Information Dominance Industry Day Questions and Answers

Opening Remarks:

1. Can you talk to any plans for EP-3 recapitalization and related funding?

The EP-X Program of Record (POR) was terminated in 2009. The Navy is instead developing a "Family of Systems" construct to recapitalize the EP-3 Airborne Intelligence Surveillance Reconnaissance and Targeting (ISR&T) capabilities within existing Programs of Record.

Broad Area Maritime Surveillance Increment 3 (BAMS Inc 3) will provide long endurance, land-based, remotely operated Signals Intelligence (SIGINT) capabilities, and will provide airborne support to Maritime Domain Awareness (MDA) and Intelligence Preparation of the Battlespace / Environment (IPB/IPE).

Medium Range Maritime Unmanned Airborne System (MRMUAS) will provide medium endurance, sea-based, remotely operated SIGINT capabilities, and will provide support to Special Operations Forces (SOF).

Unmanned Carrier Launched Airborne Surveillance and Strike (UCLASS) will provide a carrier-based unmanned aircraft system that offers long-endurance, proven ISR&T and precision-strike capabilities.

MQ-8B Fire Scout provides sea-based, remotely operated SIGINT capabilities and relays real-time ISR, battle management, and target classification data to tactical users. It can operate from all air capable surface ships as well as confined land sites.

Fire Scout is currently deployed and expected to reach Initial Operating Capability (IOC) in the 1st quarter of FY12. The other systems have proposed IOCs in the 2019 timeframe.

All of these programs are integrated into the Navy FYDP.

2. Roadmaps: Seven are complete, 2 are coming. How does industry get copies of the roadmaps?

Roadmaps are currently undergoing a final executive review before release. Once complete, please email Angela Marino, angela.marino@navy.mil, your siprnet email address. She will contact you with the appropriate links.

3. Have the White papers that Industry submitted been of use to the Navy? How have you used them?

N2N6 received 78 white papers as a result of the June 2010 Industry Day. Our Concepts and Strategies Division vetted the white papers for relevance, and forwarded those papers to the appropriate divisions within N2N6 for a detailed review. The white papers as a whole provided insight into potentially game changing technology advances in networks, network security and interoperability. They shared a common vision for the need to migrate to "cloud" architecture. They also called out emerging cyber applications and demonstrated how industry and the Navy's Science & Technology arm are working on emerging capabilities. Some papers suggested immature or non-existent technologies; unfortunately, our current constrained fiscal environment precludes us from pursuing new program starts. Several white papers reviewed by N2N6 divisions contained emerging or potentially game changing capabilities, but also acknowledged ongoing parallel efforts with ONR, DARPA, and/or PEOs on the same types of capabilities. As our roadmap efforts continue, we will revisit various white papers for consideration. Some division SMEs found value in forwarding solutions proposed by industry to NWDC/NUWC to better determine the technical feasibility of the concept and/or forwarding to ONR/PEO C4I for further consideration. Some capabilities proposed by industry are under advisement pending completion of Analysis of Alternatives (AoAs).

4. You have ambitious goals for Information Dominance. Is the Navy workforce up to the challenge?

We have some of the brightest and best Sailors in the IDC community. Our job is to challenge this generation that was raised on technology. We need to convey the sense of importance and impact they can have on Navy missions. One of the responsibilities IDC leaders have is to ensure we are providing them with clear paths to provide "Mission Value." Sailors need to understand what they do is important, while other Navy and joint warfighters must have high expectations of our people.

5. Do the Information Dominance roadmaps include direction for programs of record?

Yes, all roadmaps contain an Action Plan that includes specific recommendations affecting existing programs of record.

6. Have budgetary concerns affected the timing for release or scope of the roadmaps?

No, the first iteration of the roadmaps was not affected by the budget as the vast majority of the programmatic recommendations they contained were germane in any budgetary situation.

Navy Ballistic Missile Defense:

7. NC3 is assured comms via EAMs. Could be used with non-nuke. Why not invest with AIR Force on this?

Navy reviewed expanded use of nuclear messaging for Ballistic Missile Defense (BMD) and recommended not using Nuclear C3 Long Term Solution (LTS) for BMD. Navy and Air Force units will exchange technical data where feasible to minimize costs for the programs. Nuclear messaging has stringent Information Assurance and operational requirements that preclude its use for BMD (additional pertinent requirements are classified). Specifically, LTS needs to be a dedicated and cryptographically isolated system for US only, and BMD could expand users to coalition partners. Command Control Battle Management and Communications (C2BMC) supports high volume, high speed wideband data, LTS requires low volume high speed messaging. NC3 LTS primary users are at the strategic level and require the assured, rapid communications LTS is designed for. To add the BMD mission -- using C2BMC -- risks spillover, system failure and potential for LTS traffic to be slowed or blocked due to volume of C2BMC traffic. Critically, LTS is required by the National Security Agency to be a dedicated network, isolated from other networks. Technically, to integrate the two requires a multi-level security solution. The complexity was assessed as high risk to failure for both systems, and there was not any estimated cost savings. The LTS system is funded by both the Navy and the Air Force.

8. Does the Navy's Global Ballistic Missile Defense Systems plan include acquiring additional Cobra Judy ships or other major sensor capabilities?

The COBRA JUDY Replacement ship is under construction with a FY 14 IOC and will bring more advanced capabilities to the fleet. The Air and Missile Defense Radar (AMDR) is being planned for FLT III DDGs with an IOC in 2023

9. How is the Navy currently relying on C3I in BMD and how will this process be improved?

C3I provides the backbone of command and control (C2) in all warfare areas, including BMD. The BMD mission is inherently Information Dominance-centric, and can be divided between "Left of Launch" and "Right of Launch." In "Left of Launch", effective cyber warfare and penetrating knowledge of the adversary are critical to shaping the battlespace. "Right of Launch" is focused on network support to the warfighter.

Navy BMD C3I enables C2 to make rapid decisions inside the adversary's decision cycle. The Navy is currently leveraging a proven and fully functioning BMD C3I architecture. Navy ships with BMD capability and key Fleet Command and Control nodes are part of the BMD system. This includes mission planning systems, sensors, fire control, and command and control centers from the tactical edge connected to the National level.

In BMD, the Navy closely works with the Missile Defense Agency (MDA), STRATCOM, and other services on C3I matters to ensure effective BMD is delivered from BMD-capable ships and the future Aegis Ashore, via the Regional and Fleet Commanders, to BMDS at the National level.

While we have a working structure, we clearly see growing adversary threats which necessitate better performance and capacity on the part of our networks. More ships are needed to intercept more ballistic missiles in a complex tactical/operational environment. To this end, we are improving network capabilities and access through the addition of Advanced Time Division Multiple Access Interface Processor (ATIP) and improved integration of Maritime Operations Centers (MOCs) with Joint Tactical Terminal (JTT) and Navy Multiband Terminal. We are improving BMD Mission Planning across the theater by integrating Aegis Mission Planner, MIPS-Maritime IAMD Planning System, and C2BMC. Starting in FY12 we have proposed adding 15 TF-IAMD Navy personnel with BMD expertise in each MOC.

Starting this summer, we are making a significant step in network management with our prototype Link Monitoring and Management Tool (LMMT) at C3F and C6F.

10. BMD is challenging mission unto itself, but how do you see the impact of N2N6 in the future in terms of the larger IAMD mission?

Adversary ballistic missiles threaten our allies worldwide and our homeland- Hawaii, Alaska, Guam, and CONUS itself. Chinese development of so-called 'carrier killer' ASBMs compounds the Navy BMD challenge as our afloat forces become targets of exoatmospheric ballistic missiles in addition to the variety of cruise missiles and other threats we face. The Navy must integrate BMD into an effective, broader Integrated Air and Missile (IAMD) capability. The Navy Air and Missile Defense Command (NAMDC) at Dahlgren has the task to promote rapid delivery of new IAMD technologies; support development and validation of IAMD requirements for Joint and Navy processes; lead Navy IAMS concept, doctrine, and tactics development, and experimentation; and, advocate Navy positions and capabilities in Joint forums. We are closely aligned with NAMDC through the BMD roadmap as a part of the Navy Ballistic Missile Defense Enterprise. These alignments provide us the opportunities to play vital roles in IAMD, bringing important capabilities from across N2/N6. These include, on the right side of the kill chain, improved C3I and network integration and operational coordination. On the left side of the kill chain, this means development of constant and penetrating knowledge of the adversary and cyber skills to provide persistent access to adversary networks. Across the full kill chain, it means supporting the ability to synchronize kinetic and non-kinetic responses to give our afloat forces the confidence to operate effectively in the face of a full range of threats.

