My Other Combat System is a Network

### Inside This Issue

Congratulations 1

IA Scholarship Program Nominations Call 1

My Other Combat System is a Network 2

Should the IDC Stay RL? 6

FY14Active Duty LDO/CWO 8

FY14 Reserve LDO/CWO 9

Online Reading Room 11

IP-Related Schools 12

Points of Contact Information 20

Regional IP Captain Contact Information 21

SEP 2012

Congratulations

Capt. David H. Lepard, force weapons officer for Commander Naval Air Forces, passed the Senior Limited Duty Officer Silver Eagle and Horse Shoe award to **Capt. Gerry Slevin** from Commander Defense Information Systems Agency, Special Operations Command, during Lepard's retirement ceremony aboard the aircraft carrier USS Carl Vinson (CVN 70) Sept. 14.

The Silver Eagle and Horse Shoe award is held by the most senior Limited Duty Officer (LDO) in the Navy, and is passed down to the next most senior individual at the conclusion of the current Silver Eagle's active service.

The Silver Eagle award began in 2002 and was first presented to Capt. Merril Carlton Albury. Lepard received the trophy in May 2010.

Lepard stated he has confidence in his Silver Eagle successor, who has already worked to give LDOs a positive image with other branches of service during his own career. "He will carry on with fine tradition and display it proudly," said Lepard.

<http://www.navy.mil/submit/display.asp?story_id=69585>

IA Scholarship Program Nominations

N2/N6 is excited to announce a dedicated full-time quota for the Information Assurance Scholarship Program (IASP). The IASP is designed to develop and retain a highly trained cadre of professionals to support the DoD’s Information Technology requirements for warfighting and the security of Information infrastructure. The quota is available to any qualified IDC Officer who wishes to pursue a full time graduate education opportunity in a relevant academic discipline.

Relevant academic disciplines and programs of study supported under the IASP include, but are not limited to: Biometrics, Business Management or Administration, Computer Crime Investigations, Computer Engineering, Computer Programming, Computer Science, Computer Systems Analysis, Cyber Operations, Cybersecurity, Database Administration, Data Management, Digital and Multimedia Forensics, Electrical Engineering, Electronics Engineering, Information Security (Assurance), Information Systems, Mathematics, Network Management/Operations, Software Engineering, and similar disciplines as approved by the DoD Chief Information Officer (DoD CIO).

Participants have three options for degree completion. The first is to begin at the National Defense University Information Resources Management College (NDU iCollege) full-time or part-time and subsequently attend one of the NDU iCollege partner universities (some offer graduate degrees online). There is no limit on the number of part-time participants, but N2/N6 has one full-time quota approved. The second option is to complete the entire program full-time in residence at the Naval Postgraduate School (NPS). The third option is to complete the entire program full-time in residence at the Air Force Institute of Technology (AFIT). More information on the partner universities is located [here](http://www.ndu.edu/icollege/network/ntwk_list1.html).

Participants must maintain good standing in their degree programs and upon completion, continue in service as military members, or repay the costs of the program. Full-time participants will obligate themselves to serve on active duty for a period three times the length of education through the first year and one month for each month thereafter.

All active duty navy applicants must submit their complete nomination package (to include chain of command and detailer endorsement) to the Navy POC listed below NLT 01 January 2013.

If anyone has any questions regarding their application please refer to the Information Assurance Scholarship Program Website (which includes a link to the downloadable message located [here](http://www.doncio.navy.mil/ContentView.aspx?id=535) or contact DON CIO POC Ms. Jennifer Harper (Jennifer.a.harper@navy.mil/TEL: 703-695-1983 or the N2/N6 POC Mr. Mike Saunders (michael.saunders@navy.mil/TEL: 703-604-6292).

by CAPT James Mills and Jim Adams, USN (Retired)

**The Navy must treat information technology as a warfare capability.**

The U.S. Fleet is very capable today, but storm clouds on the horizon could not only jeopardize that situation, they could also threaten our capacity in the traditional warfare domains of sea, air, land, and space. Demand for maritime forces continues to increase to meet global requirements that include stability operations in the Middle East and western Pacific, new alerts brought by the 2010–11 Arab Spring, and counter-piracy and humanitarian-assistance missions. Heavy pressure on the U.S. budget and weariness after a decade of war resulting from 9/11 further complicate this picture.

Since the 1990s, the Navy has taken great strides to embed networking and information technology (IT) to improve operational and fiscal efficiency. Under this net-centric umbrella, a fleet can operate more effectively in a distributed fashion and reduce the operational impacts imposed by the maritime domain’s basic characteristic of distance. These technologies showed promise in reducing the greatest expenses to Fleet operations: manpower costs. The better the technology, the lower the demand for people, or so the theory goes.

The Navy can take pride in having been the first service to truly embrace net-centric and cyber capabilities and put them into practice; it continues to optimize these capabilities with increasing investments in unmanned and autonomous systems, maturing the Maritime Operations Center concept, and providing enterprise-wide networking such as establishing the world’s largest intranet. However, on both the fiscal and the capability fronts, we must now change tack or face standing into heavy weather.

**Red Sky at Morning, Sailor Take Warning**

The Navy pioneered global communications, developed the Global Positioning System that led to revolutions in precision targeting and commercial transportation, and advanced software engineering that fundamentally changed ballistics and the industrial software industry. But today, in terms of networking and IT, the service is lagging in state-of-the-art operational capacity. At one time the Navy led the development of IT, but today it is just a unit steaming in formation under the guide of a global industry driven largely by consumer demands. As dawn breaks on the new cyberspace domain, we are at a “red sky” moment.

We face 25 percent across-the-board reductions in IT spending and continued delays in IT modernization. As we strive to produce one enterprise—a global network—our Fleet’s operators and acquisition community are relearning the lesson that simply procuring commercial technology does not lead to interoperability. Without establishing a well-developed, enforceable framework to guide technology insertion, we are not adequately addressing the complexity of these networks and the burden placed on sailors to operate and maintain them. Somewhere along the line in working IT from an enterprise viewpoint, we have forgotten what the Navy’s raison d’être is. The Fleet is the real Navy enterprise. It is our main thing. Without an operationally effective Fleet, there is no need for a Navy.

Our networking and IT capabilities are just as core to an operationally effective Fleet as are new aircraft platforms, future nuclear-powered aircraft carriers, or new surface combatants and submarines. None of these traditional platforms is effective without secure and resilient software, networking, and IT.

In recent years we have seen that the network has taken on a more visible role in strike operations, ballistic-missile defense, command and control, and ship machinery and propulsion plant control. We have proliferated embedded systems into these shipboard functions, which are integral to the basic operations of our vessels, without fully understanding the impact on manpower or holistically assessing the effects on shipboard reliability. This approach increases our cyber vulnerability and operational risk due to ungraceful systems failure, which brings unpredictable behavior such as loss of steering control in a restricted maneuvering situation, failure to communicate when trying to execute tactical orders, or loss of situational awareness when defending the ship from attack. If technologies do not behave in a graceful, predictable manner when they fail, we face greater risks of loss of life or combat power.

So what are we to do? The answer is simple but difficult to accept. It is a matter of priorities. Storm clouds are building dead ahead, but we still have time to tack on to a more favorable course. A good navigational track will allow us to weather these challenging times.

**Prioritize the Fleet**

In the cyber and net-centric domain, the Fleet must take precedence over Navy support communities and be resourced as the top tier of the service’s enterprise when it comes to network capabilities. As their primary platform for planning and command-and-control functions, Fleet units are using decade-old commercial operating systems that are no longer commercially supported and five times more vulnerable than current versions. Expensive smartphones are deployed widely across the Navy–Marine Corps Intranet and One-Net, yet shipboard computer systems are expected to operate eight years or more before being upgraded.

Fleet units rely on network-based machinery and shipboard control systems that are overly complex, not resourced for on-board technicians, and connected to networks with limited resiliency. These capabilities are engineered so that interoperability “work-arounds”—additional manual procedures that sailors must take to compensate for system flaws—are assumed to be acceptable common practice.

The training pipeline is allowed to generate only apprentice-level technicians, and the logistics pipeline provides only critical spares just in time. Commanding officers are not provided the tools they need to maintain the readiness and trustworthiness of their shipboard networks. We are growing a new generation of sailors who cannot operate these networks in their degraded condition caused by battle damage (whether cyber or kinetic) without waiting for shore distance support. Instead of the expertise that was once maintained on board each ship, today we rely on “distance support.” Just as civilians must call a technician in India for assistance, sailors are expected to fix things by chatting over the phone or Internet. In an age of Stuxnet, other computer malware, and Wikileaks, these are not acceptable conditions to ensure mission success for the Fleet.

Our core competency of providing a navy to defend the nation requires that IT and cyber capabilities give precedence to the operational force and those directly coordinating it such as the Maritime Operation Centers. Ships, squadrons, expeditionary forces, operational headquarters, and key telecommunications hubs should be resourced as a priority tier and be considered first among equals.

This view runs counter to the single-enterprise perspective, which advocates an equal implementation across Navy operational and support communities, ashore and afloat. But we can no longer afford to provide a single-enterprise capability that meets all the needs of the operating Fleet as well as those of the service’s support infrastructure. Resourcing the Fleet as a priority tier will allow for more rapid modernization and currency of software and IT, thus improving performance and resiliency and reducing our exposed cyber-attack surface.

