Navy Information Dominance Industry Day
Sponsored by AFCEA Intelligence and the Naval Intelligence Professionals
June 22, 2010
The Heritage Conference Center
Chantilly, VA

What follows are questions submitted during the conference by attendees and responses provided after the conference by the Navy N2N6 staff. The questions have been grouped by general topic for an easier review.

Topic: Overview

Q: What is your strategy to transition the defense acquisition establishment from a platform-centric mindset to an information dominance enterprise framework?

N2N6 implemented a multifaceted strategy for transitioning the acquisition establishment from platform-centric to an information dominance framework.

First, N2N6 has been developing several key "roadmaps", which provide guidance regarding concepts, architectures, networks, sensors, and manpower. These roadmaps are information-centric vice platform-centric guides.

Second, N2N6 has aligned organizationally so that end-to-end insight and accountability for Navy information requirements, investments, capability and force development are synchronized. Each of N2N6's Divisions, headed by a Flag Officer or Senior Executive, is focused on providing a focused set of capabilities, that when integrated, enables information dominance within the battlespace.

Third, internal processes are in place that identify warfighting gaps and their solutions, and then align investments within the planning, programming, budgeting, and execution (PPBE) process to provide those solutions to the fleet. N2N6 works closely with Combatant Commanders (COCOMs) to identify emerging capability requirements in the Fleet. These capabilities are prioritized and then resourced through the PPBE and Program Objective Memorandum (POM) processes, culminating in an annual Sponsor Program Proposal (SPP) submission to the Department of Defense.

N2N6's recently submitted POM-12 SPP focused on critical information dominance capabilities and was well received by the Chief of Naval Operations and Defense Department leadership.

Q: Would you elaborate on the roles of Cyber and Space in your planning?

Cyber: Cyberspace operations are and will become even more critical in our planning process. Everything from the budget to maritime operations will need to incorporate cyberspace operations. Hard budget decisions will need to be made to fund the development of cyberspace capabilities through all phases of cyberspace operations. Likewise, Navy planners will need to incorporate all phases of cyberspace operations into military plans to include the impact if cyberspace capabilities are unavailable.

Space: The Navy is critically dependent on space to conduct both our core and wartime/contingency missions. A wide array of national, joint and commercial satellites currently provides Navy commanders with essential worldwide support. Space capabilities are vital to our nation's maritime operations and are foundational to our ability to operate in a networked and dispersed manner. Our Maritime Strategy demands flexible, interoperable and secure global communications capability to support the command and control requirements of our highly mobile and geographically dispersed U.S. and Allied forces. Our satellite communications capabilities confer to our deployed forces a decisive advantage across the spectrum of military operations. However, the Navy's interest in space is not limited to communications. Intelligence, reconnaissance, surveillance, navigation, missile warning and meteorology/ oceanography each have significant space components. These seminal capabilities support our operations on a daily basis, and are therefore pervasive in all parts of Navy planning.

Q: If coalition partner information dominance is part of your global information dominance strategy, and CNO's comments suggest it is, who in your organization is the POC for this?

Our Coalition partners are an important part of the Information Dominance strategy being developed by the US. Our most trusted Allies are currently working in partnership with us in several areas to better equip our forces for the future of Cyber and Information Dominance.

Within OPNAV N2/N6 there is no single POC for coalition partner information dominance as information sharing is dependant on the classification level of the information: non-classified, SECRET, and above SECRET.

For non-classified information, we have a section of our Maritime Domain Awareness (MDA) Office specifically dealing with International Engagement and Outreach. Our Allied Coalition Interoperability Branch deals with Maritime C4 SECRET and below. Finally, there is an Intelligence Engagement Branch dealing with intelligence related topics in the above SECRET domain.

Together these three groups cover all aspects of information dominance and place us in a very good position for moving ahead in concert with our coalition partners.

Q: Why should Navy lead the information dominance effort? How are others reacting to your efforts?

The Chief of Naval Operations, recognizing information as a "Main Battery" of Naval Warfighting, took a number of measures in 2009 to align the Navy's organization to achieve the integration and innovation necessary for warfighting dominance across the full spectrum of operations to include the cyberspace and information domains. The first step was to bring together the resource sponsorship for all of our information-related capabilities into one entity that include intelligence, networks, electronic warfare, cyber, meteorology, oceanography, space and unmanned systems. The second step was to establish U.S. Fleet Cyber Command to be the Navy's fighting arm and service component to the U.S. Strategic Command.

Q: Your vision statement talks about moving from a platform centric approach to enterprise capabilities. What are you greatest barriers to success?

Right now the #1 problem is lack of time – we need to develop and mature vital synergies that start to deliver Information Dominance-based capabilities to our Commanders who face an ever-increasing number and complexity of threats. The #2 problem is lack of money. We already know that funds will be tight. We have to accept that we will not be able to fund all the good ideas that we develop with our stakeholders, and with our partners and supporters in the labs, in industry and in academia. The #3 problem is culture. Having an Information Dominance outlook requires doing things in different ways, and that means finding and training and nurturing a workforce that knows how to do the things that deliver Information Dominance. It will require a huge amount of attention and focus to create a self-generating workforce that "gets it" and "does it".

Q: What are the reactions from the IC and others who you will rely upon to be successful?

As we expand our outreach within Navy, to DoD, to the IC or to other potential stakeholders, we have been well received. We expect this to continue, because our focus is on developing solutions - in coordination with our stakeholders - to maximize synergies and break out of stovepipes. Several of the Roadmaps include action plans that explicitly chart what we must do to better leverage and collaborate with other Services and the IC. To date, the response from outside the Navy has been positive.

Q: How can the new N2N6 incentivize program managers to become cross program centric?

N2N6 is focused on delivering the right capability to the Fleet at the right time so that as a Navy, we maintain our information dominance worldwide. N2N6 conducts business consistent with Navy policy and in compliance with Federal Acquisition Regulations. N2N6 has aligned organizationally so that end-to-end insight and accountability for Navy information requirements, investments, capability and force development are synchronized. As a natural result of this, Program Offices must now satisfy material requirements that are integrated across a broad spectrum of end-users, including other programs.

Q: Where do allies fit in information dominance roadmaps?

We have shared our roadmap work with our allies, but thus far there has been no coordinated Roadmap work with them. In the future we envision such a partnership, one that we frankly must include in order to tap into their visions and capabilities. Note that the MDA Roadmap is predicated on close collaboration with allies. As other Roadmaps are delivered and refined, the role of allies and other mission partners will be integrated.