11. How has the N2N6 consolidation benefited Navy's ability to support the BMD mission?

Bringing together a variety of information-centric parts of the OPNAV staff has created a synergistic environment that encourages improved cooperation of collaboration. Networks, C3I-supporting-C2, Intelligence, TCPED, a maturing cyber domain, and METOC to support "Battlespace on Demand" all fit together under the N2N6 umbrella. My ability to budget has also been enhanced. Competition for resources is within N2N6 rather than dispersed across a number of OPNAV directorates. As a result, I have improved visibility across shared roadmap development, as well as our entire portfolio. This allows us to make smarter and more timely decisions regarding what really needs to be

funded; and more importantly, what is really impacted when we have to delay efforts or have to deny funding due to our many competing requirements.

Electronic Warfare:

12. What is the Navy's gameplan for accelerating integrated topside (INTOP) capabilities to enable the type of EMS sharing and bandwidth optimization you outlined?

We believe Integrated Topside (INTOP) is a great Science and Technology (S&T) initiative and is an example of Navy's ability to pace and take advantage of technology. Currently INTOP is on the path to maturation and transition. With the ability to provide multi-function apertures, simultaneous beams and simultaneous functions, it will be an important part of EMS sharing and optimization. At this time, it is still an Office of Naval Research (ONR) S&T program and entering a prototype phase. We understand there are still some "science" efforts that are necessary to meet some objectives and acceleration is not an option at this point. From an EW perspective, we are looking forward to having INTOP delivered to the surface force and integrated into EW program efforts as soon as possible. We in N2/N6 are not aware of any plan to accelerate INTOP.

13. Improved equipment is definitely needed to keep pace with adversary advances. What are your plans to ensure enlisted technicians (EWs) are properly and adequately trained employ these new systems to counter these threats?

Electronic warfare (EW) is a priority to the CNO and throughout the Navy. The modernization of EW systems, and how personnel are trained and managed, is all part of our holistic approach to modernizing EW systems. However, we are not waiting until new systems come online, but are re-emphasizing tactical EW throughout the fleet. Our ability to maintain EW superiority is incorporated into our EW wholeness strategy - incorporation of systems, manning and training to solve EW challenges.

14. How much (or how little) can EW help the piracy problem?

The Combined Task Force 151 was established to deter, disrupt and suppress piracy. A variety of traditional EW systems are on all ships assigned as part of this multi-national task force operating in and around the Gulf of Aden, Arabian Sea, Indian Ocean and Red Sea. The ability to provide Commanding Officers and other units in the CTF with better situational awareness of ships and aircraft in their area as well as cueing for other assets such as on-board helicopters is an important EW contribution.

Some would also characterize at least one of the defense measures against piracy as non-kinetic or asymmetric EW when using Long Range Acoustic Devices (LRAD) to ward of piracy attempts. The U.S. Navy has used this equipment in support of a variety of missions and in the past we know some commercial vessels have employed this capability as a deterrence measure.

The unsophisticated nature of pirate operations does not mean EW cannot play an important role in patrolling and responding to piracy activity. As an organic capability, we believe it demonstrates the flexibility of EW systems to be effective against a relatively low end threat while, as always, being ready for more sophisticated challenges. Still, the opportunity exists to the push the envelope in innovation and EW techniques and welcome suggestions for interested parties.

15. How will Navy acquisition keep pace with the EW recapitalization sense of urgency?

Recapitalization with new baseline systems throughout the fleet is being approached in a spiral evolution or “block” strategy. To meet the sense of urgency for the challenges of today’s potential adversaries and dominating in the EMS, programs such as Shipboard EW Improvement Program (SEWIP) and others are developing and fielding upgraded components or groups of components; not waiting on complete solutions to all documented key performance parameters. This block approach allows for a much quicker pace in acquiring and recapitalizing Navy EW in an evolutionary approach. Additionally, Navy acquisition is well coordinated with our Navy investment in EW. The Navy acquisition process and EW recapitalization initiative are based on a partnership between Navy, industry, and government laboratories. Ultimately the recapitalization effort of baseline Navy EW Programs of Record will make all systems more agile and flexible with an inherent ability to receive technology insertion in responses to missions or emerging threats as needed.

16. What if the attack is not jamming/denial, but cyber and how do we exercise against this?

A key area of concern for Navy is the increasing interdependencies between EW and CNO/Cyber. Many people wrestle with the concept of EW and whether or not IO should encompass all five disciplines as previously codified in JP 3-13. In fact, EW no longer consists of relatively straight-forward jamming or broad-based denial of access to portions of the EMS. Characterizing the disciplines within IO as systems-based (EW and CNO) or content-based (EW, CNO, MISO/PSYOP, MILDEC, and OPSEC) demonstrates some of the difficulties in answering this question. This relationship can be seen as two sides of the same coin, especially as the execution of these warfare capabilities continue to mature and as we develop ever more sophisticated options to achieve specific effects.

Along those lines, a "cyber attack" can take many different forms, depending on the intended effect of the attacker. Denial of service is certainly one form of cyber attack, and perhaps the best known. Other forms of cyber attack include computer to computer manipulation that results in loss of confidence in the system or the data that resides on it. This loss of confidence can come in the form of false injection of data, outright deletion or removal of data, corruption of data or the software used to manipulate it, or redirection of data, to name a few potential avenues of attack.

Currently Navy exercises its network defenses through the Information Operations Condition (INFOCON) system used throughout DoD, and is actively participating in drafting its successor, the Cyber Condition (CYBERCON) system. Additionally, Navy is increasingly incorporating computer network defense into larger Fleet and Joint exercises to better help operational commanders understand how to fight through a network attack and ensure mission assurance on their networks.

17. With your goal of having every ship a sensor, how do you plan to handle the large volumes of data? Google processes 1 Petabyte every hour today. Can the Navy do that kind of data crunching?

An alternative question should be, "Does Navy need to process data to the level accomplished by Google?" One of the greatest challenges Navy faces now is dealing with the vast (and increasing) volume of data, as we work towards our goal of making "every platform a sensor, and netting every sensor". Assigning relevance and a level of importance to this data is integral to managing this problem. What we want is data that can be analyzed by our Intelligence professionals, and turned into timely and relevant information for our operators, not an unmanageable dump of raw data.

This problem is being aggressively addressed by our Tasking-Collection-Processing-Exploitation-Dissemination (TCPED) working group. It is actively studying Navy TCPED operations to discover a process for separating the wheat from the chaff, which should keep data transfer to a realistic level. One method of accomplishing this is the utilization of “indexing” to tag and “advertise” data.

We don’t always know what we need, so we must also be able to store partially or unprocessed data as well. Navy remains committed to working with our commercial sector partners to help grow our own capabilities to store, process and disseminate large volumes of data. However, we need to focus greater effort on providing quality data, information and intelligence to the warfighter, particularly actionable intelligence in which timeliness of information is essential.

It is a major challenge in getting where we need to go with TCPED. We believe it is a combination of knowing what to process and keeping the data transfer small. But we don’t always know what we will need so we must be able to store partially or unprocessed data as well. We need industry’s help, but ultimately we think the best answer lies in a combination of solutions.

18. Much of world is moving to cloud computing. Does the Navy have any plans to make its sensor data available and discoverable beyond each ship? Also, is the Navy pursuing secure cloud computing in parallel with the data center reduction plan?

Navy is investigating secure cloud computing and in parallel with the data center reduction plan. Cloud computing potentially offers many capabilities that may enable effective utilization of existing data centers. However, cloud computing would be only one potential consideration that helps to determine which data centers could be consolidated or reduced. Data strategy, new architectures, application rationalization, virtualized computing and continuity of operation would be some other considerations that assist in determining data center consolidation or reduction. Navy is optimistic that we can realize cost efficiencies as well as increased capabilities with the implementation of cloud computing concepts such as integrating and synergizing with a larger cloud community that includes both DoD and the Intelligence Community (IC).

In some instances, Navy is already active in moving forward to incorporate cloud computing technologies with both DoD and the IC. This will enable the truly valuable aspect of employing "every ship as a sensor" and making data available and accessible. Our information collection capabilities and

associated information sharing needs will grow much faster than our afloat bandwidth capacity so we are researching tools, applications and technology for smart "tagging and indexing" capabilities to "advertise" relevant data via limited communications paths.

We are also investigating how cloud computing might strengthen our command and control of the “Intelligence, Surveillance, Reconnaissance, and Targeting (ISR&T) Family of Systems” along with the next-generation of processing, exploitation, and dissemination (PED) operations. We envision that cloud computing will enable an individual operator to utilize sensors regardless of their location, and that this will increase our operational and tactical effectiveness while delivering a worldwide-capable PED architecture. We do not view the Navy as building its own standalone cloud construct, but instead we will build an interoperable interface with the larger US and Coalition cloud communities by partnering with DoD and IC elements to achieve a collective and comprehensive ISR&T picture that will fuse data and capabilities from various ISR collection sources to best inform the supported commander with relevant, timely and accurate knowledge.