**Ships First, Then Support**

The Navy’s configuration-management process (its method to maintain control over which specific software versions or hardware variants are installed on a ship or shore station) is coupled with an information-assurance process to assess the system for any vulnerability it may introduce to the network. Because a vulnerability to one system can lead to widespread failure or exploitation, we must streamline the two processes to facilitate a higher speed to capability. If we use technologies like cloud computing and software virtualization, these processes will be more efficient and better able to rapidly deliver needed capability to the warfighter.

For the Fleet, a new technology framework must be established to provide the flexibility to rapidly modernize shipboard systems without lengthy processes. This will also standardize systems administration and operation, lower cyber-security risk, and enhance the Naval Network’s resiliency. It should not take seven to ten years to modernize shipboard IT capabilities, then an additional five to develop sufficiently trained and experienced sailors to use them.

The tiered approach to network capability must be operationally responsive to the needs of the combatant commander and the fleet commander. While strategic cyber capabilities and priorities remain, the vast majority of network operations in the Fleet relate to activities at the operational and tactical levels of war. Through strong coordination linkages and awareness of theater threats and challenges, Fleet Cyber Command and Navy Cyber Forces must build a structure that is receptive and tuned to deliver capabilities complementary to and supporting of traditional kinetic naval warfare, and that meets the requirements of fleet commanders and forward-deployed warfighters.

**Maximize the Information Dominance Corps**

Great strides were made under Admiral Gary Roughead’s information-dominance vision, including the establishment of an organization dedicated to this mission, the Information Dominance Corps. The IDC has the preeminent expertise in all things cyber, and now it is time to take it to the next level of professionalization. In the aviation community, this would mean differentiating between specialties such as tactical strike, maritime patrol, electronic warfare, force defense, and logistics.

The IDC net should be cast wider, to incorporate skills that work at C4I-, network-, and cyber-related tasks. For example, it should make use of engineering duty officers who specialize in C4I systems, sailors with electronics and interior-communications skills, and those in the civilian IT community who have expertise in acquisition. A holistic perspective of community competencies and career development is essential to maintaining the vitality of the Navy’s resident cyber expertise and to supporting retention. The available pool of qualified cyber and IT experts is shrinking, and the Navy must articulate and execute a strategy that encourages preserving IDC skills and sends a positive message about the value of service to attract new personnel into this community.

Training and education of the IDC is recognized as a vital element of the overall strategy, and there have been successful pilot programs such as the use of cognitive tutors in Navy IT training, additional top-tier graduate opportunities, and more emphasis on IDC and Information Assurance Workforce qualifications. But a more comprehensive strategy needs to be developed and enacted.

The same skills that the Navy requires to realize IDC capabilities are also in very high demand globally. The service must develop creative mechanisms to attract this talent. The Department of Defense’s *Critical Code* report reinforces the need to find ways to improve the Navy’s abilities in systems architecture, software development, and cyber-security. Currently these are all deficient in the DOD. [1](http://www.usni.org/magazines/proceedings/2012-09-0/my-other-combat-system-network#footnotes)

At the same time, we must make sure shipboard operators do not lose sight of the basics of planned and corrective maintenance and the fundamentals of our systems that tie the underway unit to the outside world. Skilled operations of shipboard network and combat systems are vital to the mission accomplishment of each ship. IT touches not just command-and-control and information systems, but also everything from steering control to machinery monitoring, damage-control response, navigation, and even shipboard fire-main and waste services. Much of the IDC has focused on the basics of network operations and emerging cyber-warfare functions. But our Fleet’s dependencies on networks are more far-reaching than just these two areas.

The time is also right for the IDC to have a seat at the warfare commander’s table in strike groups. By aligning afloat staff billets, the IDC should establish the Information Dominance Warfare Commander to coordinate the tactical-level aspects of cyber, electronic warfare, and other information-operations capabilities.

**Reinstitute Self-Sufficiency**

The Navy has always been an expeditionary force that operates under the doctrine “You fight with only what you bring.” But now we’ve placed fiscal efficiency above operational self-sufficiency, and many of our skills and capabilities have atrophied. The demands to deploy the Fleet are not decreasing, even though the size of the Fleet is. To meet this challenge, ships will expect to see longer deployments forward. Given this dynamic, it is even more critical that we regain many of our Cold War abilities.

A large part of this issue is cultural. At one time, for chiefs and leading technicians it was a matter of personal pride to fix their gear and maintain their systems at top readiness. They were expert in the foundational principals of how to troubleshoot a system. They knew theirs forward and backward, and they maintained the shipboard system as if it had been their own sports car. Today we have created an approach in which the technician must rely on an onboard tech rep or call distance support; there is no sense of ownership of the system’s readiness. This cultural shift, due to many factors, will not work in major combat operations.

Contributing to the situation are reduced training for A- and C-school technical ratings; the inability to maintain pace with technology in the schoolhouse; assumptions that all IT is alike, so one technician can be an expert in multiple systems; and commanding officers who do not challenge the material and personnel shortfalls.

This is not a generational problem: today’s sailors are extremely bright and motivated. It is an issue of leadership. We need to make self-sufficiency once again the metric by which we measure a successful, combat-ready ship or squadron. As a prime directive, the acquisition community must acquire interoperable shipboard systems that have a robust integrated logistics train (meaning the complementary spare parts, documentation, and training needed to properly maintain the systems). The model of what is acceptable to maintain a combat-ready Fleet must be restructured. In the days of self-sufficiency, if no one in the ship knew how to fix the problem, referral went right to the systems expert. There were no delays while a generalist was sought to assist.

Which path should we take—increase the competency of our technicians, or rely more heavily on tech reps? Should we enhance the C4I and combat-systems skills in our Regional Maintenance Centers, or accept the current preference for generalist expertise? This model needs a hard look.

In the days of a downsized Fleet, any single-systems casualty has far greater operational impact across the theater. With ships more dispersed, it will be increasingly difficult for the rear-echelon-support model to succeed, especially in the face of area denial by an adversary. We must ensure that the Navy’s network, combat systems, and cyber capabilities are ready to weather major conflict.

**Get Ready for Heavy Weather**

Our networks are almost exclusively built on technologies derived from the original Internet design, in a cyber world where neighbors were trusted and security was an afterthought. Cyberspace is now filled with countless untrustworthy groups who aim to do economic, intellectual, political, or military harm to our nation. We must recognize this Achilles’ heel and seek alternative designs to counter these vulnerabilities.

The National Science Foundation chartered a Future Internet Architecture Project to meet this exact challenge. [2](http://www.usni.org/magazines/proceedings/2012-09-0/my-other-combat-system-network#footnotes) The Navy should become an early adopter of these emerging technologies to build a more resilient, defensible network. Likewise, we must develop the capacity to train sailors on their network systems with the same rigor and currency as we train engineering, navigation, and combat-systems operators to deal with on-board casualties. They must be able to “fight the network hurt”: execute core war fighting functions in the face of degraded system performance.

Just as we instituted a national interstate highway system to expand military and economic capacity, so too Navy network planners must now build capacity and alternative routes to support the free flow of information across the globe. Getting the right intelligence to the appropriate decision-maker when that person needs it will allow a smaller Fleet to remain operationally effective on a worldwide scale.

The flood of data is rising faster than our systems and networks can handle without significant investments. A recent study of the Navy’s intelligence, surveillance, and reconnaissance architecture shows that we are rapidly approaching an inflection point at which tactical systems will not be able to transmit, let alone store, the influx. [3](http://www.usni.org/magazines/proceedings/2012-09-0/my-other-combat-system-network#footnotes) The remedy is not the common mantra “We need more bandwidth.” Rather, what we need is a solution that taps into the power of cloud computing and virtualization technologies to fuse the information so that it is relevant and available to the decision-maker.

We have to face facts. Fiscal constraints will drive us to a smaller Navy. This does not necessarily mean we will be less powerful. When we have harnessed disruptive advances in technology such as air power from the sea, the reach of nuclear-powered ships, or the effectiveness of precision-guided weapons, we’ve realized improvements to our operational flexibility and effectiveness that are on orders of magnitude. Key factors in past successes were based on providing top-tier schoolhouse training, qualification programs on board ship focusing on self-sufficiency expertise, development of robust operating and casualty procedures and planned maintenance systems, and continuous drilling of these skills in combat-relevant scenarios. Keeping the information power edge is just as critical as making a disruptive technology advance.

We must invest the right level of leadership and funding into raising operational C4I and combat-systems efficiency. By returning to basics in their sustainment, training, and capability-delivery processes, we can get enough wind in our sails to chart a course that ensures the Fleet, even though smaller, is empowered by top-tier networks that allow for rich, well-understood collaboration among warfare commanders, real-time integration of persistent sensing into the commander’s situational awareness, and greater agility in meeting operational demands. With the proper leadership, setting of priorities, and process discipline, we can come about and turn this situation into a “red sky at night, sailor’s delight” advantage.

1. National Academies of Science, *Critical Code: Software Producability for Defense* , Washington, DC, November 2010.

2. National Science Foundation, *NSF Future Internet Architecture Project* , Washington, DC, 2011, [www.nets-fia.net/](http://www.nets-fia.net/) .

3. Department of the Navy, Research, Development & Acquisition (ASN RDA), *Maritime Intelligence, Surveillance, and Reconnaissance Enterprise Architecture Study* , Washington, DC, 2010.

Should the IDC Stay Restricted Line?