Q: You've talked about divesting stove-piped solutions in the Information Dominance Vision statement. What goes first?

N2N6 has aligned organizationally so that end-to-end insight and accountability for Navy information requirements, investments, capability and force development are synchronized. Each of N2N6's Divisions, headed by a Flag Officer or Senior Executive, is focused on providing a focused set of capabilities, that when integrated, enables information dominance within the battlespace.

Additionally, N2N6 has been developing several key "roadmaps", which provide guidance regarding concepts, architectures, networks, sensors, and manpower. These roadmaps are information-centric vice platform-centric guides. Systems and networks will updated, replaced, or removed as emerging technologies are matured and available within the framework laid out in the roadmaps.

Q: You're clearly re-engineering the Navy as you move away from the platform centric model. Where does the money come from to do this?

The money used to re-engineer the N2N6 comes from the savings generated by the efficiencies gained during the re-engineering process. As just one example, N2N6 has aligned organizationally so that end-to-end insight and accountability for Navy information requirements, investments, capability and force development are synchronized. In other words, as an organization, N2N6 is able to do more with less, allowing the savings, otherwise known as "the money to do this", to be reinvested.

Q: With the evolution of the global threat environment and the many challenges associated with it, how do you envision the Navy and its efforts evolving in the next several years to meet these challenges? What emerging technologies hold the most promise for enhancing your efforts going forward?

The Navy was, is, and will continue to be multi-mission oriented, with ships and sailors trained and deployed to meet a variety of assignments facing very unpredictable threats. With a focus on maximizing the amount and types of information available when and where needed, and by creating an Information Dominance Corps with the operational mindset and technical capabilities to push and capitalize on the leading edges of technology, we will provide the decision.

Q: If every platform senses and reports, and every sensor and processor is adaptively connected, dynamically tasked and every shooter can use this. What process will OPNAV develop to harmonize integrated aviation investment planning for platforms, sensors, networks across N2N6 and N8 based on OSD's 30 year aviation investment plan?

Clearly this will require a building block approach. Harmonizing integrated investment planning across ISR platforms, sensors, networks and the associated processing, exploitation and dissemination (PED) tools and systems in N2N6 is the current challenge being addressed in POM12 and POM13. Herein lays one of the principle advantages of assigning responsibility for all of these systems to the N2N6. However, as observed, this is a non-trivial task and will require careful planning and coordination. Through the coordination of multiple N2N6 roadmaps, the process of synchronizing platform, sensor, network and PED acquisition and execution is being addressed. Publication of these coordinated roadmaps will be a significant milestone in allowing other OPNAV directorates, including N8 to align with the way forward - or to identify areas of potential friction between investments.

Topic: Personnel

Q: How are you optimizing where you place people and systems to ensure processing and exploitation occurs at the best location?

Part of the DOTMLPF analysis of each Information Dominance Roadmap is to examine how best to meet personnel accession, development and placement/deployment to support processing and exploitation needs now and in the out years. The ISR Roadmap is one obvious area where this is vital; but multiple others (e.g., MDA, UxS, Cyber, Undersea Dominance) also face very dynamic personnel challenges.

Q: With Information Dominance increasing in importance, how are you changing the training necessary to train both enlisted and officer personnel?

A holistic review of training and education for the Information Dominance Corps is underway and we will roll-out our Education and Training Roadmap in the next few months. It is important to realize we are now looking at total force initiatives for education and training to address enlisted and officer requirements, both active and reserve, as well as the requirements for the civilian professionals in our work force. As part of this process, we remain committed to the foundational principle that all education and training will be driven by validated requirements for workforce competencies. We will train individuals for the special expertise needed in their ratings and we will also ensure all members of the IDC are trained to a common standard ensuring future interoperability. We will eliminate stove-piped approaches to training, for example, we are developing and will soon begin senior officer courses designed to bring our leaders up to date on the challenges that face the IDC. We are reviewing training efforts at all our learning centers to identify a common core of training for all members of the IDC. These changes will impact not only accession level training, but the training we provide at the junior and mid-career levels, as well.

Q: What is the Navy and for that matter the Services & DoD doing about training foreign language linguists who can decipher/understand info received by all these systems we're building?

Navy is in-step with a number of language initiatives launched by the Department of Defense and the Office of the Director of National Intelligence. As part of those efforts, we have begun the process of making a comprehensive assessment of our language capabilities resident in the total force. We are also assessing the language capacity currently existing in the Navy to meet both current operational requirements and future needs. This effort is the foundation for the actions we will take to more rigorously identify requirements and capabilities, allowing us to then invest in new language initiatives. We are currently leaning forward in this area, for example, the Navy's crypto-linguist community (Cryptologic Technician Interpretive (CTI)), has programmed for additional billets to support the growth in the Cyber Warfare community with the needs of future systems and requirements in mind. As the environment and mission requirements become clearer, Navy will further refine its acquisition and training programs to support them.

Exploitation of this material is a significant challenge across DoD and other agencies as well. Automated screening methods for collected material is certainly an area of interest, and is something we would welcome industry's assistance with. Language training is a daunting task, both in terms of investments in time for training, as well as cost to train. Included in costs are the security clearance investigations, an area that

limits our pool of potential linguists. Maintenance of language skills is also a challenge as this is a very perishable commodity. Last, we have to manage individual sailor career paths and offer growth in terms of leadership and non-language skills.

Q: The other Services have tried to deal with preserving expertise and specialties while addressing the broad needs in the information domain. What is the way ahead for Navy's specialty communities?

The Navy will continue to leverage each individual community within the IDC as specialists in their area of expertise. These core communities are the foundation of the IDC and we will recruit, access, promote, and retain personnel to meet the requirements of the Navy. We will cross detail our best and brightest senior officers to key Command and leadership positions across the Corps. Navy is committed to reinforcing the value of each individual community and specialty while at the same time furthering the development of the Corps.

Q: How can we better apply technology to equip and train the manpower base of Information Dominance?

In conjunction with industry partners, we will continue to invest in operational and classroom technologies to deepen each member's professional skills thus broadening the understanding of cross-Corps disciplines. For example, during the last three years Navy has been involved in a partnership to develop interactive instructional software that gauges a student's progress in specific content areas. As the student progresses, the content are adjusted to ensure new skills are mastered. Recent trials suggest learners using this system acquire skills at a faster rate than traditional instructor-led courses. We will continue to leverage the capabilities we have developed to offer instruction on-line. In the future, it is likely we will provide on-line capabilities for our sailors to earn and maintain their systems and IT certifications.

