenges that are inherently unique to the Navy; the Navy's roadmap to Risk Management Framework (RMF) implementation; our support to the Joint Information Environment (JIE), the Joint Regional Security Stack (JRSS) architecture, and Intelligence Community Information Technology Enterprise (IC ITE) efforts; Navy's role in information-age warfare; and our efforts in the cyber "fight for talent".

Navy Unique Challenges

So…what makes Navy unique? As many of you are aware, one-third of the Navy's Battle Force is operating at sea on any given day. This means that large portions of our tactical

afloat, OCONUS, and warfighting system networks are distributed on the front lines. Sustaining our global primacy requires that we dominate the battle space on, above, and below the surface of the sea, as well as in outer space. In this Information Age, we recognize and accept the premise that we must also successfully command, control, and fight our forces in the information domain, which includes the electromagnetic spectrum and cyberspace. This requires frequent and timely updates to our systems.

In this dynamic information dominance realm, operating in a benign afloat environment is challenging enough. In a communications denied or degraded environment, the complexity of fighting increases as does the difficulty of effectively maintaining command and control of our forces. With a large part of the Fleet operating forward, maintenance and modernization of our Command, Control, Communications, and Computer (C4) and cyber systems on the tactical edge is difficult. System configuration changes, security updates and patches must often be delayed until that unit is back in homeport for scheduled maintenance. As we try to pace the threat and technological advances, maintaining a highly capable Battle Force consisting of different high-optempo ship classes, variations among programs of record, and differing configurations is at best challenging. Additionally, with limited bandwidth available to our operating forces at sea and our focus on safely operating and fighting the ship, our quality of life initiatives – telephones, email, Facebook etc., – often take a backseat, impacting morale for both our Sailors at sea and their loved ones at home. Our Commanders must balance these priorities every day.

Risk Management Framework

The Navy is moving out with implementation of the Risk Management Framework (RMF). Phase I of implementation began 1 January 2015 and is in accordance with DoD CIO stated timelines for DoD implementation. Phase I includes all Navy IT assets currently accredited under the DoD Information Assurance Certification and Accreditation Process (DIACAP). Phase I will also utilize the current Operational Designated Accrediting Authority (ODAA) acting as the single Authorizing Official (AO) and the current Certifying Authority (CA) acting as the single Security Control Assessor (SCA). Phase II, which is still under development and will begin on or about July 2016, will incorporate all Platform IT (PIT): i.e, Weapons Systems; Industrial Control Systems (ICS); and Hull, Mechanical, and Electrical (HM&E) that were not covered under the previous Cybersecurity Accreditation policy. Both

Phase I and Phase II will be completed by October 2017, leaving Navy 100% complete with our implementation.

JIE, JRSS and IC ITE Efforts

The Navy is fully onboard with DoD's effort to consolidate individual service, component, and agency IT infrastructures into the Joint Information Environment (JIE). This is largely a shore-based infrastructure, and Navy's responsibility extends to the tactical edge at sea. JIE capabilities will be provided to all authorized Navy personnel afloat, ashore, and aloft by means of the following: (1) the Next Generation Enterprise Network (NGEN)/OCONUS Navy Enterprise Network (ONE-NET) and Navy Enterprise Data Center Consolidation ashore; and (2) the Consolidated Afloat Networks and Enterprise Services (CANES) network, Automated Digital Network System (ADNS) Increment III router, Navy Multiband Terminal (NMT) transceiver, and such hosted and connected applications as the Global Command and Control System Maritime (GCCS-M) and Distributed Common Ground System Navy (DCGS-N) Increment II at the tactical edge at sea.

The Joint Regional Security Stack (JRSS) is a key JIE capability being delivered over FY16 and FY17 as part of the Single Security Architecture that will enable improved command and control of the DoD Information Network (DoDIN), improved cyber security and enhanced network operations. The Navy has shaped the evolution of JRSS to incorporate additional security capabilities that are currently being used in the Navy's security stacks today. We will transition to JRSS in FY18.

The Navy also fully supports the Director of National Intelligence and the Intelligence Community's (IC) effort to enable greater integration, information sharing, and security through an enterprise approach called the IC Information Technology Enterprise (IC ITE). Much as in the case of the UNCLASSIFIED- and SECRET-level JIE, the Top Secret/Special Compartmented Information (SCI)-level IC ITE is largely a shore-based infrastructure, and Navy's responsibility extends to the tactical edge at sea. IC ITE capabilities will be provided to all authorized Navy personnel afloat, ashore, and aloft by means of the following: (1) the Office of Naval Intelligence (ONI) SCI IT, Joint Deployable Intelligence Support Systems (JDISS), Global Command and Control System Integrated Imagery and Intelligence (GCCS-I3), and designated General Defense Intelligence Program (GDIP) elements ashore; and (2) the CANES

network, ADNS Increment III router, NMT transceiver, and such hosted and connected applications as the Ship's Signals Exploitation Equipment (SSEE) Increment F and DCGS-N Increment II at the tactical edge at sea.