By CDR H. Leon Archibald

How we ensure the Navy officer corps is positioned to succeed in Cyberspace Operations is being discussed at various levels with the IDC and URL communities. The critical questions being asked are should the IDC stay RL or become a URL community? And if IDC officers become URL does that mean they would or should command at sea? These are insightful questions which could potentially change the Navy for decades to come. The “unknowns” - the known unknowns and the unknown unknowns make these questions difficult and complex. However, there are existing warfare models that are germane for consideration in how this could be effectively managed within the Navy.

**Framing the Problem**

First, should the IDC stay RL or migrate to the URL Community? The first step in defending and dominating in the cyberspace domain is to understand it. Thus, before answering this question it is imperative to define cyberspace and cyberspace superiority. Joint Publication 3-12 *Cyberspace Operations*, defines cyberspace as “A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and associated data, including the Internet, telecommunication networks, computer systems and embedded processor and controller.”[[1]](#footnote-1) Whereas cyberspace superiority is “The degree of dominance in cyberspace by one force that permits the secure, reliable conduct of operations by that force, and its related land, air, maritime and space forces at a given time and place with prohibitive interference by an adversary.”[[2]](#footnote-2) In this respect, cyberspace traverses the physical domains of land, sea, air and space through interconnected technological devices.

Leaders within the public and private sectors agree the next serious security threats are coming from the cyber world. In establishing the IDC, former Chief of Naval Operations (CNO) Adm. Gary Roughead tapped the IDC as the Navy’s premier cyberspace warriors and stated “We’ve burned the ships… There is no turning back.”[[3]](#footnote-3) To that end, the Department of the Navy (DoN) aligned its information-centric programs and capabilities to better deal with cyber threats. Therefore, the issue is not whether the IDC should migrate to URL but rather how and when should it be migrated? There is nothing “restricted” about cyberspace. Neither should there be anything “restricted” about the IDC, to include the community in which it resides.

Secondly, if the IDC migrate to URL does that mean they should command at sea? Without a doubt, command should be the ultimate goal for any officer. One need only review the Uniform Code of Military Justice (UCMJ) to be reminded of the special trust, responsibility, accountability and authority of a ship’s captain. Cyber Operations challenges the paradigm of our traditional culture of command at sea being the driving factor in URL determination and we need to ensure proper alignment of URL talent and leadership to ensure success regardless of where those commands reside. . Additionally, manpower considerations will be a factor in the near term. Currently, there is no shortage of highly qualified URL officers competitive for command at sea. In 2011, the Navy used force shaping tools to reduce the inventory of URL commanders and captains. Conversely, the cyberspace professionals are in low supply and high demand in both the public and private sectors. As with the officers in the URL community, IDC officers’ talents must be aligned to lead those commands best supporting the Navy’s cyber mission sets.

IDC officers should be provided the best education and specialized training available and detailed to assignments to ensure commands achieve and maintain cyberspace dominance. Gen. Keith Alexander, head of both the National Security Agency and U.S. Cyber Command, says most DOD networks are “not defensible” as they are currently configured. Consolidation is required to help make them more manageable.[[4]](#footnote-4) A successful cyber attack can be as disastrous and costly in loss of lives, economic havoc and general destabilization as any other attack on US interests. With this in mind, every dollar spent on training IDC officers, to command ships at sea, is a dollar not spent on building the world’s strongest cyberspace professional workforce that is able to successfully execute cyberspace operations across all spectrums.

**Finding Solutions**

The Special Warfare (SPECWAR) Officer can serve as a model for the IDC as it relates to migrating to URL and commanding at sea. SPECWAR officers are absolutely the best at what they do and their talents and leadership remain aligned tightly to their mission set. They are the nation’s foremost maritime special operations force and are fully qualified URL Officers (113X). They are authorized to wear the command at sea pin, yet they do not command ships. Because of their unique training and critical skill sets, senior Navy leadership decided it is in the best interest of the nation and Navy for SPECWAR officers to be “specialists” in the area of special operations and not “generalists.”

In short, this is a matter of understanding the added value cyberspace professionals provide to the warfighter and how best to employ them to ensure the highest return on investment for the taxpayers. Further, the Department of Labor revealed the total U.S. cyberspace workforce currently comprises less than three percent of the entire U.S. workforce; specialized cyberspace professionals (information security analysts, computer network architects, cyberspace operators, forensics analysts, and other specialized functions) comprise less than one-half of one percent of the entire U.S. workforce.[[5]](#footnote-5) With the current and future fiscal constraints looming in the Department of Defense (DOD) budget, the high inventory of URL officers and supply/demand challenge for sourcing cyberspace professionals, and the nation’s and Navy’s current state of cyberspace readiness, is it the best use of Navy trained cyber experts with significant operational experience to be commanding afloat platforms when we need them to be commanding our operational platforms for information dominance?

Additionally, to leverage and defend cyberspace the IDC should immediately be charged and held accountable to serving as Information Warfare Commanders (IWC) for Carrier Strike Groups and senior IWC positions on Numbered Fleets staffs. Furthermore, the IDC has more than ten years of experience in the forefront of developing and operating unmanned technologies. Leveraging the critical skills of IDC officers will be more important than ever as war fighting shifts from maneuver platforms as the center of the fight, to the network and cyberspace around it.

**The Way Ahead**

President Obama’s *2012 Defense Strategic Guidance* challenged the DOD to operate effectively in cyberspace and defend its networks to ensure reliable information and communications networks and assured access to cyberspace and space.[[6]](#footnote-6) To that end, old thinking is insufficient for today’s challenges in the cyber world. The nation’s critical infrastructure is at risk from threats which can degrade, disrupt or destroy crucial assets and services. To achieve dominance in cyberspace the Navy must recruit, educate, train and retain a world-class cyberspace professional workforce.

As information superiority provided the strategic advantage for victory at the Battle of Midway; cyberspace superiority will be the key to victory in conflicts in the 21st Century. Dominance in the cyber domain requires fresh ideas and new thinking at all levels. The people with the right knowledge, skills and abilities to implement new technologies will determine success in cyberspace operations. Similar to Special Warfare Officers, the IDC should migrate to the URL Community and be assigned to command at sea equivalent billets and be authorized to wear the command at sea pin. Lastly, IDC officers should be highly-educated, well-trained and detailed to assignments where they can earn surface warfare and submarine warfare qualifications thereby ensuring afloat commands are manned with operationally savvy and fleet experienced cyberspace professionals.

***About the Author***

Commander Archibald is assigned to U.S. Special Operations Command as the CIO Governance Branch Chief. His more recent assignments included: C5I Department Head/Communications Officer, USS Nassau; Combat Information System Officer, USS Harry S. Truman; Information Professional Junior Officer, Commander, Navy Personnel Command; Deputy G6 for IT Operations, U.S. Army Corps of Engineers, Gulf Region   
Division Baghdad, Iraq; Commanding Officer, Naval Computer and Telecommunications Station Bahrain; and Deputy N6 and Information Superiority Officer, U.S. Second Fleet/Combined Joint Operations from the Sea Center of Excellence. He holds a Master of Science degree in Computer Information Systems from the University of Phoenix and a Master of Strategic Studies degree from the Air War College, Air University.

Top of Form

Top of Form

FY14 Active Duty Limited Duty Officer and Chief Warrant Officer

R 171545Z SEP 12 PSN 488688K42

FM CNO WASHINGTON DC//N1//

TO NAVADMIN

INFO CNO WASHINGTON DC//N1//

UNCLAS//N01420//

NAVADMIN 285/12//

MSGID/GENADMIN/CNO WASHINGTON DC/N1/SEP//

SUBJ/FY-14 ACTIVE DUTY LIMITED DUTY OFFICER AND CHIEF WARRANT OFFICER IN-SERVICE PROCUREMENT BOARD//

REF/A/MSG/CNO WASHINGTON DC//N1/171307ZSEP12//

AMPN/REF A IS NAVADMIN 281/12, ADVANCED CHANGE NOTICE TO OPNAVINST 1420.1B, CHAPTER SEVEN, LIMITED DUTY OFFICER AND CHIEF WARRANT OFFICER APPLICATION INSTRUCTION AND POLICY//

RMKS/1. THIS NAVADMIN ANNOUNCES THE SOLICITATION OF APPLICATIONS FROM HIGHLY QUALIFIED AND MOTIVATED E6 THROUGH E9 PERSONNEL FOR THE FY-14 LIMITED DUTY OFFICER (LDO) AND CHIEF WARRANT OFFICER (CWO) PROGRAMS. LDOS AND CWOS BRING A VARIETY OF EXPERIENCE AND UNIQUE PERSPECTIVES INTO THE WARDROOM FROM THEIR ENLISTED SERVICE. THE LDO/CWO CAREER PATHS PROVIDE ADDITIONAL LEADERSHIP OPPORTUNITIES AND ENHANCE A SAILOR'S ABILITY TO CONTRIBUTE TO THE NAVY. THESE PROGRAMS DELIVER TO THE OFFICER CORPS SEASONED PROFESSIONALS WITH PROVEN LEADERSHIP ABILITIES AT AN ECONOMICAL COST. LDOS PROVIDE BROAD TECHNICAL MANAGEMENT AND LEADERSHIP SKILLS, AND CWOSPROVIDE SPECIFIC TECHNICAL EXPERTISE AND LEADERSHIP SKILLS IN SUPPORT OF THE UNRESTRICTED LINE, RESTRICTED LINE AND STAFF CORPS COMMUNITIES. LDOS AND CWOS SERVE IN A VARIETY OF LEADERSHIP BILLETS WITHIN THEIR TECHNICAL FIELDS, RANGING FROM DIVISION OFFICER TO COMMANDING OFFICER ASHORE.