Topic: Decision Superiority, Fleet Battle Management & MDA

Q: How will you determine or measure success in achieving information dominance and maritime domain awareness? Are there any metrics you are looking at?

There are three major efforts that the OPNAV N2N6 Maritime Domain Awareness Office has developed to measure success: the 2009-2010 MDA Assessment, the 2010-2011 MDA Game Plan, and the MDA Roadmap. The 2009-2010 MDA Assessment, currently in staffing, looks backward at the successes of the Navy MDA office in 2009 and measures progress made against the 2010-2011 Game Plan. Accomplishing the major milestones outlined in the Game Plan act to inform development of the larger

Information Dominance MDA Roadmap effort which looks out through 2020 and supports achieving decision superiority.

Under the Game Plan, there are five lines of operation for Navy MDA: Architecture and Acquisition, Engagement and Outreach, Operationalize MDA, Policy and Concepts, and Science and Technology. Each line of operation is progressing since the inception of the Navy MDA office in December 2008.

The leads for the five lines of operation created metrics and measures of success for their lines of operation and identified the critical objectives/ milestones/events. Every objective under each line of operation has a set of tasks. Each task has a metric and an assessment of the progress toward meeting that metric. Metrics range from such things as completion and distribution of the MDA Concept to aligning gaps and technologies. There are over 50 metrics, and each is specific to the task.

N2N6 initiated a series of Roadmaps in 2010 and MDA's Roadmap plays a central role in the N2N6 strategic vision. The MDA Roadmap has certain goals:

Attain effective understanding of the global maritime domain that could impact US security, safety, economy, or environment.

Deliver awareness to significantly advance the commander's ability to make informed, timely, and accurate decisions in support of the full range of military operations and advance maritime cooperative security objectives.

Enable decision superiority by operationalizing MDA, energizing partnerships, and harnessing technology to build a 21st century collection, data sharing, and fusion environment.

Deliver the concept, process, and architectures to share information with international, non-governmental, interagency, industry, and other partners.

These goals are being measured through individual tasks that include accountability, timeframe for accomplishment, and gap assessment.

Between the 2010-2011 Game Plan and the MDA Roadmap, a series of discrete, measurable tasks have been outlined and defined. Accomplishing these tasks will allow Navy MDA to accomplish its goal of decision superiority.

Q: Information technology is driving dramatic change and leading to an explosion in the volume of information, thereby creating both opportunities and challenges. In fact, the National Intelligence Council reported: “The growing importance of information itself a primary target in future conflicts.” Would you outline some of the significant cyber and network threats and challenges facing the U.S.?

The CNO's vision includes the idea that every platform is a sensor, and every sensor will be netted. Achieving this goal requires that extra emphasis be put on the reliability and authenticity of the information and data that flows between the nodes on the network. Increased data volume leads inevitably to increased reliance on a network that is vulnerable to both attack and exploitation. To mitigate and/or eliminate this challenge is a driving factor behind the coordination between the Convergence to a Single Network, Cyberspace Operations and Electronic Warfare (EW) Roadmaps. Information is the key to future Navy operations, and we have to get this piece right or face a scenario where we will make our platforms and operational plans useless. At the unclassified level, specific cyberspace and network threats are difficult to address. That said, understanding that we are dependent on networks for data sharing and instituting processes to mitigate the vulnerabilities and threats to those networks will remain a significant area of focus for the foreseeable future.

Q: How much of the way ahead includes leveraging capability of our Joint and coalition partners? Is there a plan to facilitate between expansion capabilities for platforms that have limited real estate for SATCOM antenna?

The capability of our Joint and Coalition Partners is vitally important to the information dominance strategy. We are in a position today where we need a Joint approach both nationally and internationally for success, as we cannot do this alone. Our coalition partners share the same vision and understand that we need to do this together. Part of the strategy is for all platforms to be a sensor, as such, the information from each platform needs to be shared as quickly as possible and not all will have access to a satellite for information exchange. The Navy, in partnership with our Five-Eyes Allies and some NATO countries, is currently testing information exchange techniques using Line Of Sight (LOS) and Beyond Line Of Sight (BLOS) non-satellite bearers to enable expeditious information sharing.

Q: Does our information dominance statement incorporate/include littoral partners? i.e. do we plan to develop partner capability to gather and fuse shared information, develop plans, execute plans?

We intend, as part of the Information Dominance Strategy, to include all partners, where able, in the development and execution of information dominance capabilities. Sharing of information with our partners is a key to the success of the strategy, and a great deal of effort is ongoing to improve our own ability and that of our partner nations. This means investment within the right areas, internally and externally as part of this process. We have seen an early return on our investment strategy with unclassified information sharing for Maritime Domain Awareness improving exponentially over the last two years.

Q: What are your greatest decision superiority challenges that industry should team with you to address? How do we need to think differently to effectively team in this space?

Much of this has been addressed already in previous questions. We think the need is to approach this challenge not from an individual system perspective, but rather from a holistic "marketplace" for information.

Topic: Information Dominance for BMD

Q: How are we adapting our Ballistic Missile Defense (BMD) strategy in a cyber warfare environment when our systems are increasingly dependent on a vulnerable net-centric infrastructure?

The Navy must adapt to the increasingly interconnected and netted environment, or we will continue to put ourselves at risk of losing the capability to command and control our platforms and weapons systems. This is especially true of systems where the dynamic flow of data and information underpins the capabilities of the system itself. In the case of BMD the reliability and speed of data flow, as well as the authenticity of that data, are integral to mission execution. The Navy must develop an IA/Network Defense policy and institute a set of standards for platform/weapons systems that ensures security is built-in from the outset of program acquisition and execution. Both the BMD and Cyberspace Operations Roadmaps are taking steps to address these issues.

Q: Why are we so focused on BMD and do not include counter offensive operations options as targeting against enemy ballistic missile sites and C2 facilities?

Our initial task was to focus the MBMD roadmap on the EPAA mission. Next phases of this roadmap will expand the mission area, to include all the kinetic and non-kinetic options. Also, as other Roadmaps start to mature, such as Electronic Warfare, Cyber and Air Dominance, you can expect to see more specific attention to targeting, some of it related to the BMD problem sets, some in other areas. [The short answer is that the Navy was assigned a new national mission under the Phased Adaptive Approach. The emphasis in that mission is on gap-filling first for defense of our forces and allies in Europe from the Iranian ballistic missile threat.] Our Roadmap for Maritime BMD does consider counter offensive capabilities (principally electronic attack and computer network attack) designed to impact adversary capability to operate and command and control their ballistic missile force.

