AG's CELEBRATE 90TH BIRTHDAY

SPOTLIGHT ON NAVAL METEOROLOGY & OCEANOGRAPHY
2 My Domain
RDML Webber

17 Room for Improvement - Cybersecurity Practices in the Fleet
NAVCYBERFOR develops and promulgates Cybersecurity Readiness Manual.

18 WOCC Senior Staff Training Opens Doors in the Navy
Course helps Navy CWO4 learn about strategic-level studies and joint operations.

20 A to Z Within Fleet Response Training Plan
Naval OPSEC Support Team shares results and identifies common deficiencies.

21 Naval Meteorology & Oceanography Command
A pictoral of the Navy’s Feet Weather Center - Norfolk.

23 AG’s Celebrate 90th Birthday
Rating’s initial job of weather forecasting expands over the decades.

25 San Diego MET Forecasts for NASA Test
Team initiates NASA’s Orion boilerplate test for underway recovery.

27 Navy Oceanographers Access Technology to Benefit the Fleet
New technologies provide better information and enhance decision-making.

29 Rise of Social Media
Awareness is key in understanding vulnerabilities of Facebook and other media.

32 Resources/Roadmaps for Cyber Warriors
NCTAMS LANT shares Information Dominance tricks of the trade.

34 Commander, Navy Cyber Forces
RDML Diane E.H. Webber

Deputy Commander
Mr. Mark E. Kosnik

Public Affairs Officer
CDR Matt Klee

Editor-in-Chief
Mr. George D. Bieber

Managing Editor
Miss Jacky Fisher

Graphics Editor &
Visual Information Specialist
Mr. Robin D. Hicks

InfoDOMAIN is the professional online magazine of Navy Cyber Forces that promotes the advancement of Information Dominance through an open exchange of better practices, tactics and current and future strategies to meet the global challenges of the information warfare domain.

Information contained in InfoDOMAIN does not necessarily reflect the official views of the U.S. Government, the Department of Defense or the Department of the Navy. Editorial content is prepared by the Public Affairs Office of Navy Cyber Forces. Articles for publication in InfoDOMAIN should be submitted through the appropriate command representative. Security and policy review must be completed by submitting commands before submissions can be considered for publication. Address all correspondence to Editor in Chief, InfoDomain, Navy Cyber Forces, Public Affairs Office, 115 Lake View Parkway, Room 135, Suffolk, VA 23435-3228; telephone (757) 203-3082, DSN 312-668-3082, FAX (757) 203-3442. Comments or queries may also be forwarded via e-mail to: george.bieber@navy.mil

FRONT COVER: July 1 marked the 90th birthday of the Aerographer’s Mate or AG rating. This Edition of the InfoDOMAIN features Fleet Weather Center-Norfolk; a brief re-cap on AG’s history; San Diego’s Mobile Environmental Team; Oceanographers’ technology and several key changes in leadership throughout the Naval Meteorology & Oceanography realm. For information and pictures of METOC & NMOC see Pages 21-31. (Photo Illustration by Robin Hicks)
Admiral’s Parting Thoughts...

When I first arrived to Navy Cyber Forces, my commitment to the Fleet was to generate Information Dominance (ID) readiness and ensure the optimum support for manning, training and equipping Navy operational forces. The dedicated team of professionals at NAVCYBERFOR more than met that challenge and delivered impressive results across the globe. As our organization transitions to becoming the ID Type Commander effective Oct. 1, 2014, and I pass the reins to the incoming Commander, RADM Matt Kohler, there is still much work to be done to continue to improve on that readiness.

As we move forward with significant changes in the coming year, be innovative, resourceful and help your fellow Sailors through the transition. It’s an all hands effort to identify and solve the problems that often come with change. Be ever vigilant to put the Fleet first and “do no harm” to our operational commanders’ ability to successfully execute their missions.

I am confident that your efforts will provide greater capabilities and readiness to the Fleet and that we are on the leading edge in terms of what ID brings to the Navy across all warfighting domains. As I pass the torch on to new leadership, I ask that you carry on with our efforts towards delivering greater integrated ID capabilities to operational forces. I am deeply moved by your dedication and commitment, and it has been my privilege to serve alongside you here at NAVCYBERFOR and throughout my Navy career. Stay strong, stay focused and continue to excel. 🎯

“Be ever vigilant to put the Fleet first and ‘do no harm’ to our operational commanders’ ability to successfully execute their missions.”

RADM Diane E.H. Webber, Commander, NAVCYBERFOR

...AT A GLANCE

RADM Matthew J. Kohler is assuming command of Navy Cyber Forces this October. A native of Erie, PA, Kohler graduated from Indiana University of Pennsylvania in 1983 and was commissioned an Ensign in 1984 through the Aviation Officer Candidate School, Pensacola, FL. His operational tours include Aviation Intelligence Officer for Fighter Squadron (VF) 102 at Naval Air Station Oceana, Virginia Beach, VA; Assistant Chief of Staff for Intelligence (N2) for Commander Amphibious Squadron One in San Diego; and Assistant Chief of Staff for Intelligence (N2) for Cruiser Destroyer Group Two/USS George Washington Battle Group based in Norfolk, VA.

Kohler’s shore tours include: Fleet Ocean Surveillance Information Center Commander in Chief/U.S. Naval Forces Europe in London, England; Bureau of Naval Personnel in Washington, DC; Joint Warfare Analysis Center in Dahlgren, VA; United States Special Operations Command in Tampa, FL; Joint Interagency Task Force South in Key West, FL.

Previous flag assignments include National Security Agency at Fort Meade, MD; Deputy Commander, U.S. Fleet Cyber Command/Deputy Commander, U.S. 10th Fleet in Fort Meade, MD, Deputy Director of Naval Intelligence/Director, Intelligence Operations, OPNAV N2/N6. He assumed his previous position as United States Africa Command Director of Intelligence (J2) in March 2013. 🎯
Information dominance will be vital in future conflicts

Our Navy’s forward presence protects the interconnected global system of trade and reinforces the security of the U.S. economy. Our engagement around the world reassures allies, builds trust with partners and friends, and prevents and deters wars. We are the foundation of the nation’s “away game,” endowed with operational agility, possessed with innovative resourcefulness, and armed with credible combat power to be used where it matters, when it matters. Sustaining our global primacy requires that we dominate the battlespace on, above, and below the surface of the sea, as well as outer space. However, successfully commanding, controlling, and fighting our forces in these areas requires dominance in the information domain, to include the electromagnetic spectrum and cyberspace.

The name we’ve given to this concept—information dominance—is still new and unfamiliar to some, but it’s indispensable to Fleet operators as a critical force multiplier. It’s no longer just an adjunct to warfighting. It is warfighting.

Alpha and Omega

Imagine a hypothetical scenario in which U.S. naval forces respond when the country of Omega, long envious of Alpha’s energy resources, attempts to overrun Alpha’s defenses and seize its oil fields. Due to our array of unmanned systems, multi-intelligence sensor and processing capacity, and robust cyber capabilities, the U.S. Fleet detects Omega’s intentions early and quickly succeeds in attaining dominance of the information battlespace without Omega’s knowledge.

Leveraging operational surprise through mastery of the electromagnetic spectrum (EMS), the U.S. forces arrive on station before Omega can launch its initial assault into Alpha. The U.S. commander is equipped with a penetrating knowledge of Omega’s force disposition, intentions, capabilities and vulnerabilities. Our Fleet’s unexpected arrival causes Omega to pause momentarily, providing time for U.S. forces to finalize their preparation of the battlespace and conduct offensive operations in cyberspace and the EMS.

U.S. oceanographers possess unmatched knowledge of the physical battlespace, including expected weather conditions, currents, sea-states and tides. The U.S. commander knows where Omega’s assets are likely to operate and when and where they cannot operate. This insight allows the U.S. commander to position his or her forces and deploy Intelligence, Surveillance and Reconnaissance (ISR) resources. He also knows the effect of the physical environment on propagation and ducting, enabling the U.S. Fleet’s Information Technology and Information Warfare professionals to tailor the friendly communications posture and electronic-warfare support measures most effectively.

The U.S. commander sees the EMS from Omega’s perspective, as well as his own, allowing the luxury of maneuvering freely and rapidly through the spectrum and take offensive actions to Omega’s disadvantage.