Afloat, the US Navy's Consolidated Afloat Networks and Enterprise Services (CANES) program is designed to build a secure shipboard network required for naval and joint operations, and consolidate and reduce the number of shipboard networks through the use of cross domain technologies and common computing environment infrastructure. The CANES Common Computing Environment is a rational migration towards a cloud enterprise approach tempered with the reality of the Navy’s unique maritime requirements.

19. How will Navy implement adoption of cloud architectures ashore and afloat in a declining budget?

Navy is currently in the initial stages of reviewing potential options regarding a “way ahead” with respect to cloud computing. Navy is optimistic that we can realize cost efficiencies as well as increased capabilities with the implementation of cloud computing concepts such as integrating and synergizing with a larger cloud community that includes both DoD and the Intelligence Community (IC). We are also investigating how cloud computing might strengthen our command and control of the “Intelligence, Surveillance, Reconnaissance, and Targeting (ISR&T) Family of Systems” along with the next-generation of processing, exploitation, and dissemination (PED) operations. We envision that cloud computing will enable an individual operator to utilize sensors regardless of their location, and that this will increase our operational and tactical effectiveness while delivering a worldwide-capable PED

architecture. We do not view the Navy as building its own standalone cloud construct, but instead we will build an interoperable interface with the larger US and Coalition cloud communities by partnering with DoD and IC elements to achieve a collective and comprehensive ISR&T picture that will fuse data and capabilities from various ISR collection sources to best inform the supported commander with relevant, timely and accurate knowledge.

20. Can you discuss what it means for the Navy to concentrate more effort on the non-kinetic, information solutions?

We are in a new era where globalization and the convergence of computer and telecommunication networks have transformed the information environment from an enabling capability to a core warfighting capability. As Admiral Dorsett described recently when speaking of the shift from an Industrial Age military force to an Information Age force, "It's now time for the Navy and frankly the U.S. Joint forces, to step up and start dealing with information in a much more sophisticated manner than they have in the past." The U.S. Navy and our adversaries recognize this fact.

New concepts in warfighting are creating opportunities to enhance Navy's contribution to National Security, but we must fully integrate information, intelligence, C2, and Cyber capability and wield it as a weapon. This concept and its instantiation means non-kinetic effects to many.

In the past, the Navy has invested in sensors, weapons, and control systems, but sub-optimized their overall effectiveness through architecture that were "welded" to each individual platform. This legacy platform-centric approach unacceptably increases our operational risk as we continue to evolve in the Information Age. We are addressing these gaps by decoupling, both programmatically and functionally, platform-sensor-weapon artifacts and reconfiguring them as distributed, adaptively networked enterprise capabilities.

However, one could say even with these enterprise-wide initiatives we are "out of balance" if we can't truly defend and attack in the information battlespace as well as operate our networks. With that in mind, one of the returns on the investment to reorganize as an Information Dominance directorate has been the increased opportunity to explore and support non-kinetic operations. Our Electronic and Cyber Warfare and ISR Capabilities Divisions are working together to accomplish these

complex tasks as we mature our thinking and developmental efforts with stakeholders across the Navy and throughout DoD.

MOC and MDA:

21. What role is the Maritime Operations Center playing in the current crises in the Middle East?

Planning for operational level maritime operations is conducted in conjunction with higher headquarters (HHQ) staffs. During the current Mideast Crisis, US Africa Command (AFRICOM) and Central Command are coordinating with and providing guidance to their maritime components; US Naval Forces Africa (NAVAF) and US Naval Forces Central Command (NAVCENT), respectively. The Maritime Operations Center (MOC) provides a framework from which Navy commanders at the Fleet or operational level to exercise command and control (C2). C2 entails both the processes (planning, directing, coordinating, and controlling forces and operations) and systems (personnel, equipment, communications, facilities, and procedures employed by the commander) as they relate to the exercise of authority and direction over assigned or attached forces and organizations. MOCs support the commander in monitoring, assessing, planning, and directing assigned missions at the operational level. In response to the current Middle East crisis, the NAVAF and NAVCENT MOCs are planning at the operational level, as well as directing, coordinating and controlling assigned forces in response to HHQ and combatant command guidance. More specifically, on 4 Mar, NAVAF, announced the stand-up of JTF-Odyssey Dawn. The joint task force will provide command and control for emergency evacuations, humanitarian relief, and any future AFRICOM mission support of the U.S. government response to unrest in Libya.

22. Your 2020 ISR Operations in HOA scenario did not include the Navy's Network Operations Centers (NOCs). Since Information Assurance (IA) is a pillar of Info Dom shouldn't the future vision include the NOC? Do you see NOCs being outsourced to DISA?

The Network Operation Center (NOC) remains an important element of Information Dominance for providing reliable, secure IP network services across all enclaves to the operational Navy forces regardless of where those operations occur. The Navy continues to review the optimal approach for delivering network services that satisfy the expectations of the operating forces in both benign and

contested operating environments. No compelling information exists today to conclude that NOCs or network services in general should or should not be outsourced to DiSA.

23. MOC Funding- How much is NIP and MIP funded? What is the focus of this funding?

The Navy Fleet MOCs are not funded by NIP or MIP funding. Programmatically, the MOC is treated as a system-of-systems. This system-of-systems approach forms a complex system that offers more capability and performance than the sum of the individual capabilities. Multiple programs of record provide installation and sustainment funds for various systems that are within the MOCs. These include GCCS, DCGS-N, NMCI, ONE-NET, and CENTRIXS to name a few. The non-POR systems installed within the MOCs are funded and sustained through OPNAV N2/N6 via the POM process. Also, operations and maintenance funds provide and support standardized Command and Control systems and missions at the numbered fleet HQs. These systems support deliberate planning at the Operational Level of Warfare. OPNAV N1 and N4 also have funding responsibilities for the MOCs. These include funds to support the Fleet MOC personnel, the MOC Accreditation and training teams and support for the Maritime Staff Operators Course at the Naval War College.

24. When you say ISR- your implication and what we see on your chart is imagery intensive. In Iraq and Afghanistan we've learned that other INT's (HUMINT, SIGINT) enabled Imagery ISR has truly enables the warfighter. PED can't/won't support an unfocused imagery "take." Why aren't we at least equally focusing on ISR (UAV) SIGINT Systems given all we've learned in the current fight? How do we "tag" imagery data like we do SIGINT data and replicate RTRG/Turbulent Wave capabilities for imagery?

Many of our current efforts are imagery focused, but not imagery exclusive. As VADM Dorsett noted in January of this year, the Navy is "tackling imagery exploitation first, as something easier to get our hands around. We're also partnering with the National Security Agency on its cloud computing and cyber pilot initiatives to facilitate how information is managed and how we flow it from one point to another. We envision close collaboration with NGA as it defines imagery tagging standards, and we expect future systems, such as DCGS-N Increment 2 will have the capability to perform multi-source analysis functions involving all intelligence disciplines.

Initial fielding of UAVs is GEOINT sensor-focused. Beginning in FY16, Navy will begin to experience massive GEOINT "take." Our current efforts are to focus on TCPED for GEOINT,

understanding it will need to expand as we begin to field platforms to collect other “INTs” later in the decade.

25. How will Navy encourage Industry participation in the development of processing algorithms and other analytic applications?

The Navy encourages industry participation in the development of processing algorithms and other analytic applications primarily through its participation in Industry Days, Broad Area Announcements (BAA), Requests for Information (RFI), and Small Business Innovate Research (SBIR) efforts. Industry also has opportunities to participate in technical standards forums. Acquisition Commands/centers contracting offices make efforts to award contracts that encourage open and standard systems that leverage Intelligence Community standards for multi-intelligence meta-data sharing. For example, the Common Distributed Ground/Surface System-Navy (DCGS-N) Increment 1’s fundamental acquisition strategy is to leverage mature Commercial-Off-The-Shelf (COTS) and Governmental-Off-The-Shelf (GOTS) products to reduce costs and ensure joint interoperability. Looking to the future, Increment 2 intends to build on the success of Increment 1 and seeks to award competitive contracts (to the maximum extent feasible) that will take advantage of GOTS and COTS algorithms and analytic applications. Additionally, Consolidated Afloat Network Enterprise Solution (CANES) has been labeled an example of the Pentagon's recent "Better Buying Power" criteria. The CANES program is designed to: (1) Target Affordability and Control Cost Growth (2) Incentivize Productivity and Innovation in Industry, (3) Promote Real Competition, (4) Improve Tradecraft in Services Acquisition, and (5) Reduce Non-Productive Processes and Bureaucracy.