Q: There was little discussion of how we conduct attack operations associated with BMD other that mentioning Computer Network Attack (CNA) – Does this roadmap envision attack operations?

CNA is a non-kinetic option in this area. We are working closely with the N2N6F3 to include all cyber capabilities in all roadmaps. Additionally, we will have linkages and synergies with other roadmaps such as Integrated Targeting/C2 that will include other offensive capabilities that apply to the BMD mission area.

Q: How can Maritime BMD information dominance improve quality of data, information and intelligence required by the follow-on block capabilities of AEGIS, SM-3 Block 2, C2BMC and other SA and C2 systems?

Maritime BMD information dominance will improve planning, expand the battlespace and increase the probability of success in BMD engagements by providing critical pieces of information in a focused and timely manner in order to allow for better deliberate planning and options in execution.

Q: Given the range of new sensors coming on-line that could potentially help provide early ballistic missile launch detection and characterization, what architecture will best enable ingestion, correlation, fusion and use of those sensor data streams for kinetic and non-kinetic BMD?

Our BMD Roadmap team is working with Navy Air and Missile Defense Command (NAMDC), as the leader in the overall Navy Ballistic Missile Defense Enterprise (NBMDE), to ensure that our Information Dominance efforts are in consonance with Missile Defense Agency's overall Ballistic Missile Defense System (BMDS). Your question is fundamental to both the efficiency of this mission and an enabler of our Information Dominance concept.

There is no simple answer for this question, as the Navy is just part of a larger national enterprise. In many ways, Navy will continue to evolve capabilities following the lead of the STRATCOM, JIAMDO, the Missile Defense Agency, intelligence community and other federal agencies. The strategy should not be for the Navy to define its own architectures, but exploit the capabilities that are developed outside of Navy, while the Navy will focus resources on filling-in the maritime gaps in the national solutions. The strategy will be to "get connected" and "stay connected" with the national systems. However, the Navy realizes these national capabilities are not always optimized for the maritime environment, especially with the limitations of Navy manpower.

Q: What will it take to attain decision superiority for national Maritime BMD mission under the EPAA framework given likely adversary enhancements in ballistic missile capabilities, fielding and employment doctrine or CONOPS?

Attaining – and then maintaining – BMD decision superiority for the European Phased Adaptive Approach (EPAA), will take coordinated execution of the CNO's vision of

Information Dominance. Decision superiority is the result of aligning the output of all our roadmaps to meet the Commander's need for BMD-related decision superiority. It will also take integration of what are today disparate air and missile defense architectures in Europe. Our Roadmap addresses how AEGIS Afloat, AEGIS Ashore and the MOCs objectively fit in an integrated BMD architecture that can deal readily with local, theater, regional and intercontinental threats. Information dominance for MBMD will also be attained by applying non-kinetic capabilities pre- and post-missile launch.

Q: Regarding roadmaps, what is the reasoning behind the sequence of your roadmaps? Is it based upon priority or other factors?

Some of the early-delivery Roadmaps were selected based on availability of specific personnel to develop the Roadmap or, in the case of the BMD Roadmap, due to national-level direction; President Obama in September 2009 directed that EPAA have its first Aegis-equipped ship on station in 2011. As the Roadmap list expanded to 15, we opted to push the timelines for some to the right, partly due to the fact that we had already applied people from our limited cadre to earlier Roadmaps, and partly because the Roadmaps are intended to extend out beyond the current FYDP, so we will take advantage of synergies we expect to develop across the Roadmaps to have all of them organized and aligned before long. All 15 Roadmaps are regarded as high priority in terms of defining the Information Dominance "battlespace."

Topic: Networks

Q: The "Ship-to-Shore" link is the #1 "Knowledge Chokepoint" in modern naval warfare. What is the N2/N6 vision for governance and optimization of that constrained, but vital resource? Who will manage it – CANES? NGEN? Others?

N2/N6 is working convergent networks towards a set of integrated, phased programs to include CANES and NGEN that will guide the Navy toward a future net-centric enterprise environment. It will be a highly secure and reliable enterprise-wide voice, video, and data network environment supporting business and warfighters with ubiquitous access to data, services, and applications from anywhere in the world. Current enterprise networks, core networks services, functional programs and projects as well as major applications will reside on the network. This will result in an interoperable, joint enterprise environment that is standardized and enables secure access to data and services.

Q: If manpower is a shrinking commodity for the Navy, how do your investments address this fact against the ever-increasing amounts of information?

Navy investments anticipate manpower challenges through the adoption of automation technologies, smarter data sharing and work flow management, and leveraging the total workforce across all available manpower, both afloat and ashore.

Q: How do you standardize and make information interoperable when you don't control all of the sources?

Data interoperability is enabled in part by information exchange standards, which is a well-bounded technical issue amenable to agreement by parties within and beyond DoD. The formal adoption of UCore is a prime example of this paradigm. As part of our architectural compliance reviews, N2/N6 looks for and encourages the use of UCore and similar standards. Achieving interoperability via agreement on the definition of the data elements to be exchanged is a difficult challenge. We are proposing to more formally define the role of Knowledge Managers and establish the Navy governance constructs they need to improve semantic interoperability within the Navy. More broadly, the Navy participates in DoD-wide Communities of Interest to reach consensus on semantic definitions for the Department.

Q: What's the balance between organic afloat information capability and reachback? Is N2/N6 considering "Information as a Service"?

This is a good question for Industry to address, bearing in mind that there is no single answer. Rather, the amount of information that should be afloat with the Commander or available via reachback will change with the tactical/operational/strategic situation, the type of information, how timely its availability actually can be in view of bandwidth limitations and potential threats to communications paths, and how quickly the Commander needs the information. Also, the dynamic balance between ashore and afloat is in flux as we attempt to streamline the kill chain by making information available directly to the weapon, while at the same time maximizing the MOCs, thereby moving information services ashore. Bottom line is delivering the information to the Commander whenever it's needed. How much needs to be onboard, or retrievable as a service, is one of our most important challenges.

Q: It seems that full integration and fusion of information requires a common data model as a foundation. How is the Navy doing in developing a common data model for Navy and Joint use?

Many past data modeling efforts have collapsed under their own weight as the models grew too large to be of use. The Universal CORE (UCore) and associated domain core standardization efforts are aimed at defining and standardizing a relatively small, manageable set of the most critical data items in each Joint Capability Area. As part of

our architectural compliance reviews, we ensure the use of UCore and similar standards. Achieving interoperability via agreement on the definition of the data elements to be exchanged is an ongoing challenge. We are proposing to more formally define the role of Knowledge Managers and establish the Navy governance constructs they need to improve semantic interoperability within the Navy. This semantic definition work can also be extended to the larger Community of Interest-based efforts to define the various domain data cores.