U.S. intelligence capability has given our forces keen insight into Omega leadership’s mission objectives, intent, C4ISR systems and fine-grain targeting data on Omega’s submarines, minefields and missile launchers. This allows the U.S. Fleet to evade detection and targeting during the critical early stages of the confrontation. Similarly, our knowledge of Omega network capabilities and force disposition allows us to implement preplanned responses that negate and defeat Omega’s offensive efforts in cyberspace.

Through a combination of kinetic strikes and network degradation, U.S. forces are able to diminish Omega’s command and control and destroy its limited maritime-patrol/over-the-horizon targeting assets, as well as its antiship ballistic- and cruise-missile capability. As a consequence, the confidence of Omega’s leadership is shaken by a lack of situational awareness, degraded command and control over its forces, and distrust of...
its sensors and warfighting capabilities, especially its non-kinetic assets. At this point, the Omega commander is overwhelmingly disadvantaged, unable to execute the planned invasion of Alpha, or strike a symbolic blow against the U.S. Fleet.

This obviously simplified scenario illuminates the operations that information dominance delivers.

What It Is

Our formal definition of information dominance is the operational advantage gained from fully integrating the Navy’s information functions, capabilities and resources to optimize decision making and maximize warfighting effects. In other words, it means delivering decision-quality information where it matters and when it matters. It fosters freedom of maneuver in all domains, and integrates our fires, which may be projected through the network (or cyberspace or the electromagnetic (EM) spectrum) for soft kill, or delivered through the physical environment for hard kill. To make these capabilities possible, we will master the information domain, just as we’ve mastered the air, surface, undersea and space domains. Accordingly, information dominance focuses on:

• Robust and agile Command and Control (C2) in all operating environments.
• Superior knowledge of the battlespace, both the physical environment, as well as threat capability, disposition and intent.
• Projecting power through the integration of kinetic and non-kinetic effects.

We refer to these three elements, or pillars, as assured C2, battlespace awareness and integrated fires. Through them, information dominance creates decision superiority, provides asymmetric advantage, and enhances the lethality of our deployed forces with non-kinetic options. By design, the pillars correspond to the Chief of Naval Operations’ three tenets:

Warfighting First: With assured C2 and enhanced battlespace awareness, commanders are able to definitively assess threats and determine their most efficient and effective courses of action using the range of kinetic weapons and non-kinetic effects available to them.

Operate Forward: Ensuring freedom of maneuver in cyberspace and the EM spectrum, and assuring the ability to direct operations and coordinate actions in contested environments is paramount for successful operations forward. Our evolving ISR assets combined with our established meteorology and oceanography capabilities contribute to battlespace awareness by delivering information on the threat and physical environments, ensuring effective Fleet operations. Reliable connectivity to the global information grid allows us to operate forward. What’s more, the global disposition of our forces contributes essential information (e.g., intelligence, weather, etc.) for dissemination to forces forward.

Be Ready: Maintaining a continuously refreshed awareness of the operating environment, including threat capabilities and intentions, allows us to be predictive, enabling our ability to prepare and coordinate well in advance of forward operations.

The critical element of the information dominance definition is integration. Blending the attributes of intelligence, surveillance, reconnaissance, oceanography, meteorology, networks, cyber, electronic warfare (EW), etc., allows for better planning, smarter decisions, and earlier results. Aligning the related restricted-line communities of Naval Oceanography, Information Warfare, Information Professional, Intelligence and the Space Cadre into the Information Dominance Corps (IDC) has likewise advanced our concept and capability development, and improved data and system interoperability. To borrow a cliché, in the case of Navy information dominance the whole...
is much greater than the sum of its parts. Comprehending it, however, requires a slightly deeper dive into the three pillars.

Assured Command and Control

Assured C2 makes the issuing of orders to distributed forces and the coordination of maneuver and fires across the warfighting domains (air, land, sea, space, cyberspace and the EMS) possible. It provides the ability to monitor the status of our forces and assess the effectiveness of our fires. It is indispensable to forward operations and securely networks our forces in all threat environments.

Practically every major system in the Fleet is “networked” to some degree, including most combat, communications, engineering, and position, navigation and timing capabilities. Cyberspace extends that network across joint and Navy business and industrial-control systems. While this connectivity provides unprecedented speed, agility and precision, it also opens attack vectors for determined adversaries. Therefore, assuring our C2 requires a robust, protected, resilient and reliable information infrastructure afloat, ashore and overseas.

Maintaining a protected transport infrastructure securely links our forces ashore and afloat in permissive, contested and denied C2 environments. Another key component is resilient networks that withstand the barrage of attacks we see today and expect to grow. We are increasing the integration and interoperability of the sea and shore segments of our enterprise architecture through technologies such as cloud computing. Moreover, we are aligning with the DOD’s Joint Information Environment and the Intelligence community’s Information-Technology enterprise frameworks to enhance interoperability and expand our ability to share and receive information from joint and national partners. Assured Positioning, Navigation and Timing (PNT) provides for the safety of navigation, targeting and C2 across our platforms and systems.

In his seminal 2012 Proceedings article, “Imminent Domain,” Chief of Naval Operations Admiral Jonathan Greenert observed that “[a] culture of electromagnetic silencing and understanding of electronic signatures will have to permeate our efforts if we are to command the EM-cyber environment.” Toward the objective of mastering the EM environment, the emerging Real-Time Spectrum-Operations system will allow us to monitor the spectrum continuously, identify conflicts, determine solutions, and differentiate between unintentional interference and intentional jamming. As current prototypes evolve, we’ll leverage this knowledge to create effects and “hide in plain sight.”

In a nutshell, the assured C2 pillar touches almost everything we do, afloat and ashore. It complements the battlespace awareness and integrated fires pillars and provides the communications we require in the most demanding conditions. We are progressing down this path with our Next-Generation enterprise network, Consolidated Afloat Network Enterprise System, Automated Digital Network System and Navy Multiband Terminal programs.

Battlespace Awareness

This is knowledge of the operating environment that allows the warfighter to find, penetrate and predict the enemy’s operations by making better decisions faster. It gives us home-field advantage at the away games. It requires a superior understanding of the battlespace, to include the physical environment, cyberspace, the EM spectrum and the threat. It also requires immediate and continuous access to essential information that updates the operational picture, facilitating prediction and decisive action. The warfighting advantage created by battlespace awareness comprises functions and payloads that are interoperable and capable of rapid upgrade relative to the threat. Battlespace awareness capabilities therefore require advanced means to sense, collect, process, exploit and disseminate information in real time.

In the case of sensing and collecting, we leverage manned and unmanned, fixed, mobile and distributed systems.

... continued on Page 6
and we coordinate across the force through a seamless communication architecture. Our manned capabilities include the EP-3 aircraft, surveillance towed-array vessels and fixed surveillance systems. Unmanned systems, such as our MQ-4C Triton Unmanned Aircraft System, MQ-8B/C Fire Scout Vertical Takeoff Unmanned Aerial Vehicle, and Unmanned Carrier-Launched Airborne Surveillance and Strike System, are key components because of their persistence and the reduced risk to our manned platforms and crews. Their increasing numbers and missions ultimately give us more options and greater operational flexibility. By stressing payloads over platforms, we are able to quickly leverage standard interfaces and common control systems, which also permit rapid technology upgrades, allowing us to pace the threat.

In processing, exploiting and disseminating, our path to superior decisions starts with ensuring that data derived from our own sensors, as well as from joint and national sources, are delivered to deployed commanders when needed. This requires sophisticated tools that pull multiple sources of data with common standards into a single picture, process high volumes of information, and save thousands of man hours both afloat and ashore at Maritime Operations Centers (MOC), Maritime Intelligence Operations Centers, the Naval Oceanographic Office, and the Office of Naval Intelligence, among others.

To further develop battlespace awareness, we are expanding the Pacific Fleet’s Intelligence Federation model Navy-wide. The federation optimizes intelligence manning, collection and communication assets. It will leverage the full range of information dominance capabilities, supplementing Navy regional expertise with the capabilities and assets of the combatant commands, combat support agencies, the intelligence community, and our allied partners. As these initiatives mature, we see the MOC becoming the essential platform for sustained battlespace awareness.