26. Will Navy adopt a single computing environment for Processing, Exploitation, and Dissemination (PED) and data display (Common Operational Picture)?

Navy intends to adopt a common computing environment (CCE), namely the Consolidated Afloat Networks and Enterprise Services (CANES) to facilitate and enable infrastructure support to the Common Distributed Ground/Surface System-Navy (DCGS-N) for Processing, Exploitation and Dissemination (PED) and for supporting the Common Operational Picture (COP). The Navy is replacing five C4I networks with a single hardware infrastructure. The Navy will install the scalable, commercial hardware to be procured under CANES on approximately 300 Navy ships in addition to shore-based sites. To respond to emergent threats and capability needs, additional options including installing

additional computing resources require additional system modifications. The Intelligence Carry on Program (ICOP) may be a stand-alone PED system or Navy may require temporary capabilities to meet emerging threat requirements until CANES is fielded to provide the support.

Assured Communications:

27. Has the Navy studied DoD BRAC consolidation examples (ex:NGA) as a model for comms redundancy, datacenter consolidation and implementing thin clients?

Navy is currently reviewing the efficiencies that can be gained and implemented which are similar to DoD BRAC and is conducting interim coordination with other agencies and services as a prospective models and partners for communication redundancy and data center consolidation. The review is expected to extend to at least September 2011 in which more will be understood and for which planning could begin for feasible consolidations.

28. Navy Multiband Terminal is a key piece of assured communications. What priority is it receiving in future budgets?

NMT remains one of the Navy's most important terminal programs that leverages the DOD's significant investment in military wideband and protected satellite communications and provides increased access to Space segment capabilities in both benign and contested environments. Given the dynamic environment in which the Navy develops its budget, it is not possible to specifically say that what priority NMT will receive in future budgets. NMT will continue to compete for budgetary resources consistent with guidance provided by the Chief of Naval Operations.

29. JALN ICD is also being pursued by Air Force. Wouldn't an air tier layer backup be a good leveraged AIR SEA Battle construct?

The primary point of the Joint Aerial Layer Networking effort is to develop a joint construct for providing aerial layer communications. There are multiple potential uses for an aerial layer, to include providing an air tier layer backup within the Air-Sea Battle construct. Navy is fully engaged with ASD/NII and the Services on the JALN analysis of alternatives study which is expected to recommend approaches for aerial layer communications for multiple scenarios, including as an air tier layer backup.

30. Will routing in space (onboard satellites) in the future enhance Assured Communications or increase the challenges?

The Navy provides UHF satellite communications to the DOD. The next generation UHF capability is the Mobile User Objective System (MUOS). MUOS does not use onboard satellite routing (routing in space). The Navy has not assessed the impact of routing in space on assured communications.

31. Does the denied satellite access issue cause you to think about an HF backup for BG comms?

HF communication remains an important capability for the Navy as an alternative beyond-line-of-sight communication capability. The low throughput capability of HF limits its applicability in meeting wideband needs. HF communications continue to provide voice and low data rate data communications capabilities, to include low data rate internet protocol (IP)-based communications.

32. Since Link 16 is going to be around for a long time, is the Navy going to invest in improvements to the datalink?

Navy has invested in near term improvements to Link 16 that include Cryptographic Modernization, Frequency Remapping, Dynamic Network Management and Enhanced Throughput. Navy, along with Air Force, is developing a longer term strategy to increase the capacity of Link 16 through improvements like Concurrent Multi-Netting/Concurrent Contention Receive and/or offloading future requirements that would further burden the Link 16 network to an Advanced Tactical Data Link network.

33. What is the role of 4th Generation 4G Broadband mobile networks?

The Navy has no specific requirement for a fourth generation 4G Broadband mobile network.. The Navy's current solution for narrowband satellite communications, the Mobile User Objective System (MUOS), uses 3rd Generation cell phone technology and an advanced fiber-optic ground infrastructure to create global user networks.

34. Most of the assured comms discussion seemed to be focused on the tactical level of war. Can you address assured comms inputs at the operational or strategic levels of war?

Assured communications efforts have been predominantly focused on communications capabilities necessary for forces operating in contested/degraded communication environments. These communications capabilities can be applied to forces regardless of the level of warfare at which they operate. The Joint Ariel Layered Network Analysis of Alternatives currently in progress will provide insight into communications required at the tactical, operational, and strategic levels.

Unmanned Capabilities:

35. Can you comment on the reported "modularity" between USAF MQ-X and USN UCLASS programs and how that would be achieved?

Coordination at the working level is ongoing between USAF MQ-X and USN UCLASS activities. It is envisioned that both potential programs could utilize Joint networks for command and control as well as incorporate much of the same sensor technology.

36. How the Air Force announcement regarding Global Hawk affect BAMS technology roadmap?

The Air Force announcement of decreasing purchase of RQ-4 Block 40s does not introduce a significant cost or schedule impact to the BAMS UAS program. The Navy and the Air Force continue to work together to understand how changes to either the Global Hawk or BAMS UAS programs would affect the other Service.

37. In your Family of Systems concept, what role is envisioned for MRMUAS?

The MRMUAS will host multi-intelligence collection capabilities on an airframe that is capable of operating from all air capable ships in the Navy's inventory equipped with appropriate control systems, communication links, and launch and recovery equipment. This ability greatly increases the Navy's capacity, responsiveness, and overall agility to conduct Maritime Domain Awareness and SOF support missions in maritime and littoral domains. The increased range and endurance, and beyond line of sight communications capabilities of the MRMUAS program make it ideally suited to take-on the FMV and

SIGINT centric Irregular Warfare (IW) mission sets currently assigned to the Navy's aging Manned airborne ISR assets.

38. When can we expect to see the UCLASS RFP?

The draft UCLASS acquisition path forward is currently under review by Navy and OSD representatives. A UCLASS RFP release is incorporated in the path forward. The dates for its release as well as other key milestone events are being evaluated. We will release these dates to industry just as soon as we can.

39. Persistent U/W ISR >70 days defaults to a large diameter. Are we open to other solution sets which meet the requirements?

Although, the Navy is committed to the development of a large diameter UUV, we will keep an eye open to other options from a family of systems perspective. As other mission requirements outside of those for the LDUUV are created, smaller UUVs may be an appropriate complement to the UUV family of systems.

40. Will MRUAS, BAMS, and UCLASS be capable of performing the EP-3 COMINT mission with linguist operators?

Navy has not yet defined the Line of Sight (LOS) and Beyond Line of Sight (BLOS) SIGINT capabilities for MRUAS, BAMS, and UCLASS vehicles.

41. We recently had a Fire Scout go rogue and violate Washington, DC airspace. What kinds of margin for error can and will be tolerated for UCLASS coming aboard a flight deck manned with U.S. sailors?

Any unmanned vehicles coming aboard an aircraft carrier will meet the safety criteria described in our Naval Air Training and Operating Procedures Standardization (NATOPS) program which prescribes general flight and operating instructions and procedures. Any unmanned vehicles brought aboard an aircraft carrier will not add any more risk to flight deck personnel than currently accepted with manned aircraft.

42. What areas are being looked at with regards to digital radio and peer to peer communications?

Navy is currently exploring the implementation of several mobile ad-hoc networking (MANET) radio waveforms to enable networked communication at the tactical edge. Our current focus has been to follow the Joint Aerial Layer Network (JALN) Analysis of Alternatives (AoA), which is evaluating multiple levels of networked radio requirements for the joint force. The Navy has been working to support the development of multiple waveforms to support this activity; such as Sea Lancet, Tactical Targeting NetWORK Technology (TTNT), Advance Networking Waveform (ANW), MAINGATE, Highband Network Waveform (HNW), 802.11x, 802.16x and enhancement to our current family of Link-16, CEC and CDL networks. Once the additional analysis is completed, the Navy will then look at implementing these waveforms in one the myriad digital radios we currently have planned or in a new system depending on operational environment.

43. Where does the Navy plan to draw the line for LDUUV acquisition? Develop requirement s around commonality and issue RFP or Navy labs run the program as the system integrator, build prototypes, then release RFPs for essentially build-to-print for piece parts.

N2/N6, NAVSEA, and ONR are cooperating closely on ONR's LDUUV INP to streamline the development process and introduce an LDUUV capability to the Fleet in the earliest possible timeframe. The team is paralleling ONR's energy and systems development with other essential efforts for the program of record. The intention is that the end-stage vehicles from the INP be as close to a build-to-print capability as is possible, leading to a minimal time lag between INP vehicle delivery and successful Milestone B approval.

44. We've heard "No new sensors for maritime ISR until endurance and power are solved for UUVs." Today, VADM Dorsett mentioned ONR investments in new sensors. If true, what phenomenology are you exploring?