Navy's transition planning for both JIE and IC ITE includes rationalizations of current data/applications, desktops, networks/domains, and cloud services to identify possible onramps to respective JIE and IC ITE services. That planning focuses heavily on the requirement to ensure such enterprise services – cloud-enabled and otherwise – operate with maximum effect around the clock at the tactical edge, in our case, at sea. As stated earlier, we will satisfy that fundamental requirement through our programmed modernization efforts that leverage not only CANES, ADNS Increment III, NMT, GCCS-M, DCGS-N Increment II, and SSEE Increment F but such other important Navy Programs of Record (PoR) as the Integrated Security Services Program (ISSP) and Tactical Switching (TsW). While so doing, we will be aggressive in leveraging any and all gains made by the JIE and IC ITE architects as they partner to set conditions for improved integration and interoperability across collaboration, identity management, information sharing, visualization, data access and other key touch points for national to tactical warfighting synergy.

Information-Age Warfare

The digital revolution has forever changed the very nature of warfare, and the cyber domain is now as important as getting underway, launching a Tomahawk or landing an aircraft – it is "Commander's Business." This change offers both challenges and opportunities. We now have non-kinetic warfare options that can be combined with kinetic options to fill-out the Warfighting Commander's quiver. Bits and bauds have the potential to disrupt adversary command and control nodes with similar effects to the 500-pound bombs we relied on in past conflicts and continue to rely on today. Our networks are now weapons systems and must be protected accordingly.

In response to the maturing nature of information-age warfare, six years ago, in 2009, we brought together the Oceanographic and Meteorological, Information Warfare, Information Professional, Intelligence, and Space Cadre officer communities – together with their enlisted, reserve, and civilian counterparts – to establish a professional and technically diverse warfighting corps on par with our surface, submarine, and aviation counterparts. The members of

this Information Dominance Corps are not the only Sailors executing Information Dominance as a warfare discipline, but they are its principal practitioners, and they bring extremely valuable skills and specialized knowledge to the fight. Moreover, they are taking on leadership roles at the highest levels, as exemplified most recently by Admiral Mike Rogers' confirmation as Commander, U.S. Cyber Command, and Director, National Security Agency/Central Security Service; as well as Vice Admiral Jan Tighe's command of Fleet Cyber Command/U.S. 10th Fleet.

Recent real world events and attacks on our networks and systems make clear that the cyber threat is increasing, Most of our networks were neither designed, procured nor maintained to be weapons systems or protected against sophisticated adversaries in this new warfare area. To address this issue, we continue to execute Task Force Cyber Awakening (TFCA), a year-long initiative established in August 2014 to (1) continue to track and oversee the execution of our defense-in-depth cyber approach in response to adversary activity on our networks, (2) gain a holistic view of cyber security risk across the Navy, (3) deliver fundamental change to the Navy's organization, resourcing, acquisition and readiness, and (4) align and strengthen authority and accountability in cyber security. We find ourselves in the position where we must modernize our older systems to mitigate vulnerabilities and limit the potential consequences that could disrupt our operations. At the same time, we must lay the foundation for the future, putting in place capabilities like Cyber Situational Awareness, which will give us the ability to monitor and detect cyber threats. We are also designing-in resiliency in current and new programs by generating common standards and protocols that will be used as guiding principles during procurement, configuration and implementation. Combined, these actions will improve our cyber posture, reduce the number of disparate systems in the Fleet, and increase the resiliency of those systems while providing the capabilities that the Battle Force of tomorrow will require.

Fight for Talent

I share the concerns of many of my colleagues in regards to the fight for talented people. Our business is becoming ever-more technical, complicating Navy's requirement to access, train and retain our Nation's best and brightest. Navy must compete not only against our sister services for this unique talent pool, but also against the corporate IT giants…whose pay and compensation packages can be more lucrative and workplace environments less severe.

Considering the exponential rate of change in technology and its corresponding impact on both our own and our adversaries' capabilities, the unique talents and abilities within the Information Dominance Corps are increasingly critical. With that in mind, we are in the process of reviewing and revising our Information Dominance Corps accession, training and education, and detailing processes so that we can recruit and retain the skilled and talented experts and leaders needed to meet the increasing demand signal from Warfighting Commanders and the Navy as a whole. We recognize that we must compete for that talent, and are looking to gain any possible advantage in that effort.

Conclusion

Warfare in the Information Age demands that the Navy, and our sister services must adapt and change. We in the Navy, through our recognition of this new warfare domain, our embrace of emerging technologies, our support for DoD and Intelligence Community modernization and efficiency efforts and, perhaps foremost, our creation of a dedicated Information Dominance Corps of information warriors demonstrate our resolve to excel in this area. We embrace our leadership role within the DoD on many of those fronts. We stand committed and ready to fight and win a potential conflict, on, above or below the sea, in space or in the information domain.

Thank you for your time and attention to these matters.