With a long-term focus on a critical physical aspect of battlespace awareness and emphasis on the Arctic, the Oceanographer of the Navy, RADM Jonathan White, led the recent update of the Navy Arctic Roadmap to ensure our readiness for potential contingencies in the polar north. Similarly, RADM White’s office is preparing for the future effects of climate change, conducting vulnerability assessments of Navy coastal infrastructure and supporting DOD strategic planning with respect to potential impacts on the global security environment.

**Integrated Fires**

This is the ability to project power across the kill chain. It blends non-kinetic effects with traditional kinetic weapons in order to fully exploit and, when necessary, attack adversary vulnerabilities. To be successful, it requires two mutually supporting functions:

- **Disrupting/Denying/Defeating Red Fires.** That is, preventing the adversary from initiating kinetic and non-kinetic operations of his own by disrupting his C4ISR and targeting ability.
- **Enhancing Blue Fires, which requires dynamic collaboration across missions, domains and with other services.** This coordination permits the exploitation of the EMS as a weapon and the integration of targeting and fire-control capabilities for increased weapon range, effectiveness and lethality. It includes the evolving electronic-warfare and offensive cyber weapons that complement our air, surface and subsurface kinetic weapons.

We are making major investments in the Fleet’s ability to maneuver freely and fight in the EM environment. Central to this investment is the concept of EM Maneuver Warfare or EMW, which anticipates future conflicts in the battlespace created where cyber and the EM spectrum converge. Core to EMW is a complete awareness of our EM signature and others’ in real time; the ability to manipulate our EM signature to control what others can detect, maximize our ability to defeat jamming and deception, and guarantee our use of the spectrum when needed; and use of EM and cyber capabilities as non-kinetic fires to inhibit adversary C4ISR, targeting and combat capabilities. Successful EMW requires the seamless integration of the communications, command-and-control, signals intelligence, spectrum management, electronic warfare and cyberspace disciplines to permit our freedom of action across the spectrum.

**The Information Dominance Corps**

The 2010 consolidation of the OCEANO, Information Warfare, Information Professional, Intelligence, and Space Cadre officer communities— together with their enlisted, Reserve, and civilian counterparts—established a professional and technically diverse corps that is rapidly coalescing into

... continued on Page 7
New Era . . . continued from Page 6

a formidable warfighting force. They aren’t the only Sailors executing information dominance as a warfare discipline, but they are its principal practitioners, and they bring extremely valuable skills and specialized knowledge to the fight. Moreover, they are taking on leadership roles at the highest levels, as exemplified most recently by ADM Mike Rogers’ confirmation as Commander, U.S. Cyber Command and Director, National Security Agency/Central Security Service; as well as VADM Jan Tighe’s command of Fleet Cyber Command/U.S. 10th Fleet.

Considering the exponential rate of change in technology and its corresponding impact on both our own and our adversaries’ capabilities, the unique talents and abilities within the IDC are increasingly critical. While we have made concerted efforts to protect and strengthen the IDC’s deep technical expertise in its traditional skill areas, we are mindful that broadening the experience of our members yields more capable information dominance leaders. As a consequence, we’re inserting common core training relevant to the broader information dominance mission at set points in the IDC career path. Beginning with accessions and again at mid-career and senior points, we are bringing IDC members together with their peers to expand their interdisciplinary knowledge, build personal relationships, and engender an esprit de corps unique to this mission. Additionally, we’re actively managing career paths and cross-detailing IDC leaders to broaden their experience and perspective. This mostly involves commissioned officers now, but will include senior enlisted and civilians as we define the process. The intended effect is a deliberate transformation of the IDC from a multidisciplinary group to a fully functional interdisciplinary corps.

Information dominance is much bigger than the IDC, but the corps’ leaders are the ones who understand it best. They are fully integrated with the Fleet and are gaining recognition as warfighters in their own right. From its beginnings in 2010, the corps has quickly matured, aggressively adapting to its warfighting mission. It has greater operational relevance and more warfighting credibility than ever before. Most important, IDC members are increasingly accepted as legitimate warfighters by traditional operators.

The Information Dominance Type Command

Finally, we are establishing Navy Information Dominance Forces, an integrated type command dedicated to the discipline. With an initial operational capability of Oct. 1, 2014, this new type command will subsume the existing Navy Cyber Forces command and integrate many of the man, train and equip elements of Fleet Cyber Command, the Office of Naval Intelligence, and the Navy Oceanography and Meteorology Command. It will initially be led by a two-star IDC flag officer who will report to the Commander, U.S. Fleet Forces Command, right alongside the existing platform type commands.

The establishment of this command is another step in information dominance’s maturation since its 2010 birth. It’s the logical next phase in the discipline’s evolution and, as we know from our experience with the platform type commands, it’s consistent with the Navy’s time-tested approach to institutionalizing other warfare areas. As it did with the advent of naval aviation, submarines and nuclear power, the Navy is adapting to the technology of the age and maintaining its warfighting advantage.

The type command will integrate the man, train and equip aspects of information dominance across the Fleet, coordinating closely with the platform type commands, the numbered fleets, systems commands, and Strike Groups to ensure information dominance is fully considered throughout the readiness kill chain. Given the network’s universality within the larger shore-based Navy, the type command will eventually extend its man, train and equip reach beyond the Fleet to facilitate information dominance readiness Navy-wide. It’s an enormous undertaking—one that we must embrace with vigor.

Information dominance is a reality. Senior leaders across the Navy, including the CNO as well as Admirals William Gortney and Harry Harris, consider it essential to our sustained forward presence, credible combat power and global influence. We are at the dawn of a new era in naval warfare, and information dominance is central to our continued prominence in an increasingly asymmetric and dangerous world. It is the way of the future for Information Age warfare. 

EDITOR’S NOTE: Reprinted from Proceedings with permission; Copyright (c) 2014 U.S. Naval Institute/www.usni.org.
Live Your Dream & Earn a Graduate Degree

OPNAVINST 1520.24c, Officer Scholarship Program

The Olmsted Scholar Program provides two years of graduate study using a foreign language while providing overseas cultural and travel opportunities and often leads to a graduate degree at a foreign university. Applicants should be available to commence language training in summer/fall 2015, begin study at a foreign university in 2016, and complete study in 2018.

A Navy selection board will convene in October 2014 to select up to 12 nominees from which the Olmsted Foundation board of directors will consider and select Navy scholars in March 2015.

This unique scholarship opportunity supports the Secretary of Defense’s emphasis on developing language skills and regional cultural knowledge across the force. Global affairs require language proficiency/regional expertise within the Navy. Although this scholarship program is open to all regions of the world, priority will be given to those whose language choice would fill a current or projected critical need of the Navy.

To utilize these scholarship opportunities, the Navy is looking for young leaders who display all the qualities of dedicated career officers who aspire to command. In particular, fitness reports must demonstrate strong leadership qualities, solid overall performance, and strong promotion potential.

Additionally, while a minimum grade point average is not specified, all applicants must have demonstrated scholastic ability in their undergraduate transcript. Factors such as academic major, participation in varsity sports, steady scholastic improvement, etc., are taken into consideration when reviewing transcripts. Applicants must also have a strong desire to learn a foreign language and to live, study and travel abroad. Finalists may be interviewed by the Olmsted Foundation.

Active-duty list regular or full-time support officers with the designators 111x, 112x, 113x, 114x, 131x, 132x, 181x, 182x, 183x, and 310x with the following qualifications may apply for the program:

- Applicants must have at least three years of commissioned service but not more than 11 years of total active federal service as of April 1, 2015.
- Superior scholastic ability as demonstrated in an undergraduate transcript.
- Foreign language aptitude background or experience in chosen countries/languages is not required.
- Exceptional military professional performance.

Applications should be addressed to:
Center for Personal and Professional Development (CPPD)

Voluntary Education Detachment
Code N2A2 Olmsted
6490 Saufley Field Road
Pensacola, FL 32509-5204

The required essay should be limited to one-page explaining why the officer wants to be an Olmsted Scholar. A preference list of up to 10 countries (with no more than two universities and locations per country) where the applicant would like to study must be included. All applicants should read the additional guidance provided by the Olmsted Foundation on their website under overseas studies before compiling their list.