N2/N6 is currently focused on the LDUUV INP which will develop UUV Power and Energy; other necessary subsystems for the required level of LDUUV vehicle autonomy and reliability are being looked into from a planning perspective but are well back in terms of priority of effort. There are sensors incorporated as part of the INP vehicle development, however, ISR or other LDUUV payload sensors are

not the initial focus of the INP. That said, the LDUUV will be designed for modular payload packages which will undoubtedly be a focus of various resource sponsors who wish to leverage LDUUV.

45. Last year's Naval Research Advisory Committee study for ASN RDA identified C2 of Unmanned and Manned Systems as an area which is deficient, lacks ownership, and needs significant S&T and R&D investment. What is the Navy doing to get to a universal or common control system for unmanned vehicles?

Navy is working for a common control systems for all unmanned vehicles. Navy is participating with the other services and other DoD agencies (OSD ATL, USA, USAF, USMC, USCG) to develop an interoperable system for controlling unmanned vehicles. Common standards for communication waveforms and planning systems software are essential elements of any common control architecture; this message has been sent consistently to all industry partners.

46. What is the status of the Navy EP-X program?

Navy cancelled EP-3E replacement (EP-X) in PB11 and is currently developing a "Family of Systems" concept to recapitalize airborne Intelligence, Surveillance and Reconnaissance (ISR) capabilities within existing programs of record. FY11 Defense Intelligence Guidance (DIG) and National Defense Authorization Act prohibit the Navy from retiring the EP-3E airframe until the capability is fully recapitalized. Twelve of the sixteen aircraft are funded for airframe sustainment with Special Structural Inspection-Kits (SSI-Ks) and Outer Wing Assemblies (OWAs) which should allow them to continue flying in support of the COCOMs until 2020 if necessary. This year, these aircraft will also start receiving the Joint Common Configuration (JCC) Spiral 3 upgrades to replace obsolescent SIGINT equipment.

47. What is happening with Common Control Station and coordination with the USAF?

BAMS UAS continues to pursue the Common Ground Station (CGS) efforts with the USAF Global Hawk (GH) program. We are developing a Joint Statement of Work to execute the next iteration of the BAMS UAS/GH CGS development. Initial efforts are already underway as part of the USAF GH Ground Station Re-Architecture contract vehicle. The Jointly developed Statement of Work supports the next phase of activities which was going to leverage the BAMS UAS contract vehicle. See answers 54 and 57 for additional information.

48. What has the Navy done with other services to eliminate UAS procurement redundancy?

The Navy participates in cross service efforts such as the Unmanned Air System (UAS) Task Force to identify and capitalize on potential synergies and efficiencies whenever possible, as well as develop common UAS interoperability standards to be used by all Services. A recent example would be the Common Control Station (CCS) initiative that aims to produce a non-proprietary, scalable, open-architecture, solution for Unmanned Air Systems, to facilitate system interoperability, usability, and commonality, and to reduce development and sustainment costs. The Navy recognizes that different UAS missions often require different system capabilities which drive differences in UAS payloads/sensors/weapons, etc. Despite those unique missions and capabilities, the Navy evaluates other service UAS solutions as part of the system Analysis of Alternatives (AoA) and system preliminary design reviews. Examples include Raven and RQ-7 Shadow procured from the Army.

49. Why did the Navy want to divest itself of the Reaper?

The Navy did not intend to transition the Reaper project to a program of record (POR). Through the use of established USAF MQ-9 contracts, that demonstration has achieved the objectives and lessons learned will be integrated into future POR's. It does not fit Navy's the "From the Sea" ISR model as it is land based and modifications for ship board launch and recovery operations would be very difficult and expensive.

50. How are we working solutions for Power and Endurance for UUVs?

ONR is leading power and energy technology development with an industry day last month and a Broad Area Announcement (BAA) coming out soon. Better energy density is not the only solution and we are looking at the entire vehicle and mission to see where we can gain efficiencies: sensor power, hotel load, CONOPS, etc. See question 53 and 60 for additional information.

51. After power and energy, what are the other key challenges that need to be addressed for UUV's?

Reliability and autonomy are two other key challenge areas for the LDUUV. To operate effectively for this amount of time, it needs to be robust against failure and able to safely operate in the open ocean without focused operator attention. That means LDUUV must have mission relevant autonomy to conduct obstacle avoidance, operate under a water space management scheme as necessary and complete its mission in a dynamic environment.

52. How are you going to ensure competition for UCLASS and MRUAV?

MRMUAS and UCLASS will promote competition through in-depth communication of requirements during dedicated industry day forums and Request for Information (RFI) cycles, and through substantial investments in trade study and system prototyping contract opportunities with multiple vendors.

53. How quickly does the Navy want to field MRMUAS capabilities?

The Navy wants to field an MRMUAS Limited Operational Capability as early as FY16. This includes potentially operating the system using a GOCO model until the Navy establishes organic operations and support capacity. The Navy will use the upcoming MRMUAS AoA phase to better assess industry's current capacity to rapidly field technically mature, reliable, and marinized systems.

54. UCLASS / UCAS-D status and difference?

The Navy Unmanned Combat Air System Demonstration (UCAS-D) continues to develop and demonstrate aviation / ship integration capabilities that will be required for the Unmanned Carrier Launched Airborne Surveillance and Strike (UCLASS) system. The first of two UCAS-D's X-47B air vehicles completed its first flight on 04 February 2011. The X-47B is scheduled to demonstrate launch and recovery operations aboard an aircraft carrier in 2013.

The Unmanned Carrier Launched Airborne Surveillance and Strike (UCLASS) program is currently conducting pre milestone A activities. The Initial Capabilities Document (ICD) is in final Navy staffing and will be reviewed by the other Services and Joint Staff prior to final validation. The document provides a

top level description of capabilities associated with persistent sea-based Intelligence, Surveillance, and Reconnaissance (ISR) with precision strike.

The ship integration, communications architectures, and control (including launch and recovery) systems developed and demonstrated for UCAS-D are the baseline upon which UCLASS will build. UCLASS will utilize sensor, communication, command and control, and weapon systems that have already been tested and fielded in order to minimize schedule risk with a goal of delivering the initial UCLASS capability in the 2018 timeframe.

Panel:

55. How do you synchronize and integrate your Info Dominance Enterprise from * to capability design to resourcing to acquisition to ops to sustainment?**

The synchronization and integration process is part and parcel of the entire Joint Capabilities Integration and Development System (JCIDS) process. JCIDS is also a key supporting process for DOD acquisition and Planning, Programming, Budgeting, and Execution (PPBE) processes. The primary objective of the JCIDS process is to ensure the capabilities required by the joint warfighter are identified with their associated operational performance criteria in order to successfully execute the missions assigned. This is done through an open process that provides the JROC the information they need to make decisions on required capabilities. The JCIDS process supports the acquisition process by identifying and assessing capability needs and associated performance criteria to be used as a basis for acquiring the right capabilities, including the right systems. The capability needs then serve as the basis for the development and production of systems to fill those needs. Additionally, it provides the PPBE process with affordability advice by assessing the development and production lifecycle cost. These lifecycle costs include the acquisition, operation, and sustainment portions of the overall Total Ownership Cost (TOC) for a given program. Synchronization and integration are performed at every step along the way from cradle-to-grave.

56. Does “consolidation” and “commonality” increase vulnerability to physical or cyber attack?

The short answer is ‘yes’. Consolidation and commonality of our networks, and the growing dependence on Commercial-off-the-Shelf technology remains a dual edged sword. There is a growing body of thought that suggests homogenizing our networks may actually increase our vulnerability. That

said, we can no longer afford the federated model that served us well throughout the 1960s and 70s. The trick is to carefully balance vigilant network security against our growing demand for data flow at ever increasing speeds – with fewer people and at consolidated locations. These problems are being carefully weighed by the various entities, both within and outside of N2N6, responsible for providing the policy, systems and security for Navy's highly net-centric platforms and capabilities.

Any increase in vulnerabilities associated with the "consolidation" and "commonality" of a system are far outweighed by the benefits achieved. In an environment with constantly changing threat, the most important characteristic of a defendable system is its agility and ability to address new threats. Standardization in a tightly configured system limits the threat vectors and allows for the building of a defense-in-depth against known vulnerabilities while supporting the ability to quickly design and implement defenses to address new threats.

57. Other warfare areas have established "Warfare Centers of Excellence" have you considered the establishment of an "Information Dominance Center of Excellence" for this warfare area? If so, where would it exist and how can industry partner with the COE? C1

The Information Dominance Center for Excellence at NPS in Monterey is an overarching Center intended to ensure relevant graduate education and support research along with delivering our Senior Leaders professional development courses. Other Centers such as the Electronic Warfare Center, Center of Excellence of IO (NIOC Norfolk) and out Meteorology Professional Development Center in Gulfport MS are examples of Fleet focused Centers.