2. UPDATED AND ADDITIONAL POLICY GUIDANCE TO OPNAVINST 1420.1B PROMULGATED IN REF A.

3. THE FY-14 IN-SERVICE PROCUREMENT BOARD WILL CONVENE 7 JAN 13. APPLICATIONS MUST BE POSTMARKED NO LATER THAN 1 NOV 12. ROUTINE ADDENDUMS TO APPLICATIONS, EXCLUDING EVALUATIONS AND AWARDS, MUST BE

RECEIVED NO LATER THAN 1 DECEMBER 12 FOR PRE-BOARD SCANNING. EVALUATIONS AND AWARDS MUST BE RECEIVED NOT LATER THAN THE DAY PRIOR TO BOARD CONVENING. ALL APPLICATIONS AND ADDENDUMS MUST HAVE MEMBER'S FULL SSN ON EACH PAGE. APPLICATIONS MUST BE MAILED TO THE NAVY PERSONNEL COMMAND (NPC) CUSTOMER SERVICE CENTER. TIME SENSITIVE SUBMISSIONS MAY BE SUBMITTED ELECTRONICALLY TO

CSCSELECTIONBOARD(AT)NAVY.MIL. HARD COPY AND ELECTRONIC SUBMISSIONS MUST INCLUDE COMMAND ENDORSEMENT. BOARD NUMBER 180 IS FOR CWO TO LTJG AND BOARD NUMBER 181 IS FOR ENLISTED TO LDO/CWO.

MAILING ADDRESS IS:

NPC CUSTOMER SERVICE CENTER

PRESIDENT, FY-14 LDO/CWO PROCUREMENT BOARD

BOARD (#180 OR #181 AS APPROPRIATE)

5720 INTEGRITY DRIVE

MILLINGTON TN 38055

PAGE 04 RUEOMFL8092 UNCLAS

4. INTERVIEW APPRAISAL BOARDS SHALL CONSIST OF A MINIMUM OF THREE NAVAL OFFICERS (LDO/CWO IF AVAILABLE). EVERY EFFORT (INCLUDING BUT NOT LIMITED TO TELECONFERENCE, VTC, DCO, ETC) SHALL BE USED TO

ENSURE AT LEAST ONE BOARD MEMBER IS FROM THE DESIGNATOR FOR WHICH THE APPLICANT IS APPLYING. MINIMUM GRADE REQUIREMENTS FOR BOARD MEMBERS ARE LTJG, OR CWO2 WITH TWO YEARS TIME-IN-GRADE. POTENTIAL BLOCK ON INTERVIEW APPRAISALS MUST BE MARKED FOR LDO/CWO CANDIDATES.

5. FOR APPLICANTS WHO HAVE OR ARE CURRENTLY SERVING IN INDIVIDUAL AUGMENTEE OR GLOBAL SUPPORT ASSIGNMENTS (IA/GSA), INCLUDE THESE TOURS IN THE ASSIGNMENT HISTORY SECTION OF THE APPLICATION. CO'S

RECOMMENDATION MUST INCLUDE VALIDATION OF ANY LISTED IA/GSA ASSIGNMENT AND THE STATEMENT IN REF A, PARA THREE.

6. APPLICANTS CURRENTLY SERVING IN IA/GSA, MAY HAVE THEIR APPLICATION ENDORSED BY THEIR FIELD COMMANDER. ALL APPLICATIONS ENDORSED BY FIELD COMMANDER MUST HAVE PARENT COMMAND CONCURRENCE. SAMPLE CONCURRENCE LETTER IS LOCATED AT HTTP://WWW.PUBLIC.NAVY.MIL/BUPERS-NPC/OFFICER/COMMUNITYMANAGERS/LDO\_CWO/PAGES/REFERENCES.ASPX.

7. COMMANDS MUST ENSURE COPIES OF THE MOST RECENT PERIODIC EVAL ARE INCLUDED IN THE APPLICATION OR LATER ADDENDUM FOR BOARD REVIEW AND CONTINUITY. FIRST CLASS PETTY OFFICERS MUST SUBMIT THEIR 15

NOVEMBER 2012 EVALUATION.

8. TIS FOR THE FY-14 BOARD MUST BE COMPUTED TO 1 OCTOBER 2013.

9. DUE TO THE LDO/CWO SUSTAINABILITY INITIATIVE, THE FOLLOWING CWO TO LDO (LTJG) APPLICATIONS WILL BE ACCEPTED FROM THE FOLLOWING CWO DESIGNATORS: 7121, 7211, 7231, 7281, 7331, 7421, 7481, AND 7511.

10. CWO APPLICANTS FOR LDO MUST HAVE AT LEAST 2 YEARS TIG AND BE BETWEEN 14 AND 16 YEARS TOTAL ACTIVE SERVICE AS OF 1 OCTOBER 13. THIS ENABLES SELECTEES A FULL CAREER OPPORTUNITY AS AN LDO. LDO (LTJG) SELECTEES WILL TERMINATE THEIR CWO STATUS AND BECOME A PERMANENT LDO UPON APPOINTMENT.

11. DUE TO THE LDO/CWO SUSTAINABILITY INITIATIVE, APPLICATIONS WILL NOT BE ACCEPTED FOR DESIGNATORS 615X, 621X, 647X, 655X, 721X, 723X, 728X, 748X, AND 751X.

12. THE FY-14 BOARD WILL CONSIDER APPLICANTS FOR CYBER CHIEF WARRANT OFFICERS (743X). PERSONNEL APPLYING FOR THIS DESIGNATOR MUST MEET ELIGIBILITY REQUIREMENTS LISTED IN NAVADMIN 139/10.

13. NAVY DIVER APPLICANTS APPLYING FOR DESIGNATOR (720X) MUST MEET REQUIREMENTS OUTLINED IN MILPERSMAN 1220-100 PARAGRAPH 18.B.(5)(A) THROUGH (E), (H), AND (I).

14. APPLICATIONS FOR THE 734X AND 738X DESIGNATORS SHOULD BE MODIFIED TO MEET THE APPROVED MERGER OF THESE TWO DESIGNATORS INTO THE AVIATION MAINTENANCE CWO 733X DESIGNATOR.

15. DUE TO ONGOING RATING MERGERS, ELIGIBLE SAILORS ARE ENCOURAGED TO APPLY FOR THE DESIGNATOR FOR WHICH THEY HAVE DOCUMENTED TECHNICAL AND LEADERSHIP EXPERIENCE, REGARDLESS OF CURRENT RATING.

16. APPLICANTS MUST MAINTAIN ELIGIBILITY THROUGHOUT THE SELECTION AND PROMOTION PROCESS. APPLICANTS WHO ARE DEEMED INELIGIBLE AFTER THE SUBMISSION OF APPLICATIONS MUST BE DECLARED INELIGIBLE BY THE CURRENT COMMANDING OFFICER. A SAMPLE FORMAT IS LOCATED AT HTTP://WWW.PUBLIC.NAVY.MIL/BUPERS-NPC/OFFICER/COMMUNITYMANAGERS/LDO\_C

WO/PAGES/REFERENCES.ASPX.

17. EACH APPLICANT AND COMMAND MUST ENSURE THAT APPLICATIONS ARE COMPLETE AND ACCURATE. INCOMPLETE APPLICATIONS COULD RESULT IN NON-SELECTION. REFER TO OPNAVINST 1420.1B (CHAPTERS 2, 7 AND

APPENDIX F) AND REF A FOR PROGRAM OVERVIEW, ELIGIBILITY CRITERIA, AND APPLICATION FORMAT.

18. FOR THE MOST UP TO DATE APPLICATION PROCESS, VISIT THE PERS-803 WEBSITE AT <HTTP://WWW.PUBLIC.NAVY.MIL/BUPERS-NPC/BOARDS/ADMINISTRATI>VE/LDO\_CWO/PAGES/DEFAULT.ASPX.

THIS SITE CONTAINS APPLICATION HELP AND A REVIEW CHECKLIST TO PRINT AND INCLUDE IN THE APPLICATION FOLDER. THIS SITE ALSO CONTAINS GUIDANCE SUCH AS CSC MAILING INFO, RECEIPTS CHECK LINK, HOW TO

MONITOR APPLICATION STATUS ON BUPERS ONLINE AFTER PERS-803 REVIEW,AND HOW TO RECONCILE APPLICATION ERRORS VIA ADDENDUM IF ITEMS OR CORRECTIONS ARE REQUIRED FOR COMPLETENESS OR ELIGIBILITY.

19. FOR VALID DESIGNATOR CODES, VISIT THE LDO/CWO OCM WEBSITE AT

<HTTP://WWW.PUBLIC.NAVY.MIL/BUPERS-NPC/OFFICER/COMMUNITYMANAGERS/LDO_C>WO/PAGES/REFERENCES.ASPX

AND CLICK ON THE LDO/CWO DESIGNATORS LINK.

20. FIRST CLASS PETTY OFFICERS SERVING IN IRAQ, AFGHANISTAN, AND THE HORN OF AFRICA WHO ARE DETERMINED CPO BOARD ELIGIBLE IAW NAVADMIN 336/07 OR NAVADMIN 018/00 ARE ALSO ELIGIBLE FOR LDO IF ALL OTHER ELIGIBILITY REQUIREMENTS ARE MET.