To support submission of Defense Language Aptitude Battery (DLAB) scores, commands may obtain DLAB testing information from:

Commanding Officer
Center for Information Dominance
(CLREC-NFLTO Code N01)
Pensacola, FL 32511-1386

By calling (850) 452-6529/DSN 459 or via e-mail at language testing@navy.mil. Information on the Graduate Record Examination (GRE) may be obtained from the local Navy college office or at www.gre.org.

This is a three-year program for which career timing is an important consideration. All applicants must contact their detailer for counseling on the career impact of participation in the Olmsted Scholar Program. In order to be considered by the Navy selection board, a written/signed statement from the detailer must be included in the nomination package. Recommended statement is as follows: “I, (detailer rank, name and title), have advised (applicant rank, name) of the potential career impact of this program.”

Application packages, with command endorsement and detailer statement, must reach CPPD voluntary education detachment, Code N2A2-Olmsted, NLT August 29, 2014. Required DLAB/GRE scores and official college transcripts may be submitted by separate correspondence to reach CPPD Code N2A2-Olmsted NLT Sept. 12, 2014.

This prestigious program is key to preparing young officers for future leadership roles as the Navy faces the ever-increasing challenges and complexities of today’s international environment.

Olmsted scholars achieve fluency in a foreign language, gain a deep appreciation for foreign cultures, acquire regional expertise by studying and traveling overseas, and may earn a liberal arts master’s degree. All eligible and interested officers are urged to consider this important program and visit the Olmsted Foundation’s website at www.olmstedfoundation.org for additional details, including important information regarding the country/city/university preference list.

Point of contact is Ms. Billie Colonna, CPPD, (850) 473-6061/DSN 753; or via e-mail billie.colonna@navy.mil.
CWOs Bridge Gap

Centuries Old Seamanship to Cyber Warfare Leadership

By Jacky Fisher, NAVCYBERFOR Public Affairs

Jack of all trades, master of none - anyone could do that. But to be a technical expert in your chosen field while serving in a time-honored leadership role...now that takes talent! The Chief Warrant Officer (CWO) program is the Navy’s premier platform to showcase both trade technical expertise and leadership skill sets, honed only by serving at least 12 years in the enlisted ranks and being a member of the Navy’s Chief Petty Officer (CPO) community.

In 2010, the Secretary of the Navy approved the establishment of the Cyber Warrant Officer designator to join the other Information Dominance Corps (IDC) CWO programs: Information Systems, Cryptology and Intelligence. The Cyber Warrant designator was created to support the development of the Navy’s cyber workforce as well as the increasing demand for cyber technical expertise. Until recently, only two Cyber CWOs were serving. But this year, the Navy increased that number to six. A local cyber Sailor, ITC Eric Nelle stationed at Navy Cyber Defense Operations Command in Suffolk, VA, was one of four newly selected Cyber Warrant Officers.

The reason for the spike in numbers for the Information Dominance designator can be attributed to the increasing demands to staff the IDC with more Sailors as well as commissioned officers to lead those Sailors. Another reason for the increase is the recent decision to drop the requirement to have a 9308 (Navy Interactive ON-NET (ION) Operator - Navy Enlisted Code (NEC)), which represented only 10 work roles in the Cyber Warrant designator.

“Very few people held the 9308 NEC,” said CWO5 Michael Sill, Manpower Resource Sponsor and Fleet Synthetic Training Officer, Navy Cyber Forces. “So the applicant pool for Cyber Warrant was really small over the past four years.” An Information Warfare (IW) Warrant Officer, Sill was commissioned in 1999 and has more than 30 years’ service in the Navy.

“In reassessing the work roles for Cyber Warrants, we realized that only a small number of jobs required the 9308 NEC. So we decided to do away with it as a prerequisite and open up the aperture,” said Sill. “Cyber Warrant is now open to CTNs (Cryptologic Technician – Networks) and ITs (Information System Technicians), as long as they have the necessary credentials and certifications to apply for Cyber Warrant. As a board member on the FY15 LDO/CWO IP Board, I was very pleased with the overall increase and competitiveness in Cyber Warrant applicants over that of past years as a result of changes we’ve incorporated in the program eligibility.

I’m confident that the four new Cyber Warrants we selected this year will bring in the exact talent that the community is seeking for this field.”

With various career paths in the Navy to earn the privilege and accept the responsibility to wear khaki – as a CPO, regular commission and new accession officer, Limited Duty Officer (LDO), and CWO, to name a few - what’s the difference, really? Only as a CWO can a Sailor serve from seaman to commissioned officer as a leader, technical manager and Subject Matter Expert (SME) throughout their entire career; a career that can span for more than three decades. Combining enlisted and commissioned service, CWO4s and below can remain on active duty for 30 years; CWO5s can serve for 33 years.

(Left to right) CWOs Sillivan, Sill and MacClanahan combined military time is more than nine decades of Navy service. (Photo by Robin Hicks)
WARRANTS . . . continued from Page 9

“The Chief Warrant Officer community continues to seek strong leaders who have the technical expertise, self-confidence, decisiveness and flexibility to keep up with the speed of change facing the IDC and the Navy,” said CW5 Timothy Sullivan, Technical Advisor for Fleet Readiness and Requirements, Navy Cyber Forces. “The role of a Chief Warrant Officer is unique and clearly a privilege. In addition to being leaders in their community, they are expected to maintain their technical proficiency and apply that knowledge to advise senior leadership and drive change where it is required.”

Sullivan, commissioned in 2001, was recently promoted to IW CW5, and has more than 28 years’ service in the Navy. “One of our top priorities is placing our CW5s in the right billets where they will have the strongest impact. The Cyber Warrant Program is a clear example of how our community takes this seriously,” said Sullivan. “The recent changes in the program have allowed the selection of our most talented cyber experts and will clearly strengthen our cyber workforce.”

The Chief’s mess is geared towards ‘sailorization’ – the ‘care and feeding’ of junior Sailors, ensuring their personal development gets on track and stays on track. Chiefs are known and are depended upon to manage the enlisted community as a whole and develop those Sailors to one day serve in critical roles such as division and department chiefs and eventually, Command Master Chiefs. Behind every great leader is a seasoned mentor, another critical task best performed by Chiefs. The tried and true answer to a question when the correct answer is not at the ready – Go ask the Chief. Junior officers must learn myriad skill sets: technical, managerial and even administrative, to name a few. Who better to answer that call than a seasoned Chief.

In the Navy, Chiefs operate as technical experts in their rates and as mentors for traits not found in any book for the most junior Sailor to the most junior officer. Warrants, serving as managers and leaders, bridge the gap between the Chiefs community and Line Officers. It’s “truly the best of both worlds,” said CW5 Montana McClanahan, Deputy NetOps5, NETWARCOM.

“There is a Chief Warrant Officer - the word ‘Chief’ is first for a reason. It demonstrates a level of credibility.”

CW5 Montana McClanahan, Deputy NetOps5, NETWARCOM

“Chief Warrant Officer community continues to seek strong leaders who have the technical expertise, self-confidence, decisiveness and flexibility to keep up with the speed of change facing the IDC and the Navy.”

CW5 Timothy Sullivan, Tech Advisor for Fleet Readiness & Requirements, NAVCYBERFOR

“Cyber Warriors . . . continued on Page 11

Mess when we take the same oath as Line Officers,” said McClanahan. “But we never entirely leave the Chiefs community. That is the challenge and the beauty of being a Warrant.”

Currently the Warrant community Navy-wide is 1,624 strong and is on track to increase that number to 2,000. The dynamic political and world stages today have the potential to lead to further future growth. “As Warrants we must continuously step up our game to lead from the front,” said McClanahan. “It is our charge to stay technically proficient so we can effectively lead those ‘cyber warriors’ from the front.”

From network defense to information assurance, ‘cyber’ influences every community within the Navy, and Navy’s Cyber Warrant Officers are at the forefront of those actions. “There’s an app for everything” in today’s Navy - ships navigation, food and medical services, payroll, communications between platforms, communications between platforms and those on the ground … every aspect in carrying out the Navy’s mission on a day-to-day basis. With the Navy so reliant on computers, the opportunity for vulnerabilities and intrusions is great.

Just follow the news. Cyber issues are affecting multiple aspects of our lives for military and civilian sectors alike, which equates to growth opportunities and promotion. It is never too early in a Sailor’s career to prepare to compete for a CWO designation in the appropriate ID program that correlates to one’s rate.