Q: Who owns the "excepted" networks? Governance & Operations? Is there a common touch point?

The Excepted Networks are owned by the Echelon IIs who operate them under NETWARCOM oversight. The CARS Task Force is responsible for putting the Governance in place and functions as a single touch point.

Q: Mark Andress mentioned in his morning comments the intent to “Acquire open architectures,” specifically for SEWIP. Can you expand on this acquisition approach in the context of consistency with the Naval Open Architecture (NOA) initiative, intellectual property ownership, the use of product lines in the implementation of this approach, and the expected cost savings?

Open Architecture continues to be a critical aspect to alleviate both our acquisition and interoperability challenges. We know that cost savings are significant; however, initial investments are required, proving difficult in a fiscally constrained environment. As for interoperability, architectures must be open and modular. Much like the commercial world, we need to ensure that network system components can be interchanged and enhanced without a ripple effect through the whole system. For aviation, concepts such as the Future Aviation Capability Environment (FACE) are the first step to defining a standardized combat system processing environment. In addition to cost and interoperability savings, investments in modular, open systems will accelerate fielding capabilities, because most innovative mission system functionality can be allocated down to the software level.

Specifically regarding Surface Electronic Warfare Improvement Program (SEWIP),

PEO IWS awarded the SEWIP Block 2 contract, which satisfied many NOA tenets. They used results from performing an OA Assessment of SEWIP Block 1B to identify how to make SEWIP Block 2 more open and they used the NOA Contract Guidebook extensively in developing the SEWIP Block 2 contract for selection criteria and for contract execution to ensure that OA is build into the product. Additionally, they leveraged and reused products developed by ONR's Multi-Function Electronic Warfare (MFEW) modular open architecture technology S&T effort to reduce risk and improve system performance. The winning prime is wholly reusing many of the released

software modules, including software for pulse processing, Horizontal Situation Indicator (HIS)/displays, adjunct sensor interfaces and some firmware.

Q: What advances in IT acquisition policies will decrease time to field capabilities while ensuring Navy does not have to face the "mother-of-all" integration problems?

While we agree that IT acquisition policies take too long to field new capabilities, especially considering the pace of IT improvements, Navy must follow DoD's lead in any changes to acquisition policies. Navy will advocate for changes that speed capability to the fleet, within current statutory, regulatory, policy, and other constraints, or as made possible by changes to these constraints. Navy will not, however, advocate circumventing these constraints. Navy will also support more robust risk mitigation efforts, as opposed to risk averse processes, to reasonably accelerate capability to the operating forces.

Q: With interoperability and commonality such a priority, why isn't the government developing partnerships with academia, nonprofit standards organizations, and industry to develop a ubiquitous C2 standard for UxVs and SIGINT/FMV/GEOINT/Network sensors?

This is much bigger than the Navy, as the Navy is just part of a larger national enterprise. In many ways, Navy will continue to evolve our capabilities following the lead of the Department of Defense (DoD), Intelligence Community and other federal agencies. Our strategy should not be for the Navy to define its own architectural standards, but to leverage the solutions provided at the larger DoD enterprise in conjunction with the Office of the Under-Secretary of Defense for Intelligence(OUSD-I) for ISR. We are currently building our ISR solutions around the OUSD-I led DCGS Distributed Integration Backbone (DIB). The DIB will provide interoperability between the Services using existing and future Navy architectures.

Q: Can you comment on security vis-à-vis social media?

Social media is a powerful means of communicating that offers tremendous advantages to the Navy and Navy personnel. The use of these means of communication does not come without risk however. Security begins and ends with the user, therefore it is critical that everyone using social media understand the risks and take appropriate action to safeguard themselves, their families, and the department. This requires us to further develop existing training to remain relevant. As the ones who enable these communications to take place over the Navy IT infrastructure, it is critical that we balance the use of these increasingly important means of communication with the overall security of the network.

Q: As we move toward one "Network" how do we plan to control, monitor, and leverage the infrastructure of the host nations?

The current Outside Continental United States Navy Enterprise Network (ONE Net) environment leverages the host nation telecommunications infrastructure extensively and will continue in this manner throughout the transition to NGEN. Most off base cable plants are owned and managed by the local telecom. Consistent methods for data protection and monitoring are employed across the Enterprise to ensure data paths are secure and reliable today, and planned for the future.

Topic: Space

Q: In your future vision you show the tactical nodes using SATCOM. How will this vision work in a SATCOM denied environment?

Navy strategy to operating within a SATCOM degraded environment is centered on maximizing Protected Communications capacity and flexibility. Capacity will be increased by the fielding of the Navy Multi-band Terminal (NMT) and use of the Advanced EHF communications satellites. Flexibility will be expanded by the employment of a Protected Communications Asymmetric communications architecture which will provide Protected Asymmetric uplinks to existing GBS and SHF communications paths. Additionally, Navy is supporting the Joint Aerial Layer Network AoA (Analysis of Alternatives) in support of a Wideband line of sight networking capability.

As part of the Joint Aerial Layer Network (JALN), the vision of networking tactical nodes can be achieved in the future by leveraging connectivity to this network, which is built on the premise of operating in a SATCOM denied environment. N2/N6 is developing netted sensors concepts that gracefully degrade to Line of Sight (LOS) warfare in SATCOM denied environments. Netting sensors at the tactical level delivers advantages such as the ability to enhance targeting processes in the absence of Beyond Line of Sight (BLOS) assets through localized, enhanced multi-INT fusion and correlation. Additionally, as technologies mature, Processing, Exploitation and Distribution (PED) functionality may migrate closer to the tactical level, further enhancing survivability. N2/N6 is coordinating requirements development and experimentation/validation activities to inform upcoming POM decisions as early as FY13.

Q: You have been very clearly describing a system which is dependent on many high bandwidth communications links. You have described some very subtle approaches to protect the information from cyber warfare. However, at a very basic level our networks,

our COMMS links are not protected. They are vulnerable to jamming. At least 90% of out COMMO rides commercial links. Most of that supports ISR. What will be your response to jamming?