21. POINTS OF CONTACT:

A. FOR GENERAL LDO/CWO CAREER PATH AND POLICY QUESTIONS, CONTACT CWO5 MITCH ALLEN AT (901) 874-3044/DSN 882 OR VIA E-MAIL AT MITCHELL.ALLEN(AT)NAVY.MIL.

B. FOR NUCLEAR LDO/CWO APPLICATION AND ELIGIBILITY QUESTIONS, CONTACT LCDR TODD NICHOLS AT (703) 604-5489/DSN 664 OR VIA E-MAIL AT CHRISTOPHER.NICHOLS4(AT)NAVY.MIL.

C. FOR APPLICATION AND ELIGIBILITY QUESTIONS CONTACT CWO3 CLAY SUMMERS AT (901) 874-3170/DSN 882 OR VIA E-MAIL AT CLAY.SUMMERS(AT)NAVY.MIL OR MS. MARISA BEAL AT (901)874-3262/DSN 882 OR VIA E-MAIL AT MARISA.BEAL(AT)NAVY.MIL.

22. RELEASED BY VICE ADMIRAL S. R. VAN BUSKIRK, N1.//

FY14 Reserve Limited Duty Officer and Chief Warrant Officer

R 171537Z SEP 12 PSN 488470K31

SUBJ: FY-14 INACTIVE DUTY NAVY RESERVE LIMITED DUTY OFFICER AND CHIEF WARRANT OFFICER IN-SERVICE PROCUREMENT PROGRAM ANNOUNCEMENT BOAR

NAVADMIN 284/12

MSGID/GENADMIN/CNO WASHINGTON DC/N1/SEP//

SUBJ/FY-14 INACTIVE DUTY NAVY RESERVE LIMITED DUTY OFFICER AND CHIEF WARRANT OFFICER IN-SERVICE PROCUREMENT PROGRAM ANNOUNCEMENT BOARD//

REF/A/MSG/CNO WASHINGTON DC/171307ZSEP12//

AMPN/REF A IS NAVADMIN 281/12, ADVANCED CHANGE NOTICE TO OPNAVINST 1420.1B,CHAPTER SEVEN, LIMITED DUTY OFFICER AND CHIEF WARRANT OFFICER APPLICATION INSTRUCTION AND POLICY//

RMKS/1. THIS NAVADMIN ANNOUNCES THE FY-14 INACTIVE DUTY NAVY RESERVE LIMITED DUTY OFFICER (LDO) AND CHIEF WARRANT OFFICER (CWO) IN-SERVICE PROCUREMENT SELECTION BOARD. THE NAVY RESERVE IS SEEKING

APPLICATIONS FROM HIGHLY QUALIFIED E6 THROUGH E9 PERSONNEL FOR THE FY-14 LDO AND CWO PROGRAM. LDOS AND CWOS BRING A VARIETY OF EXPERIENCE AND UNIQUE PERSPECTIVES INTO THE WARDROOM FROM THEIR

ENLISTED SERVICE. THE LDO AND CWO CAREER PATHS PROVIDE ADDITIONAL LEADERSHIP OPPORTUNITIES FOR SAILORS AND ENHANCE THEIR ABILITY TO CONTRIBUTE TO THE NAVY.

2. ELIGIBLE SAILORS ARE ENCOURAGED TO APPLY FOR THE DESIGNATOR FOR WHICH THEY ARE MOST QUALIFIED, REGARDLESS OF CURRENT RATING. REFER TO OPNAVINST 1420.1B, OPNAVINST 1120.12, AND REF A FOR ELIGIBILITY

CRITERIA AND APPLICATION FORMAT. FOR THE MOST UP TO DATE INFORMATION REGARDING APPLICATION PROCEDURES, AND BOARD MEMBERSHIP APPLICATIONS, VISIT THE LDO/CWO WEBPAGE AT <HTTP://WWW.PUBLIC.NAVY.MI>L/BUPERS-NPC/OFFICER/COMMUNITYMANAGERS/LDO\_CWO/PAGES/REFERENCES.ASPX.

3. THE FY-14 IN-SERVICE PROCUREMENT BOARD WILL CONVENE 7 JANUARY 2013 AND WILL CONSIDER CANDIDATES FOR THE FOLLOWING OFFICER DESIGNATORS:

AVIATION MAINTENANCE (633X)

ADMINISTRATION (641X)

INFORMATION SYSTEMS (642X)

INTELLIGENCE (645X)

SECURITY (649X)

CIVIL ENGINEER (653X)

BOATSWAIN (711X)

SPECIAL WARFARE TECH (715X)

ORDNANCE TECH-SURFACE (716X)

SPECIAL WARFARE COMBATANT CRAFT-CREWMAN (717X)

AVIATION MAINTENANCE TECH (733X)

INFORMATION SYSTEMS TECH (742X)

INFORMATION WARFARE TECH (744X)

INTELLIGENCE TECH (745X)

4. TIME IN SERVICE (TIS) ELIGIBILITY DATE FOR THE FY-14 BOARD MUST BE COMPUTED TO 1 OCTOBER 2013. APPLICATIONS MUST BE POSTMARKED NO LATER THAN 1 NOVEMBER 2012, AND 0ADDENDUMS TO APPLICATIONS MUST BE RECEIVED NO LATER THAN 1 DECEMBER 2012. COMMANDS SHOULD ENSURE COPIES OF THE MOST RECENT PERIODIC FITREP OR EVALUATION FOR THEIR APPLICANTS ARE SUBMITTED IN THE ORIGINAL APPLICATION OR IN AN ADDENDUM TO ENSURE CONTINUITY FOR BOARD REVIEW. APPLICATIONS, COMMAND ENDORSEMENTS, AND SUPPORTING DOCUMENTATION SHOULD BE SENT TO:

REGULAR MAIL:

NAVY PERSONNEL COMMAND (NPC) CUSTOMER SERVICE CENTER

PRESIDENT FY-14 INACTIVE DUTY NAVY RESERVE LIMITED DUTY OFFICER AND CHIEF WARRANT OFFICER IN-SERVICE

PROCUREMENT PROGRAM BOARD (#315)

5720 INTEGRITY DRIVE

MILLINGTON TN 38055

EXPRESS MAIL:

NAVY PERSONNEL COMMAND (NPC) CUSTOMER SERVICE CENTER

PRESIDENT FY-14 INACTIVE DUTY NAVY RESERVE LIMITEDDUTY OFFICER AND CHIEF WARRANT OFFICER IN-SERVICE

PROCUREMENT PROGRAM BOARD (#315)

5640 TICONDEROGA LOOP BLDG 768 RM E302

MILLINGTON TN 38055

5. TO CHECK FOR RECEIPT OF APPLICATIONS AND ADDENDUMS, APPLICANTS MAY CALL THE NPC CUSTOMER SERVICE CENTER AT 1-866-U ASK NPC OR CHECK THE CUSTOMER SERVICE CENTER ONLINE SITE BY LOGGING IN AT:

<HTTPS://AHDSEDSTWS16.AHF.NMCI.NAVY.MIL/OA_HTML/NPC.HTML>. (ALL LOWERCASE LETTERS EXCEPT THE "HTML")

6. POINTS OF CONTACT:

A. FOR GENERAL LDO/CWO CAREER PATH AND POLICY, CONTACT LCDR AL CONCEPCION, LDO/CWO RESERVE OFFICER COMMUNITY MANAGEMENT, AT (901) 874-3291/DSN 882 OR VIA E-MAIL AT ALVIN.CONCEPCION(AT)NAVY.MIL.

B. GENERAL BOARD APPLICATION PROCEDURES/ELIGIBILITY CAN BE FOUND AT <HTTP://WWW.PUBLIC.NAVY.MIL/BUPERS-NPC/OFFICER/COMMUNITYMANAGERS/L>DO\_CWO/PAGES/REFERENCES.ASPX

OR VIA E-MAIL AT PERS-9\_CW\_LDRESBOARD(AT)NAVY.MIL.

7. RELEASED BY VICE ADMIRAL S. R. VAN BUSKIRK, N1.//

Online Reading Room

We are going to start populating an online reading room. This is intended to be a living breathing list, so please forward any others you’d like to see listed to Joe Sullivan. That way we can keep up to date on all of the goings on in or near our community.

ARMED FORCES JOURNAL: <http://www.armedforcesjournal.com>

ARMY SPACE JOURNAL: <http://www.smdc-armyforces.army.mil/ASJ/index.asp>

C4ISR JOURNAL: <http://www.defensenews.com/section/C4ISR/C4ISR-Journal>

CHIPS: <http://www.doncio.navy.mil/chips/>

DEFENSE-AEROSPACE: <http://www.defense-aerospace.com/>

DEFENSE AR JOURNAL: <http://www.dau.mil/pubscats/Pages/aRJ.aspx>

DEFENSE AT&L MAGAZINE: <http://www.dau.mil/pubscats/Pages/DefenseAtl.aspx>

DEFENSE NEWS: <http://www.defensenews.com>

DEFENSE SYSTEMS MAGAZINE: <http://www.defensesystems.com>

FEDERAL COMPUTER WEEK: <http://www.fcw.com>

FEDERAL TIMES: <http://www.federaltimes.com>

GOVERNMENT COMPUTER NEWS: <http://www.gcn.com>

The Grid Magazine (DISA): <http://www.disa.mil/News/The-Grid-Magazine>

IAnewsletter: <http://iac.dtic.mil/iatac/IA_newsletter.jsp>

INFO DOMAIN (NAVY CYBER FORCES): <http://www.public.navy.mil/fltfor/cyberfor/Documents/Spring-Summer_2012_Web_updated.pdf>

JOINT FORCE QUARTERLY: <http://www.ndu.edu/press/jointForceQuarterly.html>

MILITARY INFORMATION TECHNOLOGY: <http://www.military-information-technology.com/military-information-technology>

PROCEEDINGS: <http://www.usni.org/magazines/proceedings>

SIGNAL ONLINE: <http://www.afcea.org/signal/>

WASHINGTON TECHNOLOGY: <http://www.washingtontechnology.com>

IP-Related Schools

This section highlights IP-related schools that may be available. This list will show you the course name and schedule. It is our goal to put as much information as possible in these charts, looking out a minimum of three class convening dates. If you know of other schools that would be beneficial for our IP officers, please let Mr. Joe Sullivan ([joseph.c.sullivan@navy.mil](mailto:joseph.c.sullivan@navy.mil)) know and they will be added to the list. Note that we have added IDC course offerings for career planning and potential opportunities of cross detailing.