“Your career is not a 20 year long FOD (foreign object damage) walk down, so don’t look to the left and right at your peers. Advancement takes personal initiative and motivation,” McClanahan said. “Seek those positions that will challenge you professionally and . . . continued on Page 11
personally, always be looking forward and upward.”

Three CWOs with more than nine decades of experience and knowledge and their message to IDC Sailors is consistent and clear - maintain your technical expertise and leave the ‘well-rounded’ tasks for the line officers. To become a Warrant and stay viable, a Sailor must stay in billets that are within their technical expertise and that will allow them to continually improve.

‘Stay in your technical expertise’ does not equate to pigeonholing oneself. Diversity in terms of operational tours helps an IDC Sailor expand within their technical career. Serving on a variety of platforms – ships, submarines, expeditionary units and in the aviation community – is the only way Sailors have the opportunity to earn a warfare pin. And in this respect, it’s easy to spot a broad-based Sailor - one with multiple warfare pins, in addition to their ID warfare pin.

The CWO community has undergone many changes since its inception over the centuries and continues to evolve to meet the needs of today’s Navy (see sidebar - History of Warrants). Longitude/latitude and grids on a map no longer delineate the front lines and battlefields. After land, sea, air and space, a fifth dimension of warfare has been recognized – cyberspace. ID CWOs and IDC Sailors stand vigilant in this dynamic environment as forerunners as this fifth dimension of warfare evolves.

To find out more about the application process or ask eligibility questions, read the OPNAVINST 1420.1B, Enlisted To Officer Commissioning Programs Application Administrative Manual, dated Dec. 14, 2009 and the applicable governing documents outlined under the reference tab.  

EDITOR’S NOTE: CWO5 Sullivan has transferred to Fleet Forces Command and serves as a Staff Action Officer for N84/N23.  

History of Warrants  
Warrants are as old as navies themselves – starting with the British Navy. In the 14th and 15th centuries, war at sea was not common. When ships were required, vessels belonging to traders and merchants were drafted in to service. The ship would be commissioned and a captain was put in command. The land-bound, part-time Soldiers lacked the necessary skills to pilot, navigate or handle a ship. The crew needed to be augmented with a ship’s master, his principal officers and Sailors, better known as “swabbers.” Commoners with specific and critical skills were employed and issued royal Warrants that bound them to serve the king.

When the colonies were breaking away from the British Empire and the Revolutionary War was imminent, the colonies used the British naval establishment to model their own Navy. Congress agreed to construct 13 frigates Dec. 13, 1775. Commissioned and Warrant Officers led the colonies’ Navy.

By the 1800s, commissioned Warrant grades - CWO to “rank with but after ensign” - were introduced to the Navy. World War I saw the need for Warrant ranks to meet the demand of the rapidly evolving technology of the time. This need grew larger at the onset of World War II.

The Limited Duty Officer (LDO) community came on line and for a decade, from 1948 until 1958, to work shoulder-to-shoulder with the CWOs. In 1958 Senior and Master Chief Petty Officers were added to the Career Compensation Act.

The “Williams Board” in 1959 set about to study the impact of all these grades and concluded CWOs should be phased out. Four years later that decision was reversed by the “Settle Board” that determined the phased out Warrants created a void not effectively filled by the increased numbers of LDOs and Master Chiefs – “a void incompatible with the Navy’s needs for more, not fewer, officer technical specialists.”

Several viewpoints are credited for the origin and meaning of the term ‘Mustang’ when given to a Sailor who attains a commissioned rank.

‘Mustang’ depicts a wild horse that, once captured and saddled broken, can tow the line. But he will always retain that natural streak of independence. Having been wild and free, mustangs are considered more intelligent with an innate survival instinct not seen in pampered thoroughbreds.

Today’s Navy Warrant Officers proudly wear the mantle of ‘Mustang’ as they continue this exceptional legacy.
PENSACOLA, FL— RADM Michael S. White, Commander, Naval Education and Training Command (NETC), recently made his first official visit to the Center for Information Dominance (CID).

White is traveling to Navy Learning Centers throughout NETC’s domain to learn firsthand about the training being delivered to the Fleet.

Conveniently located only two miles from Naval Air Station Pensacola, where NETC is based, CID is one of the earlier learning centers White visited.

Based at Corry Station, CID is the Navy’s learning center that leads, manages and delivers Navy and joint forces training in information operations, information warfare, information technology, cryptology and intelligence.

With nearly 1,300 military, civilian and contracted staff members, CID oversees the development and administration of 202 courses at four commands, two detachments and 14 learning sites throughout the United States and Japan. CID provides training for approximately 24,000 members of the U.S. Armed Services and allied forces each year.

Following a short presentation from CID Commanding Officer, CAPT Susan K. Cerovsky, on the overall mission and scope of CID, White visited two classrooms and a lab at CID Unit Corry Station.

While there, he received briefs from several instructors including: Ship’s Signal Exploitation Equipment Increment "F" Maintenance Course Supervisor, retired Master Chief Petty Officer and CID Civilian of the Year, Tom Priest; Joint Cyber Analysis Course Manager, CTN1 Jason Taylor; and A+ Instructor, IT1 Ryan Butler.

CID Unit Corry Station instructors teach 38 courses of instruction within the Cryptologic and Information Systems Technician ratings, with about 12,500 students graduating from various schools annually, making this the largest command within the CID domain.

“Our CID instructors are the reason why CID continues to produce the world’s finest information dominance warriors,” Cerovsky said. “When our graduates leave here, they are fully prepared to join the Fleet and to perform their mission, thanks to the hard work by these first-rate instructors.”

At the end of his tour, White had an opportunity to chat with IT “A” school students who were in a computer lab. The students were practicing building and repairing Ethernet or CAT 5 cables. Similar to oversized telephone lines, these cables are used to connect computers to networks.

White also received a quick tutorial from SR Vincent Owens, 19, of Frenchville, PA, on assembling new Ethernet cables. Owens showed White how to make a new cable by deciphering the wiring scheme and attaching an RJ-45 connector to each end of the cable.

Owens said he was honored to meet White, and that he never expected to meet an admiral, let alone have a one-on-one conversation with one.

Owens said he was pleasantly surprised that White was genuinely interested in the work he and his classmates were doing in the IT lab, and to have the opportunity to show off some of his newly-acquired technical skills.

“It was a really cool experience to be able to show... continued on Page 13
Breaking Language Barriers, CIDU Instructor Earns Senior Language Professional of Year

MONTEREY, CA—A Center for Information Dominance Unit (CIDU) Monterey instructor was selected as the Navy’s 2013 Senior Language Professional of the Year. Chief of Naval Operations (CNO) ADM Jonathan Greenert recognized CTIC(IDW) Pamela “Kassandra” De Voto, an Arabic Military Language Instructor (MLI) at CIDU, in an official Navy message.

“It is important to recognize the role that Language, Regional Expertise and Culture (LREC) play in modern naval operations,” Greenert wrote. “In today’s operational environment, LREC is central to everything from Humanitarian Operations to building lasting relationships with our foreign partners.”

De Voto, a native of Chicago, spent most of her childhood moving around. For a period of time she lived in Italy, where she became fluent in Italian.

Her aspiration to learn multiple languages was influenced growing up in a polyglot household.

“I like language; always have,” said De Voto. “In fact, I still haven’t caught up to my parents in number of languages spoken.”

In December 2001, De Voto graduated from Purdue University on a Reserve Officers’ Training Corps (ROTC) scholarship with dual degrees in Aerospace Engineering and Computer Engineering, with a minor in Linguistics.

A year later, with two college degrees under her belt, she decided to join the Navy as an enlisted linguist. She attended Basic Arabic at the Defense Language Institute (DLI) in Monterey with follow-on training at Goodfellow Air Force Base, TX.

In May 2011, she reported aboard CIDU as an instructor in the DLI Middle East School One (ME1). During her tour at DLI, she qualified as a Senior MLI, an Enlisted Information Dominance Warfare Specialist, and a Master Training Specialist.

Her language expertise was put to use in numerous program reviews and curricula development projects for all DLI’s current Arabic programs, said De Voto. She also made use of her computer and technical skills in a number of projects, including the development of electronic delivery for tests and the design of new student management software for use throughout DLI.