Navy strategy to operating within a SATCOM degraded environment is centered on maximizing Protected Communications capacity and flexibility. Capacity will be increased by the fielding of the Navy Multi-band Terminal (NMT) and use of the Advanced EHF communications satellites. Flexibility will be expanded by the employment of a Protected Communications Asymmetric communications architecture which will provide Protected Asymmetric uplinks to existing GBS and SHF communications paths. Additionally, Navy is supporting the Joint Aerial Layer Network AoA (Analysis of Alternatives) in support of a Wideband line of sight networking capability.

Our Spectrum Usage Information Dominance Roadmap, with a large amount of support from our well-established Range of Warfare C2 (ROWC2) effort, is addressing this problem area. It is not an easy problem now, and we expect it to continue to be one of our hard problems that industry can best help identify solutions. We are exploring CONOPS that will enable us to “fight through” and command and control under denied and degraded communications environments and exploring network capabilities to gap fill for denied links and broadcasts.

Q: How does the Space Cadre fit in to all of this and what's the plan?

The basis of establishing the IDC was to bring together the experts for all of our information-related capabilities (intelligence, networks, electronic warfare, cyber, meteorology and oceanography, space and unmanned systems) into one entity. The Space Cadre is part of that group of professionals; and the skills and expertise they bring to the table are integral to achieving dominance in the information age. The plan, which is already in the process of implementation, is to build a competency-based workforce with capability-driven manpower requirements. We are placing renewed emphasis on recruiting and retaining our Navy Space professional workforce, ensuring the right billets are identified as Space Cadre, and filling those billets with the right people. The Navy is committed to filling vital space leadership positions. We will provide active career management and continued opportunities for Space Cadre professionals in both Navy and Joint assignments. We will enhance career progression paths and promotion opportunities and infuse naval operational expertise in the space community. We are closely monitoring the nation's new and emerging space strategy and we will continuously review the way we approach and engage in space. To do that, we must continue to rely on the experience and expertise of Navy's space professionals to navigate in the rapidly changing strategic environment in space.

Topic: Maritime ISR

Q: In neither the "futures" chart nor the "EW Roadmap" was there a reference to UUV roles. Assuming that the energy/endurance issues are resolved, where do you see UUVs fitting into Decision Superiority and EW?

The current UUV energy and endurance challenges are driven by the power requirements for the vehicles' propulsion systems and not the relatively smaller demands of their sensor payloads for IPE, ISR, and ASW missions. The payloads required for UUVs to perform Decision Superiority and EW missions would raise the overall UUV energy requirement by several orders of magnitude. While current Navy UUV development is focused on developing sensor platforms, additional roles such as Decision Superiority and EW could be considered as the maturity and potency of power and energy technologies evolves and concepts of operation are developed.

Q: VADM Dorsett had a slide depicting sensors, processing and transport. DCGS-N was listed in transport but not processing. Can you discuss the vision for ISR processing and what role DCGS-N will have?

DCGS-N is the core ISR analysis/exploitation capability fielded afloat (CVN, LHA, LHD, LCC) and ashore (MOCs, ONI Suitland, NSAWC Fallon). The ISR Roadmap effort, supported by several on-going studies such as "The Afloat - Ashore Mix" and "UXV Interoperability," will further define and refine the role of DCGS-N as the center of gravity for the Processing, Exploitation and Dissemination (PED) aspects of the Navy's overarching ISR CONOPS and enterprise architecture. In essence, the thrust of future efforts will be to move away from platform-centric PED to an information-centric PED capability with the DCGS-N capability at the heart of analysis and exploitation.

Moreover, the Navy's strategy moving forward is to support full DCGS-N alignment with Department of Defense and Intelligence Community Intelligence Information Enterprise initiatives. DCGS-N is the Navy's critical interface to Joint intelligence in alignment with USD (I) and the DCGS Family of Systems. The scope of DCGS-N includes supporting critical I&W functions, red Common Operating Picture (COP), targeting cycle requirements, enterprise ISR capabilities, and first/second phase exploitation for numerous ISR platforms.

Q: What is your vision for submarine controlled and/or launched UAS?

The vision is not about who launches as much as who is able to access the information of platforms performing missions in their area. That being said, there remains room for

investigating smaller UAV or UUV platforms operating from submarines in the mid-future.

Q: Specifically looking at UUVs, the roadmaps do not appear detailed enough for the development community to respond to. When do you see N2N6 articulating (perhaps decomposing is a better word) technical requirements that build up a capability which addresses CFFC operations needs?

While the Navy has defined what capability areas UUVs should be employed in, further analysis to determine the missions and supporting technical requirements for these capability areas is underway. Design reference missions are currently being developed for UUVs and these will continue to be developed as part of an iterative process as specific UUV missions become better defined and technology matures to allow increased potential capability. Current Navy strategic UUV goals are built around developing the capability to deploy Large Diameter Unmanned Undersea Vehicles (LDUUVs), from a forward based operational squadron, on independent missions by 2020. This requires work to achieve the following UUV endurance/autonomy goals:

- UUV capable of 30 days submerged operations by 2014
- UUV capable of 70 days submerged operations by 2016
- UUV capable of fully autonomous operations by 2018

Q: Standardized tagging and ingest of ISR data is key to enterprise-wide exposure and discovery of the collected ISR data. How is that standardization being governed and enforced across the Navy ISR architecture? What about similar governance for ISR Platform and sensor mission data, such as collection plan, navigation plan, and health & status:

Standards for ISR related data are set from the Combat Support Agency (CSA) that manages that mission area, such as the National Geospatial Agency for Geospatial products. The enterprise aligns to the CSA standards, which ensures interoperability. Internal to the Navy, we provide governance, technical standards guidance and compliancy reviews to ensure that deployed systems, such as DCGS-N meet enterprise requirements. From the DoD aspect, the Department of Defense (DOD) Intelligence Information System (DODIIS) defines the standards for intelligence systems and applications interoperability and is managed by DIA.

Q: How do we ensure that the development of our PED and reachback capability, as well as associated ISR CONOPS, keeps pace with the emergence of the new multi-INT platforms, sensors and data streams that are in your Roadmap?

Ensuring processing, exploitation and dissemination (PED) development and fielding keeps pace with acquisition of new ISR platforms is a central tenet of the Information Dominance ISR roadmap. It is increasingly clear that the success of any enhancements in ISR demand coordinated and integrated development of all parts of the TCPED process. Assigning the ISR platforms, networks, sensors, knowledge management and PED systems all to N2N6 was a critical first step in allowing dramatic improvement to the synchronizing developments and acquisitions. Improvements in current PED processes and capacity as well as modernization of ISR CONOPS will precede development and acquisition of new multi-INT platforms and will facilitate accelerated fielding and operation.

Q: What are the biggest hurdles that you need industry to try to help you overcome in the ISR arena?