Connecting the key centers, functions and contributions of the key elements among Information Dominance organizations may not lend itself to a singular center but rather more a lead center that integrates and synchronizes the efforts. We do seek a better overarching construct that addresses concept development, operational excellence and professional development centers and welcome industry inputs as to how best to form an overarching construct to include industry.

58. What are the key engineering disciplines (software, electrical, etc) to ensure the achievement of the Navy's vision for information dominance? What are your plans to ensure sufficient capability in these disciplines?

One of our fundamental shortfalls today is Operations Research professionals and the Naval Postgraduate School has added some focus in this area. However, all types of engineering disciplines are necessary for the achievement and success of N2/N6.

59. Are the system commands and PEOs and their "spiderweb" of technical authorities helping the Navy achieve its Information Dominance vision? Are there technical areas for which "technical authority" for the Navy is either not robust or non-existent?

The technical authority "spiderweb" has been focused on the current Navy technical approach; however, we still have fundamental short falls in the OPS RESEARCH and SYSTEMS of SYSTEMS ENGINEERING disciplines. During the process of integrating programs in N2/N6 we have discovered gaps in our cross-SYSCOM requirements analysis and systems engineering. However, this is also present in industry as traditional technical domains have driven by past SYSCOM/PROGRAM alignments, thus creating profit driven technology gaps across several companies.

60. When and how will CANES architecture be disclosed or become public info?

The CANES system design/architecture will be part of the CANES Full Deployment Request for Proposal (RFP). The current schedule reflects RFP release in Q3FY12.

61. How do you see the recent Navy-Air Force Air/Sea strategy agreement affect your networking and IT plans?

The Information Dominance Roadmaps are very much focused on realizing the same Warfighting capabilities and efficiencies that will support Air/Sea Battle concepts. The Information Dominance Roadmaps will deliver capabilities that support Warfighting needs in benign, degraded and denied operating environments.

The Convergence to a Single Network (CSN) Roadmap specifically addresses the potential interoperability of Navy and Air Force networks with a set of game-changing actions designed to achieve an integrated network and communications environment that will enable users (DOD, Federal, Allied, Coalition and Non-Governmental Organization partners) to: 1) seamlessly access and share classified and unclassified information globally; 2) operate in all environments, supported by common services, standard interfaces and authoritative governance; 3) provide secure information exchange with minimum barriers for operational efficiency and mission success; and 4) readily share data and information. The CSN Roadmap will help the Navy move from a platform-centric to a net-centric environment, where all platforms (manned and unmanned) can access and extend the Global Information Grid (GIG).

The CSN Roadmap also includes actions to improve network operations and management and to standardize data and information-sharing protocols that will support integration with Air Force operations centers.

62. How do you plan to align gap analysis from Info Dominance roadmap work with the CNO Interoperability and Integration Summit kill chain efforts? How will those gaps inform investment decisions?

CNO and his staff have insight into all of our roadmaps, and they are a tool that is being applied by the staff in all appropriate cases.

63. In order to establish Enterprise software licensing agreements the Navy must first know what software it owns. Industry determines this with automated discovery and asset management software solutions. When does the Navy plan to invest in these types of technologies to allow it to get to the quick wins that will come from enterprise wide software licensing?

The Department of the Navy (DON) is actively working to identify and execute an enterprise solution for IT Asset Management (ITAM). The USMC is serving as the DON Lead Integrator for Enterprise Software Licensing (ESL) under the DON CIO IT Efficiency Initiative for Enterprise Software Licensing (ESL), and is responsible for identifying and establishing enterprise-wide DON ITAM and IT Service Management (ITSM) tools and procedures in FY 2011. The USMC has fielded BelManage (BelArc, Inc.) and Navy is looking to leverage existing enterprise licenses for the same product.

64. Is the Navy going to invest in the JTRS program? I understand the Navy is buying DMRs?

Navy has committed to procure radios from the Airborne, Maritime/Fixed Site (AMF); Handheld, Manpack, Small Form Fit (HMS); and Multifunctional Information Distribution System-JTRS (MIDS-J) programs. AMF will provide the Navy's standard shipboard, submarine and shore terminal for MUOS. HMS will provide MUOS capability to Navy ground units of the Naval Expeditionary Combat Command (NECC) as well as for shipboard emergency MUOS communications capability. MIDS-J is being integrated onto the F/A-18E/F to provide Link-16, Tactical Air Navigation (TACAN), and J-Voice, and to serve as the platform for the future Joint Aerial Network to the Tactical Edge (JAN-TE) waveform.

65. How would you define the difference between electronic warfare and cyber warfare and what are the key challenges to merge them together?

Some have argued that the difference between electronic and cyber warfare is that EW is targeted at hardware and cyber is targeted at software/information. Regardless, both enable network operations as well as facilitating our ability to defend and attack in the information battle space. In actuality we are seeing less of a distinction between the two warfare areas and more of a convergence in their overall effects. Yes there are technical/tactical differences between the employments of the two, but in an operational sense, their individual and integrated usage simply allows for many more vectors to achieve the same desired non-kinetic effects.

The key challenge to merging them together is to overcome the idea that cyberspace is simply a network and therefore can only be attacked via the network. The electromagnetic spectrum is the foundation of cyberspace as well as the realm of EW. EW, as well as cyber warfare, can contribute to the success of operations by using offensive and defensive tactics and techniques in a variety of combinations to shape, disrupt, and exploit adversarial use of the EM spectrum while at the same time protecting friendly freedom of action in that spectrum. Our Electronic and Cyber Warfare Division is capitalizing on this idea as we mature our thinking and developmental efforts with stakeholders across the Navy and throughout DoD.

66. What about HUMINT? What are we, the Navy, doing to increase our Human Intelligence collection capabilities?

The Navy HUMINT force of over 350 trained HUMINTers continues to find success at the Military Source Operations (MSO) Cat III level and continues to explore ways to expand its MSO CAT II/I capability. The Enterprise mission is being met by established collection platforms within the Expeditionary and Special Warfare components as well as service level collection conducted by other Navy elements. Fleet N2X positions are established at major staffs and selected Numbered Fleets. Navy HUMINT Teams (NHTs) continue to support and have received accolades for their efforts at Joint Operating Base – Afghanistan (JOB-A).

Navy launched a pilot FORMICA training course in December 2010 and continues developing a plan for a baseline FORMICA capability to ensure Navy intelligence professionals, including operational and independent duty intelligence specialists supporting the Fleet as well as Expeditionary and Navy Special Warfare elements are able to debrief and report in a timely manner in accordance with DoD instructions.

Additionally, Navy continues to support the Enterprise with instructors at FTC and HT-JCOE. Navy will also provide the Commanding Officer for HT-JCOE East when it stands up.

67. Is the Navy looking at "Open Source" Intel, i.e. Real World ship track data on Google Earth; Twitter data; Facebook; and Flickr? Are we putting resources to analyze this information?

Yes, the Navy is looking at all available, relevant information to incorporate into all-source analysis, in accordance with applicable policies. The increasing volume of collection (to include open source) continues to pose a significant challenge; we are working closely with other Intelligence Community elements to improve the management of this information.

68. GEOINT Info Data: No reflection of Marine Forces (MARFOR), maybe implied, but operationally there is a requirement for interoperability. Is the Marine Corps a partner in development of C4 architecture?

The Marine Corps is a partner in the development of C4 architecture. They are currently involved in the development of the Joint Command and Control (JC2) Analysis of Alternatives (AoA). JC2 is the way-ahead post Global Command and Control System Family of Systems (GCCS-FoS). They also participate in Saturday Sessions with the VCJCS, where C4 architectures are frequently discussed. In addition, the Marines have participated in semi-annual plan build conferences where discussions of future C4 architecture take place.

69. How is the Navy looking to balance investment in C4ISR mission capabilities in Networks/Comms/Cloud, etc. with ashore enterprise network investments, i.e. NGEN? Where do you see promising opportunities for reducing infrastructure costs? Joint, national agency partnerships? Commercial/gov't cloud services, etc?

In the near-term 2017 architecture, consolidation will start with the CANES program to establish a Common Computing Environment (CCE), a single infrastructure with Cross Domain Solutions (CDS), increased systems management for visibility and control, and inherent security controls for the entire C4I infrastructure and hosted applications. NGEN will be transitioning capabilities from NMCI to the future vendors of NGEN segment contracts, with new capability insertion commencing with technical refresh opportunities. Solutions meeting functional requirements (user mobility, leveraging cloud and thin client alternatives, improved cybersecurity features, and efficiencies in total ownership costs) are desired. Joint or Federal solutions that satisfy requirements and lower total cost of ownership will be considered.