In June this year, De Voto reported to Annapolis, MD, as the first enlisted Sailor to work in the International Programs Office of the United States Naval Academy.

“I have always taken pride in doing my job well, and doing that requires that you know how to use the tools of the trade,” she said. “The fact that I like this particular toolset is just an added bonus.”

CIDR Michael Cooney, CO of CIDU-Monterey, poses with CTIC Pamela De Voto after awarding her Senior Language Professional of the Year for 2013.

For more information about CID, please visit http://www.netc.navy.mil/centers/ceninfodom/.

RADM White how to make a cable,” Owens said. “It was neat to be able to show someone besides an instructor or fellow student what I’ve been learning in IT “A” school.”

Most of the students White spoke with at the IT lab were new accessions, or Sailors who only a few weeks earlier were attending boot camp at Recruit Training Command Great Lakes, IL.

White said he was impressed by the quality and speed of these students as they make the transformation from recruits to full-fledged Information Systems Technicians, and he gave the credit for that transformation to the dedicated and talented CID instructors.

“The quality of the instructors just amazes me,” White said. “That they are able to mold these young men and women into productive IDC Sailors in such a short time speaks volumes to their quality.”

After five months of intense training at CID this class of IT “A” school students will join the Fleet later this summer as the newest crop of cyber warriors within the Information Dominance Corps (IDC).

“Their motivation energizes me every day,” White said. “CID is clearly an incredibly professional organization that’s building the future of our Fleet. The Information Dominance Corps have a growing role and the important training being conducted by CID can’t be under stressed here.”

For more information about CID, please visit http://www.netc.navy.mil/centers/ceninfodom/.

NETC . . . continued from Page 12
PENSACOLA, FL – Center for Information Dominance (CID) Commanding Officer, CAPT Susan K. Cerovsky, commissioned her nephew into the Navy Reserves June 9, 2014.

Standing in front of a World War I-era field ambulance at the National Museum of Naval Aviation, on board Naval Air Station (NAS) Pensacola, Cerovsky, who has served the U.S. Navy for nearly 29 years, passed on a Cerovsky family tradition of military service when she swore her nephew, Christopher Michael Cerovsky, into the U.S. Navy Reserves as a future Medical Corps Officer.

“I’m so proud of him,” Cerovsky said. “He is so smart, so squared away and so motivated. I’m sure he will make an outstanding naval officer.”

Christopher, 21, graduated from Mississippi State University Magna Cum Laude, this past spring with a Bachelor’s degree in biological sciences and a minor in microbiology. He also is a member of the prestigious Shackouls Honors College.

Christopher will be attending Temple University School of Medicine at Philadelphia, this fall. His medical education will be fully paid for thanks to his recent acceptance into the Navy’s Health Professions Scholarship Program (HPSP) in exchange for service as a commissioned Medical Corps officer.

Navy Officer Recruiting Station Pensacola Medical Officer Recruiter, LT Juan Serrato, explained that the HPSP is a highly competitive program.

“It’s really a proud moment when you see fine young men and women enter the Navy through the HPSP scholarship program,” Serrato said. “The academic excellence that this young man displayed helps ensure the future success of Navy medicine.”

Upon graduation from medical school in four years, Christopher will be promoted to an active duty Lieutenant, and he will serve in the Navy for eight years.

Not only has Cerovsky passed along her tradition of Naval service, she also presented what will undoubtedly become a family heirloom - the Naval Education and Training Support Command training manual “Useful Information for Newly Commissioned Officers,” which she received when she was sworn into the Navy nearly three decades ago to ENS Cerovsky.

“I don’t think they publish this manual in printed form anymore,” Cerovsky said. “But it still contains useful information for newly commissioned officers.”

ENS Cerovsky said he was humbled to be presented with such a thoughtful gift along with the honor of being sworn in by his aunt, the CID Commanding Officer.

“I am just overwhelmed,” Christopher said. “I’m grateful to be able to carry on our family tradition of naval service. Thank you all for being here today. I’ll do my duty to the best of my abilities and I won’t let any of you down.”

Also present during the ceremony was ENS Cerovsky’s father, Roger Cerovsky; his mother, Alison; his brother, Brian; his grandparents, Shirley and George Cerovsky; and uncle, CDR Evan Hipsley.

(Clockwise) CID Commanding Officer, CAPT Susan K. Cerovsky, swears ENS Christopher Michael Cerovsky into the U.S. Navy Reserves as a future Medical Corps Officer June 9, 2014, at the National Museum of Naval Aviation on board Naval Air Station Pensacola. CAPT Cerovsky, signs her nephew, ENS Cerovsky’s, commissioning paperwork. Family members pose with ENS Christopher Cerovsky following his swearing in. Christopher is the family’s newest naval member.
translated law-enforcement training materials benefit bangladesh uniformed services

by mc1(t) jason t. poplin, fleet combat camera pacific

pensacola, fl – joint interagency task force-west (jiatf-west) completed three weeks of maritime law enforcement training with bangladesh’s uniformed services in the port city of chittagong back in february 2014.

personnel from border guards bangladesh, bangladesh coast guard, the u.s. embassy in dhaka, and jiatf-west participated in classroom training.

course materials, consisting of briefings, lectures and student guides, were all available in both english and bangla. the navy’s center for language, regional expertise and culture (clrec) in pensacola, fl, provided translation services.

according to lcdr stephen bower, officer in charge of jiatf-west’s integrated maritime skills training team, having course materials available in the students’ native tongue is critical to their ability to comprehend complex maritime topics and enhances the potential for these students to train others in the future.

“In a force where the majority of the members have little to no English skills, having a guide in their native language is absolutely essential,” bower said. “by providing text, pictures and diagrams in their native language, the students were able to comprehend the topics more accurately and quickly than if the training were conducted through an interpreter alone.”

During previous international training events, contracted translation services have proven costly, difficult to arrange within time constraints, and were of varying quality, according to bower. however, he had high praise for the translation service provided through clrec.

“both the officers and interpreters had participated previously in u.s. government-sponsored instruction,” bower said. “the feedback i received was that our products were the best they had seen with both the slides and books comprehensively translated by someone with an obvious high level of proficiency in both english and bangla.”

clrec offers an array of language, regional expertise and culture training and support solutions for the navy and other department of defense (dod) entities preparing for maritime missions.

clrec director christopher wise said that with respect to jiatf-west’s bi-lateral training mission, more than just general terms and everyday phrases and expressions were required.

“The clrec team was able to coordinate accurate translations of technical, specialized terminology tailored specifically to jiatf’s training mission,” wise said. “this assisted all involved to communicate more clearly on a range of topics from technical aircraft terminology, to law enforcement and military doctrine, to the inner workings of an improvised explosive device.”

Since its inception in 2006, clrec has become the focal point of language and culture awareness training provided to u.s. fleet maritime forces.

established aboard the center for information dominance (cid) at corry station in pensacola, fl, clrec’s mission is to build language skills and understanding of foreign cultures among u.s. sailors to reduce culture shock, help foster close relationships between the u.s. navy and america’s global partners, and make u.s. service members better ambassadors of our nation.
PENSACOLA, FL – For the third year in a row Center for Information Dominance (CID) has received the Navy’s Retention Excellence Award. In addition to CID, all four of CID’s subordinate commands – CID Unit Corry Station, CID Unit Monterey, Navy Marine Corps Intelligence Training Center (NMITC), and Fleet Intelligence Training Center (FITC) – also were selected as repeat winners for the Retention Excellence Award.


“These successful commands have implemented and maintained the six key programs that form the foundation of a successful retention effort,” Moran wrote in his message. “These programs, when properly implemented and executed are a strategic investment in our Navy’s future. Congratulations and well done.”

“This award – the third year in a row for the Center for Information Dominance – is yet another indicator that CID continues to be one of the Navy’s top performing learning centers,” CID Command Master Chief Travis Brummer said.

CID Commanding Officer, CAPT Susan K. Cerovsky, said she was proud of her Sailors, instructors and staff for winning this award for the third year in a row, and continuing a CID tradition of keeping quality Sailors in the Navy.