There are several significant hurdles that we must overcome to reach our objective capability, but the three biggest that industry can help us with are:

Unmanned Undersea Vehicle Energy/Endurance. Cannot move to the next step in UUV development until we can solve the energy/endurance issue. To achieve the long-range stand-off and persistence necessary to make UUVs effective autonomous ISR systems, energy sources beyond those available today must be developed.

Unmanned/Unattended System Autonomy. Need to continue to develop the ability of ISR systems to operate and self-optimize with minimum human intervention. Not only will this significantly increase the effectiveness of ISR systems, but will also facilitate their operations in denied areas.

Sensor/Platform Adaptability. Need to develop modular and/or pod technology that enables rapid, multi-INT sensors to be shifted among a variety of platforms both manned and unmanned to support dynamic warfighting environments/demands. This plug-and-play approach will be essential to enable deployed ISR assets to respond rapidly to emerging situations across the spectrum of maritime operations.

Q: Does weaponization or UAVs include non-kinetic weapons/capability?

Yes. Just as with manned platforms all capabilities will be considered for UAVs, to include the ability to attack a target with kinetic or non-kinetic effects.

Q: What is the connection between UCAS/UCLASS and FA-XX?

Just as the Navy UCAS-Demonstration program will provide and demonstrate necessary technology and procedures for operating an UAS on and around an aircraft carrier, the UCLASS program will provide and demonstrate those new technologies and procedures required for integrating unmanned aircraft with the Carrier Air Wing in an

operational environment. The technology, procedures, and lessons learned from UCLASS will benefit any future carrier based aircraft, including possible unmanned, optionally manned, or manned concepts.

Q: Unmanned platforms are regularly mentioned. What programs will be highest priority?

The Navy will continue to prioritize unmanned programs that provide enhanced capability in and from the maritime environment.

Q: How will N2N6 harmonize or influence sensor, network development with other directors responsible for platforms and weapons upon which they must be fielded?

We have had great participation in our roadmap development process from the platform sponsors, SYSCOMs and TYCOMs. We are also fortunate that with the reorganization, many of the platforms now reside within N2N6F2 so this harmonization takes place on a daily basis.

Q: Does your way-ahead reflect a shift in emphasis toward irregular warfare (and away from MCOs)?

No, not a shift. Rather it is an acknowledgement that irregular warfare requires as much consideration in the development of ISR capabilities as major combat operations have traditionally. Goal of our efforts is to take a balanced approach to both, ensuring that we don't compromise our ability to contribute to one at the expense of the other.

Topic: CYBER

Q: How are we going to ensure you can deliver "Decision Superiority" in the Cyber Battlespace?

We believe decision superiority will be achieved through the integration of policy updates, network development and intelligence requirements. Updated cyberspace security policies will ensure that the confidentiality, integrity, availability and authenticity of data, information and networks are commensurate with mission needs, information value and associated risks. Dynamic Network Defense Operations policy will be characterized by the integrated ability to detect, analyze, counter and mitigate cyberspace threats to our networks and systems. The Navy must also acquire and build networks, systems and software with security and resiliency as foundational requirements. To enable these policies, the Navy is rapidly expanding our knowledge of our own networks, as well as working to develop accurate and timely intelligence of

adversary capabilities and intentions to exfiltrate data from and/or hold those networks at risk.

Q: How are you defining Cyber Situational Awareness and Cyber Common Operating Picture (COP)?

The desired end-state of a Cyber COP should largely echo the requirements and utility of the existing Maritime COP architecture. At a minimum, a Cyberspace COP should provide a networks baseline to aid in identifying anomalous activity. It should also provide unified command and control of Navy networks, building upon a shared picture to ensure timely network I&W in support of key decision makers.

Q: What is the way forward for multi-level security requirements? Will this impact convergence to a single network?

Navy Multi-Level Security (MLS) requirements are developed and vetted similarly to all our C5ISR requirements. The MLS end-state requirement of being able to share and use information across our business and warfighting enterprise has been long standing. We have incorporated this requirement into our acquisition programs for over the past decade. An enterprise solution which addresses information assurance and protection has not been established. There are many promising concepts and projects within industry and the DoD attempting to address a technical solution. One solution may be to implement a robust data labeling strategy within an agreed upon identity management system. Currently this is being worked across the services and agencies. Enabling concepts such as convergence to a single networking environment may better position our enterprise to incorporate commercial and DoD solutions. Information security and operational security will be at the heart of any and all MLS solutions.

Q: SECDEF has recently suggested that the US Navy is over equipped with expensive assets (carriers, cruisers/destroyers, subs, and aircraft) relative to current threats, and has questioned the ability, and perhaps wisdom, of the United States to pay for the sustainment of these assets. In that context, can you comment on current and future budgetary pressure and its impact on the ability to build, sustain and employ an effective US Cyber Warfare capability?

A robust program for cyberspace operations will incur significant costs, and inevitably lead to tough decisions which will impact the traditional “platform-centric” Navy. While this may seem dire, it offers an opportunity to put the abstract concepts of cyberspace operations in terms of concrete trade-offs. We will need to articulate that in order to institute full-spectrum Navy network security; the price will come at the cost of cutting tangible assets (ships, aircraft, and personnel) to some degree. The Navy’s fundamental missions will continue to require platforms spread throughout the world’s oceans, but as they become increasingly interconnected, attention will naturally focus

on the speed, accuracy and integrity of the data flowing between them. Under the current –and likely future budgetary constraints, these questions will force the tough decisions that have been hitherto pushed to the side.

Q: Does N2N6 have a strategy for improving multilevel security capabilities?

The Navy focuses on utilization of MLS capabilities developed through the joint community. The Navy through SPAWAR and PEO C4I played a large part in the requirements definition and development. In the past, Navy led the way in the development of MLS and Cross Domain capabilities. The Joint Cross Domain Exchange (JCDX) system was the world's first Protection Level 4 MLS C4I system. The Navy fully supports and is actively engaged with the Unified Cross Domain Management Office's efforts to identify and promote a more coherent strategy for various cross domain devices deployed today.

Topic: Science and Technology

Q: What steps are being taken to improve the capturing and vetting of operational requirements and more importantly the transformation and articulation of these requirements in technical terms that individual programs and industry can use to provide material solutions that actually meet the original operational requirements?

N2N6 works closely with Combatant and Fleet Commanders to identify their capability requirements. Capability deficits and subsequent requirements are communicated throughout the various Navy Enterprises through both regularly scheduled and ad hoc meetings, seminars, and conferences.