This is a link for IP qualification study materials:

<https://private.navyreserve.navy.mil/CNIRC/Training_OPS/Information%20Professional/IP_Training/QUALS/Shared%20Documents/Forms/AllItems.aspx>

**INFORMATION PROFESSIONAL BASIC COURSE (A-202-0006)**

PURPOSE: To provide new Information Professional officers with a fundamental knowledge of the IP Community and the IP’s place within the Information Age Navy; to provide them with a foundation of skills and information that will enable them to develop, communicate, and promote innovative solutions, and to provide them with an introduction to the values that guide the IP Community.

SCHEDULES:

PENSACOLA (CID)

7 JAN – 4 FEB 2013

19 FEB – 18 MAR 2013

1 -26 APR 2013

13 MAY – 10 JUN 2013

19 AUG – 16 SEP 2013

6 JAN – 3 FEB 2014

18 FEB – 17 MAR 2014

31 MAR – 25 APR 2014

19 MAY – 16 JUN 2014

18 AUG – 15 SEP 2014

**ICMC (INFORMATION AND COMMUNICATION MANAGER COURSE) (A-202-0041)**

PURPOSE: To provide basic and advanced communication and information systems training for junior officers and senior enlisted billeted as senior enlisted communicators or communication/information system managers/officers.

SCHEDULES:

NORFOLK

1-22 OCT 2012

7-28 JAN 2013

25 FEB – 15 MAR 2013

22 APR – 10 MAY 2013

17 JUN – 18 JUL 2013

3-23 SEP 2013

SAN DIEGO

4 – 24 SEP 2012

29 OCT – 19 NOV 2012

26 NOV – 14 DEC 2012 (PEARL HARBOR)

28 JAN – 15 FEB 2013

25 MAR – 12 APR 2013

20 MAY – 10 JUN 2013

29 JUL – 16 AUG 2013

NOTE: Seats are in extreme demand and very difficult to get, so it is imperative to plan ahead.

**C4I SYS ENG (C4I SYSTEM ENGINEERING COURSE) (K-121-0181)**

PURPOSE: To provide system operator/administrator/maintainer personnel onboard Global Command and Control System - Maritime (GCCS-M) and Tomahawk Weapons System (TWS) ships with a basic understanding of applicable system hardware and connectivity, applicable system software, primary system support organizations, system documentation and data communications leading to the ability to conduct system level troubleshooting.

SCHEDULE:

VIRGINIA BEACH

15-19 OCT 2012

3-7 DEC 2012

28 JAN – 1 FEB 2013

25-29 MAR 2013

15-19 APR 2013

24-28 JUN 2013

19-23 AUG 2013

SAN DIEGO

3-7 DEC 2012

19-22 FEB 2013

25-29 MAR 2013

5-9 AUG 2013

16-20 SEP 2013

EVERETT, WA

11-15 FEB 2013

15-19 JUL 2013

PEARL HARBOR, HI

3-7 DEC 2012

22-26 APR 2013

YOKOSUKA, JAPAN

5-9 NOV 2012

4-8 MAR 2013

**STWO (STAFF TACTICAL WATCH OFFICER) (J-2G-0079)/(K-2G-0128)**

PURPOSE: To provide STAFF, SHIP, and AIRWING Officers with the tactical procedural skills required to plan, coordinate, and execute combat operations in a multi-threat, battle group/force surface/subsurface combatant task group environment.

SCHEDULE:

VIRGINIA BEACH

ACDU NAVY: Quota Control

Text: TACTRAGRULANT, DSN: 433-7807, COMM: (757) 433-7807

SAN DIEGO

ACDU NAVY: Quota Control

Text: TACTRAGRUPAC; DSN: 553-8337, COMM: (619) 553-8337

**AKMC (AFLOAT KNOWLEDGE MANAGER COURSE) (K-2G-7010)**

PURPOSE: Designed to provide the Strike Group Afloat Knowledge Manager (KM) with the education and training required to assist SG leadership in determining and managing critical information flows across the organization.

SCHEDULE:

For scheduling information, contact:

* Mr. Tim Snyder (619-553-0461; DSN 553-)
* Mr. Dennis Schulz (619-553-0537; DSN 553)
* Ms. Jill Robertson (619-553-8350; DSN 553)

**JIOOC (JOINT INFORMATION OPERATIONS ORIENTATION COURSE)**

COURSE OBJECTIVE: The objective of the Joint IO Orientation Course is to educate and train U.S. Government (USG) personnel in the military grades of Lieutenant/Captain (O-3) to Captain/Colonel (0-6) and civilian equivalents in the basics of joint Information Operations (IO), with a primary emphasis at the Combatant Command level. Specifically, the course focuses on teaching joint IO doctrine and Department of Defense IO policy guidance as they apply to the operational level of joint warfare. This course is particularly relevant to those serving in support of IO cells and other staff positions that require a basic knowledge of Joint IO. If IO planning skills are desired, then the student should take the JIOPC.

<http://www.jfsc.ndu.edu/schools_programs/jc2ios/io/jiooc.asp>

SCHEDULE

**JIOPC (JOINT INFORMATION OPERATIONS PLANNING COURSE) (P-520-0050)** COURSE MISSION: The mission of the Joint Information Operations Planners Course (JIOPC) is to establish a common level of understanding for IO planners and IO capability specialists who will serve in joint operational-level IO billets. This course is a prerequisite for personnel assigned to the Joint IO career force.

<http://www.jfsc.ndu.edu/schools_programs/jc2ios/io/jiopc.asp>

SCHEDULE

JOINT C4I STAFF AND OFFICERS COURSE (JC4ISOC)

COURSE MISSION: The mission of the JC4ISOC is to educate and train joint C4I decision makers in C4I concepts in the joint/coalition/interagency environments, the DoD’s organization and how it supports the C4I process, and the management and operation of current joint C4I systems and joint operational procedures associated with both strategic and theater/tactical systems. Students are required to demonstrate their learning by means of successfully completing an end of course examination and through participation in a C4I planning practical exercise.

<http://www.jfsc.ndu.edu/schools_programs/jc2ios/c4i/general_info.asp>

SCHEDULE:

13-1 15 Oct 2012 - 02 Nov 2012 (TS/SCI)

13-2 28 Nov 2012 - 14 Dec 2012 (Secret Level Only)

13-3 28 Jan 2013 - 15 Feb 2013 (TS/SCI)

13-4 04- 22 Mar 2013 (TS/SCI)

13-5 15 Apr – 3 May 2013 (TS/SCI)

13-6 29 May – 14 Jun 2013 (Secret Level Only)

13-7 22 Jul – 9 Aug 2013 (TS/SCI)

13-8 9-27 Sep 2013 (TS/SCI)

OTHER JOINT C4I TRAINING OPPORTUNITIES

Defense Information Services Agency Training Branch ([http:www.disa.mil/go/go434.html](http://www.disa.mil/go/go434.html))   
DISA’s Training Branch supports the DOD-wide IA education, training and awareness program. The branch develops and maintains curricula to support the DOD IA professional and user certification programs, and disseminates IA products to meet DOD-wide IA training and awareness requirements.

Information Assurance Courses (<http://ia.gordon.army.mil>) - School **of Information Technology, Ft Gordon, GA.**  
The Information Assurance (IA) Division, U.S. Army School of Information Technology, provides high quality Information Assurance/Computer Network Defense training and certification for Department of Defense personnel worldwide. Training is primarily for Department of Army personnel, but personnel from all services and other federal agencies are authorized to attend.

Joint Command, Control, Communications, Computers, and Intelligence Systems Curriculum (<http://www.nps.edu/Academics/GeneralCatalog/414.htm#o433>) - Department **of Information Science, Naval Postgraduate School, Monterey, California.**

Joint C4 Planners Course (JC4PC), (4C-F55/260-F15) (<http://www.signal.army.mil/jc4pc/>) – Fort Gordon, Georgia

MISSION: Educates C4 planners in doctrinal C4 concepts in the Joint, Interagency, and Coalition environments. The course focuses on the technical aspects of Joint C4 planning associated with Strategic, Theater, and Tactical level systems within the deliberate and crisis action planning (CAP) processes.

NAVY POC: NPC - COMM: (910) 874-4750 - DSN: 882-4750

SCHEDULE:

15 OCT – 9 NOV 2012

16 JAN – 13 FEB 2013

22 APR - 17MAY 2013

3-28 JUN 2013

29 JUL – 23 AUG 2013

**INFORMATION WARFARE COURSES**

INFORMATION DOMINANCE MID-CAREER COURSE

The course is designed for the IDC O4 and will include numerous topics of concern for all communities within the IDC. A list serve email will be sent soon seeking interested 04 officers to attend.