“Bravo Zulu to our commands,” she said. “This is really a team effort and by reaching these retention goals, we are doing our part to fulfill the CNO’s priority of meeting current challenges while building a relevant and capable future force.”

CID Career Counselor, Eric Tremaine, said the award was the result of a unified team effort across the CID domain to retain the best and brightest Sailors and instructors.

“This achievement would not have been possible without the phenomenal Sailors who volunteered to serve as collateral duty career counselors throughout our domain,” he said. “These counselors have guided our Sailors with exceptional results.”
A recent article in Federal Computer Week (FCW) noted a “cultural shift” in the Department of the Defense, and especially the Navy, in seeing computer networks as more than just tools and warfighting enablers. Rather, they are now a part of the combined battlespace which we operate. VADM Jan Tighe, commander of U.S. Fleet Cyber Command and the Navy’s 10th Fleet, recently spoke at a Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) & Networks conference in Arlington, VA, where she said that while the Navy’s senior leadership is keenly aware of the cybersecurity challenges ahead, “As you get lower down the food chain, it gets a lot more spotty – there are pockets of understanding, there are pockets of non-understanding.”1 Clearly, there is room for improvement in how we practice cybersecurity in the Fleet.

It is for this reason that Commander, Navy Cyber Forces (NAVCYBERFOR), the Navy’s Capability Type Commander (TYCOM) for all things “Cyber,” created the Commander’s Cybersecurity and Information Assurance Handbook in 2011 with updated yearly revisions thereafter. Through the success of the Handbook as an awareness and compliance tool, and in light of the Fleet’s understanding of day-to-day cybersecurity best practices, NAVCYBERFOR developed the Cybersecurity Readiness Manual (CSRM) for the Fleet as a tool for Cybersecurity Workforce (CSWF) managers and technicians.

The CSRM augments tactical directives (such as Navy Computer Tasking Orders, or CTOs), already-established Planned Maintenance System (PMS) actions, guidance from Systems Commands (SYSCOMs), and industry best practices from the SANS Institute on the 20 Top Critical Security Controls (CSCs).2 It provides managers and technicians with a checklist to guide their routine operations, and recommended procedures for carrying out those checklist actions to improve their cyber defensive posture.

This manual is not the end-state for Fleet cybersecurity readiness, but rather the beginning. NAVCYBERFOR will continue to publish quarterly updates for further refining of the manual through collaboration between various stakeholders such as; the Space and Naval Warfare (SPAWAR), the PEOs and other systems commands, Fleet Cyber Command, platform TYCOMs and the Fleet. Their feedback and collaboration is absolutely critical to ensuring our Sailors have the right guidance in front of them to use the tools at their disposal effectively.

All commands should use the CSRM and provide feedback. It can be downloaded from the NCF N75 Portal, https://usff.portal.navy.mil/sites/cyberfor/n7/n75. Note that the document is For Official Use Only (FOUO) and requires Common Access Card (CAC) logon to access. All manner of collaboration on the continued evolution of this document is welcomed and encouraged.

Cybersecurity is not just a technical concern, it is a cultural and leadership concern. RADM Wray, in a Naval message preceding his retirement from active duty and as the President of the Board of Inspection and Survey (INSURV) in 2013, said it best when he charged commanders and Commanding Officers to “Build a culture of technical rigor on your ship,” and “Instill within the minds and hearts of your crew those essential attributes and practices which will make them ready.”3 This gets straight to the heart of why the Commander’s Cybersecurity and Information Assurance Handbook and CSRM were created – to provide the guidance necessary to inform this cultural shift, and enable Sailors to start building on the best practices available to keep our networks secure.

Works Cited:

About the Author:
LT Howard is an Information Professional (IP) Officer of the Navy’s Information Dominance Corps (IDC). He is assigned to Commander, Navy Cyber Forces (NAVCYBERFOR) in Suffolk, VA. He is a former enlisted Information Systems Technician and, following commissioning, a Surface Warfare Officer, with more than eight years of combined at-sea experience operating Information Technology (IT) systems and programs.
FORT RUCKER, AL -- There are several joint forces training centers around the U.S. and even though Fort Rucker is not one of them, a fair share of Airmen, Sailors and Marines can be seen on the installation from time to time.

And even though there are programs currently set up that welcome warriors from other services, a new joint operations initiative is beginning to take root at the Warrant Officer Career College (WOCC), here.

U.S. Navy CWO4 Carl Smith, an information professional assigned to USS Abraham Lincoln (CVN 72), graduated in May from the Warrant Officer Senior Staff Course, where he learned about strategic-level studies and joint operations.

“We had to go clear up to the Pentagon to get the approval. We had to make provisions to make sure no one was taking a seat away from an Army Soldier,” said CWOS5 Todd Blake, WOCC staff and senior staff course director. “It is as beneficial for our students as it is for the Navy to have the joint workings here, especially when we do the practical exercises. As much information...
comes from the students as it does the instructors.”

Blake said the inclusion of other service members is a win-win for everyone, and that there is interest from the Navy and the Marines. “The more the merrier, because the more we have in each class the more that everyone can benefit on our side and theirs,” he said. “Training like this makes it really become three dimensional.” Smith said he is very proud to be representing the Navy in the class, and that he is thankful he was able to secure a spot.

“Working jointly is important because we are working to meet one common goal and we are working at this level in the same areas,” he said. “We have to work together and be focused as one. If we can intermingle and work with one another, we will interact within themselves.

“Naval officers would greatly benefit from this joint training. Getting the lingo down was challenging at first, learning all the acronyms and such, but now when I work jointly with other branches, the work will go much smoother,” he said. “I wish I would have gotten this course much sooner. I would have greatly benefitted from it before I deployed with a joint staff operations group for communications at Camp Victory (Iraq).”

Smith said allowing other warrant officers to receive the training is something that the military needs to look into to see the big picture and think out of the box for policies, procedures and strategies, adding that communication between the services is key.

Smith’s classmate, CWO4 David Behm, Operations Company Headquarters, 20th Infantry Division, Pennsylvania National Guard, said that when senior leaders deploy, they are working with other service branches, and that they have to understand how they function and interact within themselves.

“The training environment hasn’t changed at all. He has been able to offer insight that we might not have gotten,” said Behm. “He has brought a different view and perspective to class discussions. We need to have this insight on what the other services are doing and how they operate.”

Students focus on the big picture during the course, where they are taught how to be senior staff officers and advisers to senior staff officers, and is not military occupational specialty specific, said Blake.

This program on integrating other service members into Army classes is brand new for WOCC, with Smith being only the second individual from another service branch to go through.

Last year, another Naval officer was the initial candidate. That officer, CWO4 David Miller, felt there was a gap in training and education for the Navy CWO since there are no formal plans in place to prepare W2s in the Navy for “additional responsibility, leadership roles or operating in the joint environment.”

Miller began searching for military education opportunities, and after meeting several dead ends discovered the WOCC, which he believed institutionalized the profession of the Warrant Officer corps, and had a “formalized process for ensuring all warrant officers receive professional military education from the time of their acceptance as a Warrant Officer through their promotion to CW05,” he wrote.

After many months of struggling to get approved to attend the Warrant Officer Senior Staff Course, he arrived at Fort Rucker ready to learn and pave the way for future Navy and Marine Warrant Officers.

“I am a better officer for having attended the course,” said Miller. “I definitely improved my depth of knowledge.”

During Chief of Staff of the Army Gen. Raymond Odierno’s visit to the college last year, he stated that he believes the course “should be Joint” and that he hoped to “see more Warrants from the other services in the future.”

With support from the Chief of Staff, the course director, Fort Rucker senior leaders and WOCC faculty and instructors for the course to be open to all Warrant Officers, Fort Rucker might be seeing more Navy and Marine khaki around the installation.
Over the past several years, the Naval OPSEC Support Team (NOST) has been challenged with incorporating OPSEC into the Fleet Readiness Training Plan (FRTP). Whether lack of documented policy, limited inspection criteria, or just other shipboard competing requirements, OPSEC has faced challenges being a focus in the Fleet.

Leveraging the Navy Information Operations Command (NIOC) Norfolk’s Electronic Warfare Technical Guidance Unit (EWTGU) assessment of Fleet units, the NOST introduced an easy method of building an OPSEC program, from start all the way to annual assessment during the FRTP. As a result, ships increased compliance with OPNAVINST 3432.1A training and assessment requirements, are better prepared to incorporate OPSEC into operational planning and increased their readiness and OPSEC posture during deployment.