70. Could you articulate how the DOD/DISA cloud, Navy cloud, and Navy NGEN will be implemented? Do the services have a unified vision? Is it information sharing or hosting?

Navy's Consolidated Afloat Networks Enterprise Services (CANES) Common Computing Environment is envisioned to be a private cloud on each ship, and is the first general Navy cloud for application migration. The Common Computing Environment will provide infrastructure as a service, eliminating the need for each shipboard system to have its own hardware. The future networking

environment will bridge network gaps and seams to facilitate secure interoperability among existing networks and influence future development. Interoperability of network activities, functions, and services across traditional Navy, DOD, and Coalition COIs will enable expanded situational awareness and increased access to worldwide resources to develop the operational picture. Next Generation Enterprise Network (NGEN) will initially focus on providing similar capabilities that were delivered under the Navy Marine Corps Intranet (NMCI) contract, to include leveraging thin client and cloud computing opportunities presented by industry and/or offered by DISA and other DoD services.

71. PED has been referred to throughout the day. DCGS-N has been mentioned. Can you provide specifics about DCGC-N? DIB vs. Brain Approach? Investment Plan? Who owns DCGS-N?

DCGS-N Increment 1 has two primary baselines associated with it. DCGS-N Increment 1 Block 1 is focused on low-risk Intelligence, Surveillance, Reconnaissance, and Targeting (ISR&T) support capabilities within the Common Computing Environment (CCE). Additionally, Block 1 Early Adopters Engineering Change Proposal (EA ECP) further aligned Block 1 with the PMW 160 Consolidated Afloat Networks and Enterprise Services (CANES) Early Adopter CCE. Block 2 has minor capability enhancements to transition functionality and leverage additional CCE/Core Enterprise Services (CES). Prototyping and experimentation will demonstrate and mature new capabilities and select best-of-breed solutions prior to insertion into a given baseline. DCGS-N Increment 1 received Full Deployment authorization in April 2010, and the Program anticipates achieving Full Deployment across its Total Inventory Objective in FY14.

DCGS-N Increment 1 Block 1 provides imagery intelligence (IMINT), geospatial intelligence (GEOINT), and signals intelligence (SIGINT) data; it produces and automates workflows/mission processes on Multi-Function Workstations. Block 1 provides an initial enterprise-wide data sharing capability via shore-side reachback. The desired Joint DCGS Enterprise capabilities are realized as additional DCGS nodes are brought on-line, inter-Service DCGS Integration Backbone (DIB) Enterprise services are added and inter-Service security accreditations mature. These capabilities enhance intelligence support to the development and execution of strike and fires missions, and enhance the timeliness and accuracy of ISR&T support to the full spectrum of Naval and Joint operations. In addition, Block 1 accesses, posts, and stores ISR&T data and products to allow publish-and-subscribe discovery of and access to data quickly across the Joint Enterprise using the DIB.

DCGS-N Increment 1 Block 1 EA ECP features a smaller footprint, reducing the total number of racks from three to one, depending on the CANES Early Adopter network available on each platform. Block 1 EA ECP builds on Block 1 and provides additional capability to the Fleet, including imagery and targeting enhancements using the Graphical Exploitation Reporting Tool (GERT) as well as improved Signals Intelligence (SIGINT) applications using widgets through the Ozone Widget Framework. The Block 1 EA ECP system is scheduled to field aboard USS BONHOMME RICHARD (LHD 6) in Spring 2011.

DCGS-N Increment 1 Block 2 will feature additional functional enhancements, expanding on initial DCGS-N Block 1 capabilities. Block 2 design will begin in FY11. Block 2 will continue to rely on a reachback capability enabled by the DIB and existing communication networks, and take advantage of evolving Maritime ISR Enterprise partnership efforts with the Office of Naval Intelligence. Interoperability within the joint enterprise will be enhanced by incorporating DIB 1.3 standards. This system will be installed on Aircraft Carriers and Large Deck Amphibious Ships.

DCGS-N will have completed full deployment of Increment 1 capabilities across its Total Inventory Objective by FY14. ISR&T performance and capability software upgrades are planned for every two years. These upgrades will include the integration of new sensors and additional operational workflows to enable evolving Navy and Joint DCGS Enterprise CONOPS. The DCGS-N program will leverage existing experimentation processes to foster development of new capabilities.

DIB vs. Brain Approach?

The DCGS Integration Backbone (DIB) is governed by USD(I) and is utilized across all DCGS Family of System programs. It provides a common set of services and standards to facilitate sharing intelligence, surveillance and reconnaissance information across the enterprise. DCGS-N Increment 1 is using DIB 1.3.1 with its next major baseline. The Army's "Brain" solution utilizes the DIB and the latest Google/Hadoop DFS/MySQL, Open Standards. DCGS-N has integrated the DIB in support of USD(I) mandates and, as DI2E and other frameworks mature, the Navy will continue to evolve along with them. The "Brain" is but one of many alternatives that exist. The DCGS-N engineering team is continuously reviewing the appropriate technological capabilities in conjunction with our cost and schedule constraints to meet our "next generation" fielding solutions.

Investment Plan?

The Navy's ISR investment strategy is part of the overall Navy budget and innovative solutions to the Navy's ISR problems may be procured in the future. Investment is currently focused on understanding the Navy's Tasking, Collection, Processing, Exploitation and Dissemination (TCPED) "challenge" and developing a proposed architecture that will posture the Navy for meeting the FY16 tipping point, or explosion of sensor data. The TCPED Study being conducted through PMW 120 and OPNAV will hopefully illuminate the areas where the Navy needs to focus future investment.

Who owns DCGS-N?

From a resourcing perspective, it is OPNAV N2/N6 - the Navy's resource sponsor for DCGS-N. From an Acquisition Community perspective, DCGS-N's Milestone Decision Authority is Assistant Secretary of Defense (Network and Information Integration) (ASD(NII)). From an operational perspective, our requirements are generated within the DCGS-N Requirements Working Group (DRWG) led by NAVCYBERFOR personnel, with critical participation from COMTENTHFLT personnel, OPNAV, Center for Naval Intelligence, USFFC and others. These operational requirements are ultimately vetted via the Joint Capabilities Integration and Development System (JCIDS) process up to the Joint Requirements Oversight Council (JROC).

72. What are the Navy's plans for upgrading or replacing DCGS-N?

DCGS- N Increment 2 is the Navy's primary Intelligence, Surveillance, Reconnaissance, and Targeting (ISR&T) and Multi-Intelligence Fusion and Analysis (FA) capability for the future. It will build upon the capabilities provided by DCGS-N Increment 1 and Maritime Domain Awareness (MDA) Spiral 1 and converge afloat and ashore ISR into an integrated Information Dominance enterprise. DCGS-N Increment 2 will provide the capability to exploit the Navy's tremendous investment in ISR platforms over the next 10 years and provide this data beyond the immediate sensor readout. Increment 2 will provide significant capability to satisfy the Navy's Tasking, Collection, Processing, Exploitation, and Dissemination (TCPED) strategy. DCGS-N Increment 2 will support evolving fleet needs through early and frequent delivery of enhanced enterprise capabilities starting in 2014, to include reachback, access to additional sensors, and an ISR storefront with modular tools (e.g. widgets). It will leverage joint and national infrastructure efforts to ensure Navy's joint C4ISR interoperability. It will be software-based

within CANES (afloat) and the ONI Enterprise Architecture (enterprise node), incorporate MDA/MFAS capabilities, and process, exploit, analyze, and disseminate multiple types of intelligence data from the Navy's new ISR tactical sensor platforms.

DCGS-N Increment 2 will greatly improve the Navy's ability to: 1) detect and identify maritime threats, 2) fuse National, Tactical and inter-theater data for operational use, and 3) Allow better DCGS Family of Systems (FoS) and Intelligence Community (IC) visibility into maritime collection requirements.

DCGS-N Increment 2 development will begin in FY13. Capability fielding will commence in FY14 and run through FY17. The current plan is for DCGS-N Increment 2 capabilities to be fielded at the Office of Naval Intelligence, Maritime Operations Centers ashore and afloat, and on 23 Force-level ships.

73. Is the current DCGS configuration (or upgrade there to) adequate to handle UAS sensor data post BAMS IOC?

In short, yes. To date, DCGS-N Increment 1 has demonstrated interoperability with BAMS-D. Additionally, PMW 120 has met with the BAMS Program Office and operational community to discuss the BAMS Concept of Operations and strategy for storing and distributing BAMS data, including the current limitations of DCGS-N systems. A key requirement of DCGS-N Increment 2 will be to provide a system that will be capable of handling the explosion of sensor data that will be available in the post BAMS IOC timeframe. The first upgrade to this system (Block 2) will be able to partially fulfill these requirements but it is anticipated that all of the BAMS (and follow-on) platform sensors will be "processed" by the next generation of DCGS-N which will be DCGS-N Increment 2.