INFORMATION DOMINANCE SENIOR LEADERSHIP SYMPOSIUM (IDSLS)

This IDC focused symposium is designed to:

- create a Senior Symposium to focus IDC leaders on the core competencies of the Corps including Space/C4I/Acquisition;

- provide a forum for leaders to help shape the future of the IDC and equip them to pioneer, field, and employ game-changing capabilities;

- enable IDC leaders to develop a broader understanding of information as a warfighting capability.

Commands are requested to forward a prioritized list of nominees to Mr. Rich Voter (NAVCYBERFOR). Eligible personnel include Active and Reserve Component O6/O5, E9/E8, and Senior Civilians (GS-15/14 or equivalent) in key IDC positions.

Past IDC courses have benefitted greatly from inclusion of leaders from across the extended Information Dominance family including: USMC, USCG, NCIS, and others. The nomination of key leaders from these organizations is highly encouraged and will be considered.

If you have any questions or require additional information, please contact CAPT Livsey-Loeblein at [carol.loeblein@navy.mil](mailto:carol.loeblein@navy.mil) or (703) 855-0367.

Class Dates:

INFORMATION WARFARE BASIC COURSE

Eight week course taught in Pensacola. Provides Information Warfare Professionals with the knowledge for the development of skills, practical application of the tools and techniques necessary to fight and win in the information age, and integrate and execute Information Operations effects for the fleet.

CRYPTOLOGIC RESOURCE COORDINATOR

Two week course taught in Pensacola. Provides prospective battle group CRCs with a formal introduction to organic, local, national, and joint cryptologic resources that are available ISO Battle Group IDTC evolutions and deployment operations.

SEABORNE INFORMATION WARFARE COURSE

Five week course taught in Pensacola. Provides prerequisite knowledge and comprehension of duties that are common to all afloat Information Warfare (IW) officers and senior enlisted assignments. Courses of instruction include information on the following units: Information Operations/Information Warfare, Afloat Systems Management, TACELINT, OPELINT, Targeting, and Cryptology.

**INTELLIGENCE COURSES**

NAVAL INTELLIGENCE OFFICER BASIC COURSE

Twenty week course offered in Virginia Beach. Provides new-accession and lateral transfer U.S. Navy officers, designated Restricted Line, Special Duty Intelligence (163X), with the knowledge and skills to perform as first tour intelligence officers in operational fleet assignments. Students receive training on security and intelligence organizations, basic coordinate systems, basic imagery interpretation, U.S. and threat weapons systems characteristics and employment, electronic warfare and defense analysis, targeting, naval strike force operations, amphibious operations, mission planning, strategic warfare concepts, space-borne sensors, advanced imagery systems and multisensor interpretation, special intelligence, asymmetric warfare, all-source intelligence fusion, operational intelligence fundamentals, and high value individual targeting.

ADVANCED MARITIME OPERATIONAL INTELLIGENCE COURSE

Six-week course taught in Virginia Beach. Trains and educates intelligence officers, enlisted personnel, and civilians how to plan and direct intelligence operations, perform collection operations and management, process and exploit collected information and intelligence, conduct analysis and produce intelligence, and disseminate and integrate intelligence into maritime operations. AMOC will focus on analytical excellence and the "art" of using advanced tools to create depth and generate the timely, relevant and predictive intelligence our forces need in the 21st century. AMOC will produce graduates who are equipped to tackle the analytical, planning, and operational intelligence challenges the Navy faces now and in the future.

NAVY COLLECTION MANAGEMENT COURSE

Three week course taught in Virginia Beach. Provides intelligence personnel the knowledge and skills necessary to perform the various duties of an Intelligence, Surveillance, and Reconnaissance (ISR) Collection Manager at both the Tactical and Operational Levels, with an overview of ISR Collection Management (CM) at the Strategic Level.

**NAVAL OCEANOGRAPHY COURSES**

SENIOR METOC OFFICER AFLOAT

Two week course taught in Norfolk and San Diego. Provides METOC managers afloat with the knowledge and skills necessary to execute tactical decision-making processes in support of Carrier and Expeditionary Strike Group operations. The focus is on the integration of METOC considerations into CSG/ESG decision-making processes. An overview of METOC support structure, community expectations, and requirements are included. The SMOA course is taught by a post-sea tour 1800 officer and incorporates real life observations, experiences, and lessons learned.

**SPACE COURSES**

SPACE 200 (A-531-0200/CDP: 05RF)

Space 200 is the NSSI's mid-career course for space professional education.

It develops space professionals who think critically about the application of space power. The course investigates three major areas: Space Systems Engineering, Space Power and Space as a Contested Environment. In each area students actively participate in exercises challenging them to determine what to do given the dynamics and uncertainly of the national security environment. Space 200 is 4 weeks long and is scheduled 17 times a year.

Contact a course authority, the NSSI (<https://www2.peterson.af.mil/nssi/CESET/nssi/schedule.htm>), or NAVCYBERFOR liaison office Colorado Springs ((719) 593-8794 ext 270 or 281) for more information.

SCHEDULE

SPACE 300 (A-531-0300/CDP: 05PM)

Space 300 is the NSSI’s capstone course for space professional education.

It develops space professionals who understand national policy considerations and strategic thought within an international geopolitical environment. Students will be able to critically address space acquisition capabilities, and power at the operational and strategic levels across the range of military operations as well as space power’s strategic contributions to national security. Space 300 is 3 weeks long and is scheduled 12 times a year. Contact a course authority, the NSSI (<https://www2.peterson.af.mil/nssi/CESET/nssi/schedule.htm>), or NAVCYBERFOR liaison office Colorado Springs ((719) 593-8794 ext 270 or 281) for more information.

SCHEDULE

ADVANCED SPACE OPERATIONS SCHOOL (ASOPS) ASOpS offers many courses tailored to the operational warfighter. The most popular courses for Navy personnel are listed below, but are by no means all inclusive. Visit the school website at <https://www2.peterson.af.mil/nssi/CESET/asops/index.htm> for a complete listing, class convening schedules, prerequisites, and more details.

SPACE FUNDAMENTALS COURSE (SFC) (A-531-1112)

SFC is a two-week space familiarization course convened 9 times a year for military and civilian personnel with little or no space experience who work in an operations or space support role. Students will develop a fundamental understanding of capabilities, limitations and vulnerabilities of space systems. Target audience: Officers: O-1 to O-6; Enlisted: E-5 to E-8; Civilians: GS-9 to GS-15; Most attendees will have very limited space knowledge/experience.

SCHEDULE

SPACE AND MISSILES INTELLIGENCE FORMAL TRAINING UNIT (SMIFTU) (A-531-1111)

The Space and Missiles IFTU offers newly assigned space Intelligence specialists a broad-based understanding of the basic space environment, orbital dynamics and their limitations, mission areas related to space operations, specific U.S. space system development, along with continually updated country threat briefings and current subjects of space intelligence interest. In addition, members are exposed to specific systems, their designs and the mission areas these platforms are tasked to support. The curriculum also includes entry level space applications and practical exercises. SMIFTU is 3 weeks in duration, convened 4 times per year.

SCHEDULE

SPACE OPERATIONS EXECUTIVE LEVEL COURSE (SOC-E) (A-531-1113)

SOC-E is a 1.5-day course designed for senior-staff personnel, commanders and senior-ranking individuals (O-6, E-9, GG/GS-15, YC-03 and above) new to the space operations career field, or those simply requiring a refresher course in the capabilities, limitations and vulnerabilities of critical DoD, national, civil and commercial space systems. Target Audience is senior-staff personnel, commanders and senior-ranking individuals (O-6, E-9, GG/GS-15, YC-03 and above) new to the space operations career field, or requiring a refresher course in the capabilities, limitations and vulnerabilities of critical DoD, national, civil and commercial space systems. SOC-E is 1.5 days long, convened 6 days per year. A mobile version is also available.

SCHEDULE

SATELLITE COMMUNICATIONS ADVANCED COURSE (SATCOMAC) (A-531-1116)

The Advanced Space Operations School (ASOpS) course is being offered. See ITBTP for all information.

SATCOM Advanced Course is a 3-week course designed to provide in-depth SATCOM expertise to space professionals in efforts to enhance their system knowledge to constructively influence SATCOM development, acquisition, employment and sustainment and craft innovative TTPs - all translating to the delivery of more effective SATCOM combat capabilities to warfighters.

This course will cover topics such as SATCOM systems application, employment, and warfighter-related capabilities, limitations, vulnerabilities (CLVs) and effects. The target audience is broad, to include all services, but is limited to those in the satellite communications field.

SCHEDULE

DIRECTOR OF SPACE FORCES COURSE (DIRSPACEFOR OR DS4) (A-531-1117)

The DIRSPACEFOR course is a five-day course designed to provide AFSPC selected senior leaders (0-6 and above), education and training in preparation to serve as the senior space advisor to the COMAFFOR or COMAFFOR/JFACC. Emphasis is placed on AOC operations and the role the DIRSPACEFOR plays in integrating space into theater operations and advising the JFACC on Space Coordinating Authority role. Offered twice a year, target audience ranks O4-O7.