Unrealized requirements, whether previously identified, or emergent, are validated and prioritized. These prioritized requirements are then resourced through the planning, programming, budgeting, and execution (PPBE) and Program Objective Memorandum (POM) process.

As part of this process, the requirement is assigned to a program office to manage. The program office is responsible for determining, based on the budgetary constraints, how to best provide the solution that satisfies the validated requirement in accordance with Federal Acquisition Regulations (FAR) and the Defense Acquisition Workforce Improvement Act (DAWIA) approved program management, contracting, system engineering, financial management, and information technology best practices.

The material solutions provided by the Program Offices are evaluated, tested, and approved at FAR and DAWIA mandated milestones, thereby ensuring the products

supplied to the Combatant and Fleet Commanders meet the original operational requirement.

Q: You said small, innovative companies will work primarily through large integrators, although you did mention SPAWAR and TENCAP. Do you really think an "industrial" approach to innovation is good for the future, especially in C2, ISR, and Cyber Warfare? Do we need fundamental changes in how we acquire?

A strong, innovative industrial base already exists in this country and rapidly responds to market pressures - a new "industrial approach" to innovation is not required. What is required is a better approach to the acquisition/procurement of innovative technologies from this industrial base, especially with cyber technologies.

The Navy now has the right leadership and strategic direction in place to start focusing this industrial base to better support our fight in the info/cyber domain.

Small, innovative offices like TENCAP work directly with small innovative businesses to quickly satisfy emerging Fleet needs and should continue to leverage this innovative industrial base to stay ahead of our adversaries.

Q: What guidance are you getting from ODNI, OSD(NII) and USD(I) that is informing your decisions on the technical way-ahead?

Listed organizations provide strategic policy and technical guidance on priorities within Defense Intelligence and the Intelligence Community (IC). Technical guidance drives interoperability from the strategic to tactical levels of war. Examples of the IC and Defense Intelligence informing decisions on the technical way-ahead for the Navy are Intelligence Community Directive-501 from ODNI for information sharing and the Distributed Common Ground System-Navy Family of Systems for Intelligence, Surveillance, and Reconnaissance (ISR) from OSD(NII)and USD(I).

Guidance from offices such as ODNI, OSD (NII), and USD (I) (and other organizations such as DDR&E, JCS, and USD (AT&L)) impact our technical and management approaches. For example, we are working with OSD (NII) on how to redefine and streamline traditional Command and Control for the 21st century warfighter, with AT&L on harvesting Joint Capability Technology Demonstration products, and with the JCS Joint Capability Area structure by aligning our program management/technology acquisition to the OSD Capability Portfolio Management model. OSD (NII)'s Net-Centric Data Strategy and Services Strategy also inform our efforts to achieve a netted force. We contribute to the Navy's T&E efforts in identifying and resolving issues with the testing of complex systems of systems, information assurance and other issues as highlighted in recent DDR&E initiatives in these areas. Additionally, our Defense

Science Board participation stressed a greater emphasis on interoperability, and we are contributing to current efforts on the developing IT Acquisition Reform.

Q: Where do small, innovative companies with specific areas of expertise plug into the Information Dominance way-ahead?

Small, innovative companies primarily plug into the Information Dominance way ahead in three ways – two more immediate and one longer term.

The two immediate paths are through the Small Business Innovative Research (SBIR) program and the congressionally chartered TENCAP model. For the SBIR, a percentage of our Total Obligation Authority (TOA) is set aside to encourage innovative approaches from small companies and individuals who would otherwise not have an opportunity to participate. For the TENCAP model, emerging Fleet needs and capability gaps are taken directly to small innovative companies for solutions that can be quickly be satisfied in 12-18 months. For both of these paths, each successful innovative approach is transitioned, integrated and implemented into a Program of Record.

On a longer term basis we make our requirements known to the Office of Naval Research (ONR), who through the range of available Science and Technology vehicles, solicits approaches through Broad Area Announcements (BAA), among other venues, for innovative approaches, often involving small and/or disadvantaged companies. As these innovations work their way through the technology maturation process and find their way into our PORs.

Q: Is the Navy considering - new mission - monitoring of deep water drilling sites with UUV's?

While the Navy maintains several multi-purpose assets which can be leveraged to assist in maritime environmental protection and cleanup, this remains primarily the responsibility of the United States Coast Guard and the Oil and Gas Industry. The Navy is investigating the possibility of monitoring and protecting our offshore infrastructure from malicious threats. If taken on, this new capability may or may not involve the use of UUVs to survey or protect offshore infrastructure such as that used by the offshore oil and gas industry.

Q: What are your most critical areas of emphasis for S&T needed to address the technology gaps in the roadmaps?

We need to be able to give the Commander the assured communications to support his/her mission areas with reliable C2 and reachback to required information that is not immediately at hand. Flexible, survivable and defendable communications are paramount, and we have yet to arrive at any real answers to this point.

Q: Can you speak to acquisition reform?

Current Federal Acquisition Regulations (FAR) are codified in Title 48 of the Code of Federal Regulations. Within the Department of Defense, statutory authority to issue and maintain the FAR resides with the Secretary of Defense, subject to the approval of the Administrator of Federal Procurement Policy. Acquisition reform occurs when Congress passes new legislation, signed by the President, which adds to, amends, or removes applicable sections of the FAR.

Q: How does Navy take advantage of and influence industry-driven technology advancements while managing operational impacts and investment costs?

We are adopting a strategy of "buy a little, test a lot" and rapid prototyping that we believe will allow for more responsive acquisition to keep pace with the explosion of new technologies. Our Technological Innovation Branch keeps abreast of the latest technological developments and works in partnership with ONR, academia, the Fleet experimentation community, etc. to assess operational potential of those technologies. In addition, each Roadmap will include an assessment of total ownership cost for any functional solution included in the action plan.

The Navy Sea Trial process is our primary venue to insert new technology into operational environment. At this level, we see how new technology can help adapt current TTPs. But the real key to new technology is to co-develop and introduce new doctrine in conjunction with new technology. Today, we are using the Office of Naval Research (ONR) C2 Rapid Prototype Continuum (C2RPC) to insert new TTPs and new technology as an integrated solution. The ONR C2RPC acts as our C2ISR incubator that will then transition capabilities directly into our C2ISR systems. As far as controlling investment cost, we work closely with USFF to evaluate our solutions, and then make POM investment decisions trading current readiness for future readiness, which means the Fleet may have to operate with some reduced capability until we can fully field future systems. This is a risk-based decision that is made in every POM.