74. Is there a "Joint" plan for DCGS? i.e., a "seamless" system across Navy, USAF, Army?

Currently, USD(I) is looking at a program called Defense Intelligence Information Enterprise (D2IE) to provide a common framework for hosting a wide variety of analytical tools, including GEOINT, SIGINT, HUMINT, OSINT and other applications. DI2E will allow the services to build in a collaborative environment, demonstrate, test and share a common framework in order to prove the benefit and identify future cost avoidance for the Service DCGS programs and other enterprise initiatives. There is no plan to replace the Service-specific program of records DCGS systems.

75. With more data sharing and updates to capabilities "on the fly" there will be more potential for system crashes or enemy IW. Is the Navy looking at secure/assure processing as well as comms? Also,

are there protections being added as more processing and data is moved forward to protect against losses?

For several years, the Navy has operated with a conglomeration of individual systems aboard its platforms or shore commands. We have been working to increase interoperability and realize efficiencies in an effort to reduce the cost of these systems and make better use of available resources. We started with sharing data among individual systems at the platforms and commands, and continue to strive to adopt more of an application-store construct that leverages a common infrastructure throughout the Navy. A major enabling step to achieve this objective is the establishment of the Consolidated Afloat Network Enterprise Services (CANES) program. We have been executing risk reduction efforts in this area with the introduction of the Common Computing Environment (CCE), and the installation of core applications as software-only on this common infrastructure. A continuing challenge that we face is that, over the years, each ship and each shore command has become its own unique operating environment with a mixture of capabilities and infrastructures. We are working to standardize those environments and applications, which will enable increased confidence in our ability to leverage remote updating technologies from trusted data repositories using the assured communications paths that we have in place as well as those that are planned for the future. In addition to that, the Navy's C4I community is implementing an Application Integration Framework (AIF) that will facilitate the abstraction of discreet capability packages from the core capability, further enabling enhanced capabilities to be developed and rapidly fielded without the traditional risks of bringing the entire core capability crashing down. The abstraction construct enables the core to be updated as well as any individual enhanced capability "plug-in" asynchronously since it will be based on standards that will not change between the two. This increases the flexibility our acquisition teams have to rapidly introduce capabilities without triggering a full regression and operational test that would delay capability introduction by several years.

The Navy operational environment is not that different than our sister Services. All of us have the challenge of connecting capabilities to and from our "edge" users. The technologies being employed today put the capabilities locally on the edge platforms (e.g., ships), and leverage smart synchronization technologies to ensure that the data being provided to those users and from them are complete and accurate. We can't rely on the amount of bandwidth required to constantly synchronize entire databases, so we have adopted an encrypted, "changes only" approach that recognizes the limitations of on/off-ship communications pipes. In the future, we intend to further reduce the application

footprint required on the local platform, since we recognize that different platforms require different applications to support the accomplishment of their mission. We intend to leverage the Defense Enterprise Computing Center (DECC) infrastructure that the DoD has implemented, and the Service Level Agreements that are available with these robust nodes. This will enable us to further streamline the installation process and take more advantage of "reachback" capabilities with assured administration for the computing required to run the various courses of action our Commanders need to make informed decisions.

76. There has been much discussion about interoperable comms, standards, common interfaces, etc. Additionally, it was stated earlier that systems must be designed so that software can be designed to be updated "on the fly." All of these things increase your exposure to cyber attack. What are you doing to secure those systems from that threat vector?

The Navy has embraced the adoption of Host-Based Security Systems (HBSS), which will guard against unauthorized ports/protocols/IP addresses exploiting the dependence we have on the network. In addition to HBSS, we are keeping a close eye on keeping our environments up to the latest compliance with Information Assurance Vulnerability Advisories and Messages (IAVA/IAVM). The Navy takes its network security extremely seriously, understanding that the Commanders depend upon that connection and the data operating on it to make the best decisions about commanding their forces and controlling their engagements.

77. The President's FY12 budget reflects over $60M RDTE to continue CANES development and demonstration, contractor integration testing, and proposals submission by the two competitors. With FY11 CR shorted the program by 30%, what will OPNAV N2N6 do to field CANES on time?

OPNAV N2N6, working closely with the CANES Program Office is taking corrective action to mitigate programmatic impacts from the FY11 CR and minimize impact to a Down-Select in FY11 and Limited Fielding in FY12.

78. Where is NGEN? Last year, it was the superset of all navy networks (admin and tactical). Is the Navy confused about how the networks converge (CSN)?

Initially, we will focus our efforts on aligning programs, to include transitioning from NMCI to the Next Generation Enterprise Network (NGEN), OCONUS Navy Enterprise Network (ONE-NET), and Consolidated Afloat Networks and Enterprise Services (CANES). Ultimately, we will establish a seamless environment between the afloat and ashore environments.

79. What is the N2N6 plan for mission planning systems like JMPS?

The Joint Mission Planning System - Maritime (JMPS-M) Operational Requirements Document (ORD) of 15 Jun 2003 doesn't clearly address Unmanned Air Vehicle (UAV) and Unmanned Aviation System (UAS) requirements, platforms or missions. While the JMPS-M Integrated Master Schedule (IMS) notes Broad Area Maritime Surveillance (BAMS)/MQ-4 efforts to develop a Mission Planning Environment (MPE) on JMPS-M, no other UAV/UAS is currently planning to utilize JMPS-M. JMPS is, however, the accepted path forward for mission planning for Naval Aviation platforms. As such, where it makes financial and operational sense, UAS platforms will be investigated for migration to JMPS.

80. How is the Navy (N2/N6) utilizing the Joint Information Operations Range (JIOR), specifically as you move forward with Information Dominance? Are you planning to utilize the "range close loop model?" For example the question posed on "How do you operate in a degraded satellite operations contingency?" do you tie in your wargaming facility with the Joint IO Range?

This question is an operational issue that falls under the scope of NETWARCOM and C10F. Navy uses the JIOR to support training, and test and evaluation (T&E) evolutions. Designed to improve carrier strike group staff familiarity and integration of organic submarine assets, Fleet Synthetic Training-Joint (FST-J) exercises use the JIOR to integrate cryptologic direct support elements (CDSE), located at Navy Information Operations Commands (NIOCs), into staff planning and operations. CDSE operators receive hands-on signal analysis training while conducting identification and reporting of SIGINT emitters to the strike group staff and FST-J exercise evaluators.

Using the close loop model, Navy conducted several proof-of-concept tests designed to provide remote connection capability at various classification levels. As a result, CDSE personnel at NIOC Hawaii were able to use the JIOR for remoted, pre-deployment training on CLUSTER SNOOP and CLASSIC TROLL

(submarine collection) systems located in Damneck, VA, without incurring travel costs. Future enhancements will bring a persistent training environment to other NIOCs desiring/needing remote control capability. This capability will also provide Center for Information Dominance Learning Sites an avenue to conduct further individual and functional training. The Navy is also investigating use of the JIOR for computer network operations capability development and training.

81. ADM Dorsett indicated that the only real plus up to the Cyber area is manpower. Doesn't that concern you? What other steps can you talk about to defend the NIPRNET and SIPRNET? What kinds of capabilities do you need from industry to better defend the networks and mitigate the need for additional manpower?

The Navy has made significant investments in Computer Network Defense capabilities across the DOTMLPF spectrum for both NIPRNET and SIPRNET. Our implementation includes a number of Defense-in-Depth products and services that require sufficient investment in manpower to ensure the availability of qualified people for an increasing range of Information Dominance operations. Industry can assist the Navy by providing additional capabilities in the area of situational awareness and continuous monitoring via tools that will reduce manpower by collecting, processing, and disseminating IA sensor data to decision makers in a more effective an efficient manner. These include, but are not limited to, additional capabilities in the area of automated correlation, visualization, reporting, anomaly detection, vulnerability detection/remediation, and configuration management for tactical networks, which are necessary to reduce our current manpower requirements and enable the warfighter to provide a wider range of cyber operations.

82. How is the Navy interacting with and leveraging the USD(I) ISR Task Force? Is the ISR Task Force interested in afloat and underwater manned vehicles?

OPNAV N2/N6 is a member of the USD(I) ISR Task Force and is coordinating ISR development efforts. Currently, mission needs are air and land focused to support service personnel on the ground, but afloat and underwater unmanned vehicles are avenues we expect to pursue as mission requirements evolve.