SCHEDULE

**NAVAL POSTGRADUATE SCHOOL OPPORTUNITIES**

NAVAL POSTGRADUATE SCHOOL-RESIDENT PROGRAM

Purpose: To provide top tier, graduate education to DoD military officers and civilians. The IP community currently has quotas in the following curricula: Space Systems Operations, Space Systems Engineering, Computer Science, Joint Command, Control, Communications, Computers, Intelligence Systems, and Information Technology Management. Learn more at www.nps.edu Contact your detailer for in-resident opportunities.

Schedules: Rolling admission process

NAVAL POSTGRADUATE SCHOOL-DISTANCE LEARNING PROGRAM

Purpose: To broaden the professional and intellectual horizons of students, preparing them to assume leadership roles in tomorrow's defense environment. Opportunities exist in the following programs:

\* Fundamentals in Information Systems Technology (eFIST)

http://www.nps.edu/Academics/GeneralCatalog/414.htm#o431

\* Information Systems and Operations (ISO)

http://www.nps.edu/Academics/GeneralCatalog/414.htm#o429

\* Information Systems Technology (IST)

http://www.nps.edu/Academics/GeneralCatalog/414.htm#o430

\* Systems Analysis (SA)

http://www.nps.edu/Academics/GeneralCatalog/414.htm#o440

\* Systems Engineering (SE)

http://www.nps.edu/Academics/GeneralCatalog/316.htm#o356

\* Space Systems (SS)

http://www.nps.edu/Academics/GeneralCatalog/316.htm#o347

\* Human Systems Integration (HSI)

http://www.nps.edu/dl/Cert\_Progs/HSI.asp

\* Knowledge Superiority (KS)

The following supported Degree Program can be obtained entirely online:

* Master's of Computing Technology (MCT)

http://www.nps.edu/Academics/GeneralCatalog/414.htm#o417

The following CED3 supported Degree Programs can be obtained synchronously:

\* Systems Engineering Management--Product Development Leadership Education for the 21st Century (SEM-PD21) Degree Program

http://www.nps.edu/Academics/GeneralCatalog/316.htm#o355

\* Master of Systems Analysis (MSA) Degree Program

http://www.nps.edu/Academics/GeneralCatalog/414.htm#o444

\* Master of Science in Systems Engineering (MSSE) Degree Program

http://www.nps.edu/Academics/GeneralCatalog/316.htm#o353

\* Master of Science in Space Systems Operations (MSSSO) Degree Program

http://www.nps.edu/Academics/GeneralCatalog/316.htm#o322

* Master of Science in Electronic Systems Engineering (Electronic Warfare (MSESE-EW) Degree Program

http://www.nps.edu/Academics/GeneralCatalog/316.htm#o322>

Schedules: Rolling admission process. See www.nps.edu <http://www.nps.edu/> for more information.

**National Defense University**

[www.ndu.edu](http://www.ndu.edu)

CIO curriculum:

[www.ndu.edu/icollege/pcs/pcs\_cio.html](http://www.ndu.edu/icollege/pcs/pcs_cio.html)

IP OCM

CAPT(s) James Darenkamp

[james.darenkamp@navy.mil](mailto:james.darenkamp@navy.mil)

901.874.2846 (DSN 882)

**NAVCYBERFOR IP Community Sponsor Contacts**

Mr. Joe Sullivan

757.417.6722 X2 (DSN 537)

[Joseph.c.sullivan@navy.mil](mailto:Joseph.c.sullivan@navy.mil)

LCDR Ken Romo (SKILLPORT/IAWF Issues)

757.417.6750 (DSN 537)

[kenneth.romo@navy.mil](mailto:Henry.knight@navy.mil)

NAVCYBERFOR fax: 757.417.7902 (DSN 537) (for qual/AQD requests)

**IDCOE/NPS Contacts**

CAPT Jennith Hoyt

831.656.2228

[jehoyt@nps.edu](mailto:jehoyt@nps.edu)

**SPACE CADRE**

CAPT Patrick Owens

[patrick.owens@navy.mil](mailto:patrick.owens@navy.mil)

**Flag Officer Contact Information**

The following contact information for our IP Flag Officers and their assistants is provided below:

**RADM Simpson**

LT Brad Hatcher

[ervin.b.hatcher.mil@mail.mil](mailto:ervin.b.hatcher.mil@mail.mil)

301.225.6010

**RDML Webber**

LCDR Michelle Layne

[sylvia.layne@navy.mil](mailto:sylvia.layne@navy.mil)

240.373.3640

**RDML Herbert**

LCDR Seth Taylor

[seth.f.taylor@navy.mil](mailto:seth.f.taylor@navy.mil)

757.417.6769 (DSN 537)

**RDML Bond**

Major Justin Miller, USAF

NORAD/NORTHCOM J6

[justin.miller@northcom.mil](mailto:justin.miller@northcom.mil)

719.556.8146

**OCM AND SENIOR DETAILER**

IP Senior Detailer

CAPT Katherine Mayer

[Katherine.Mayer@navy.mil](mailto:Katherine.Mayer@navy.mil)

IP Junior Detailer

LCDR Wilfredo Cruz-Baez

[wilfredo.cruzbaez@navy.mil](mailto:wilfredo.cruzbaez@navy.mil)

LDO/CWO Detailer

LT Eric Dobson

[anthony.e.dobson@navy.mil](mailto:anthony.e.dobson@navy.mil)

Civilian Military Assistant

Lucille Tate

[lucille.tate@navy.mil](mailto:lucille.tate@navy.mil)

Phone Numbers

Voice: ***901*.*874.3993*** (DSN 882)

Fax: 901.874.2744

NPC Customer Service Center: 1.866.U.ASK.NPC

**Regional Captain Contact Information**

The following contact information for our IP Regional Captains is provided below:

**AFGHANISTAN**

CDR Steve Wendelin

[steven.m.wendelin@afghan.swa.army.mil](mailto:steven.wendelin@navy.mil)

**BAHRAIN**

CAPT Kathy Creighton

[kathy.creighton@me.navy.mil](mailto:kathy.creighton@me.navy.mil)

**COLORADO SPRINGS, CO**

CAPT Joe Spegele

[joseph.spegele@northcom.mil](mailto:joseph.spegele@northcom.mil)

**DJIBOUTI**

CDR Steve Jacobs

[Steven.jacobs@usafricom.mil](mailto:Steven.jacobs@usafricom.mil)

**EUCOM**

CDR Robby Schimelpfening

[robby.schimelpfening@eucom.mil](mailto:robby.schimelpfening@eucom.mil)

**FLORIDA (includes Georgia)**

CAPT Gerry Slevin

[gerard.a.slevin.mil@mail.mil](mailto:gerard.a.slevin.mil@mail.mil)

**FT MEADE/ANNAPOLIS, MD**

CAPT Jeff Link

[jeffrey.p.link.mil@mail.mil](mailto:jeffrey.p.link.mil@mail.mil)

**HAWAII**

CAPT John MacMichael

[john.macmichael@navy.mil](mailto:john.macmichael@navy.mil)

**JAPAN (includes IPs in western Pacific)**

CAPT Veronique Streeter

[veronique.streeter@fe.navy.mil](mailto:veronique.streeter@fe.navy.mil)

**MID-SOUTH (includes TN, TX, IL, MS)**

CAPT Kathy Mayer

[katherine.mayer@navy.mil](mailto:katherine.mayer@navy.mil)

**MONTEREY, CA**

CDR James Watson

[jamesjwatson@gmail.com](mailto:jamesjwatson@gmail.com)

**NAPLES, IT**

CAPT Sandra Jamshidi

[sandra.jamshidi@gmail.com](mailto:sandra.jamshidi@gmail.com)

**NEWPORT, RI**

CDR Todd Mullis

[todd.mullis@nwc.edu](mailto:todd.mullis@nwc.edu)

**NORFOLK/HAMPTON ROADS**

CAPT Danelle Barrett

[danelle.barrett@navy.mil](mailto:danelle.barrett@navy.mil)

**PACIFIC NORTHWEST**

CAPT Brian Pearson

[pearson.brian@cvn72.navy.mil](mailto:pearson.brian@cvn72.navy.mil)

**SOUTHERN CALIFORNIA**

CAPT Craig Goodman

[craig.goodman@navy.mil](mailto:craig.goodman@navy.mil)

**STRATCOM (Nebraska)**

CAPT Peter Falk

[falkp@stratcom.mil](mailto:falkp@stratcom.mil)

**WASHINGTON, DC**

CAPT Scott Margulis

[scott.margulis@osd.mil](mailto:scott.margulis@osd.mil)

**VIRTUAL IP MENTORING GROUP (for Reservists and those not in a geographic area with easy access to monthly meetings)**

CAPT Tom Follo

[thomas.follo@navy.mil](mailto:thomas.follo@navy.mil)

1. Joint Publication 3-12, Cyberspace Operations (Final Coordination), 10 April 2012, page 93, GL-4 [↑](#footnote-ref-1)
2. Ibid, page 93, GL-4 [↑](#footnote-ref-2)
3. Information Dominance (N2N6) Quarterly Briefing, 13 September 2010 [↑](#footnote-ref-3)
4. http://www.federalnewsradio.com/?nid=398&sid=2709897 [↑](#footnote-ref-4)
5. Department of Labor, Bureau of Labor Statistics states that the total number of information security analysts, web developers, digital forensics professionals, and computer network architects combined = 272,670 (0.21% of 128MM), 2011 [↑](#footnote-ref-5)
6. Defense Strategic Guidance, Sustaining U.S. Global Leadership: Priorities for 21st Century Defense, January 2012, page 11. [↑](#footnote-ref-6)