Prior to or during the 2.0 phase, each unit should have an OPSEC Officer appointed in writing who must attend core OPSEC training per OPNAVINST 3432.1A. The NOST recommends the OPSEC Officer attend the two-day Navy course held in alternating months in Norfolk and San Diego, as well as taught via Mobile Training Team (MTT) in Japan, Hawaii, Washington State and Mayport, FL.

During the 2.1 phase, the NOST will coordinate a ship visit with the unit OPSEC Officer to assist in the development or revitalization of the ship’s program. This is accomplished via a check sheet developed by the NOST and used to identify program status, any best practices or benchmarks, and any areas that could be improved. The NOST will additionally use this opportunity to offer guidance and resources to ensure the ship has all the proper tools and information needed for a successful and sustainable program. An OPSEC assessment completion date and assessment follow-up date will also be set for the unit, usually 30-45 days after the 2.1 visit. The assessment can be completed using the resource CD provided by the NOST or via the Operations Security Collaboration Architecture (OSCAR) on-line risk assessment tool hosted on Secure Internet Router Protocol Network (SIPRNet).

Once a unit completes their assessment, sharing the results with the NOST prior to the pre-coordinated follow-up date will result in minimum impact to the ship’s daily routine as well as allow the NOST to focus on areas of concern, if any. Sharing results also allows the NOST to compile metrics, identifies common program deficiencies throughout the Fleet for mitigation, and provides best practices or recommendations for other units. Upon completion of the follow-up visit, the NOST will generate a final report summarizing the assessment, usually within 45 days after the visit. Providing the report to the Immediate Superior in Command (ISIC) will assist OPSEC Officers in mitigating any deficiencies prior to deployment, ultimately improving the units overall OPSEC posture.

For more information about OPSEC within the FRTP, contact the NOST at opsec@navy.mil or 757-417-7100. NOST products and resources can also be obtained via the following links:

- www.facebook.com/navalopsec
- www.slideshare.org/navalopsec
- www.youtube.com/usnopsec

By Robert “Scott” Carey, Naval OPSEC Support Team
Picture Story by Robin Hicks, NAVCYBERFOR Public Affairs

(Below) Sailors on board Fleet Weather Center - Norfolk man the 24/7 watchfloor producing Resource Protection, Optimal Track Ship Routing and weather support for the Fleet and Naval installations. (Clockwise on Page 22) Another angle of Fleet Weather Center-Norfolk’s 24/7 watchfloor. AGAN David Francisco (right) briefs current synoptic weather situation to AG1 Daryl Meer (left) on the Fleet Weather Center-Norfolk watchfloor. AGC Asya Andrews works with a Naval Integrated Tactical Environmental System (NITES) laptop. AG2 Adam Hill (right), AG3 Michael Clute (background), and AGAN Victor Germain (foreground) analyze a graphical weather forecast (GWEAX) from the Fleet Weather Center-Norfolk, for an operational unit currently underway. One of four Resource Protection Duty Officers, AG2 Ryan Vaughan prepares weather watches and warnings for Naval installations throughout Fleet Weather Center - Norfolk's area of operation. AGAN David Francisco briefs current synoptic weather situations. AGAN Michael Clute takes an observation using a handheld anemometer.

... continued on Page 22
STENNIS SPACE CENTER, MS -- July 1 marked the 90th birthday of the Aerographer’s Mate or AG rating, established for the Navy’s fledgling aviation enterprise to ensure the Navy had a dependable source of weather forecasting for aviation safety.

Although AGs still forecast the weather for flight operations, they have added considerably to their portfolio during the last 90 years. New areas of support include hydrography, oceanography, Unmanned Underwater Vehicle (UUV) operation and sonar data processing. As part of the Information Dominance Corps, AGs enhance battle-space awareness by providing the characterization, forecast and impacts of the environment.

“Our mission sets grew and changed as the needs of the Fleet changed and we continued to expand our capabilities. But the one constant through that change is that we serve as the Navy’s operational scientists,” said Master Chief Aerographer’s Mate Ken Walker, Naval Meteorology and Oceanography Command (NAVMETOCCOM) Master Chief, the Navy’s senior AG.

Using the latest technology and in addition to aviation, the Navy’s approximately 1,000 AGs play a vital role in all of the Navy’s traditional warfare areas, as well as the new realm of Information Dominance. They also support safety of navigation, the Navy’s humanitarian aid/disaster relief efforts and safety at sea.

They have become the Navy’s accepted experts in the operation of UUVs, which they use extensively in mine warfare operations and hydrography, or bottom mapping for access routes and charting.

“AGs are the backbone of Operational Navy Oceanography. As a group, they are smart and technologically adept. They have always been willing to accept new and additional duties - whatever they have been asked,” said RDML Tim Gallaudet, NAVMETOCCOM commander. “That’s why the job has... continued on Page 24
expanded so much into oceanography, hydrography and Information Dominance - because they were willing and able to learn new things and take on new responsibilities. The U.S. Navy is a more safe and effective fighting force because of the AGs - and I know this to be a fact from my firsthand experiences with AGs in the Persian Gulf, Western Pacific and Mediterranean, Arabian, Yellow and Red seas.”

The rating has come a long way from the first seven-man AG class of 1925 to today’s technologically-savvy members who forecast the entirety of the natural environment and analyze the impacts of specific environmental conditions on a particular platform, weapons system or operation. In 1925, balloons carrying instruments into the atmosphere and airplanes with recording data and weather instruments attached to the wings were considered high tech; the first electric programmable computers were still 20 years away.

Some things have not changed, as AGs still forecast environmental conditions for battlespace awareness. But, more importantly, AGs throughout their history have integrated new technologies into environmental data collection and have continually found more and better ways to optimize warfighting.

Walker said the biggest change in the work of AGs during his 29 years in the Navy is centered on the junior Sailors.

“When I came in the Navy, our A-school graduates were weather observers. The predominance of our work was taking observations, launching weather balloons, plotting charts, tearing teletype data and using communications gear to receive facsimile charts,” he said. “With the ever-growing technological advances a great deal of that work became obsolete. AG-A school was revamped to reflect those changes and the graduates now head to the Fleet as Apprentice Forecasters. This change has allowed us to expedite the timeline for getting our Sailors into AG-C school and back out to the Fleet as Journeyman Forecasters.”

The Navy established the AG rating to ensure a cadre of educated weather forecasting professionals would be available to forecast the weather for the new Naval flight operations. Naval aviation started in 1910, but the weather forecasting rating didn’t start until 1924.

In 1923, LT Francis Richelderfer, a pilot, weather officer and head of the Navy weather desk, recognized that an enlisted rate offering advancement potential was needed for Navy weather forecasting to prosper. The weather office had been plagued by high attrition rates of its enlisted personnel into other specialties or out of the Navy.

The enlisted forerunners of AGs were quartermasters with an aviation specialty. Formal instruction in aviation-related weather courses for the Navy was first taught by Alexander G. McAdie of Harvard University. McAdie coined the term “Aerographer,” so the name of the rating is a constant reminder of the rating’s roots. The rating, initially known only as “Aerographer,” became Aerographer’s Mate in 1942.

The size of the rating has expanded and declined through the years, but the importance of environmental forecasting has not been challenged since the days of McAdie. Environmental forecasting plays a key role in battlespace awareness, one of the three pillars of Information Dominance, so don’t be surprised if AGs are still forecasting the impacts of the environment in another 90 years.

Photo Illustration by Robin Hicks
San Diego MET Forecasts for NASA Test

From U.S. Naval Institute News Editor

The members of the Mobile Environmental Team (MET) from Fleet Weather Center San Diego (FWC-SD) participated in a historic event on USS San Diego (LPD 22), Feb. 18 through 21, when they forecasted meteorological and oceanographic conditions for the Underway Recovery Test (URT) of NASA’s Orion Exploration Flight Test ONE (EFT-1). The MET also launched weather balloons to collect upper air soundings for both on board NASA debris modelers and Mission Control. In addition, the team provided forecasts to enable safe ship and recovery operations.

“We wrote four-day forecasts, and we started writing them 10 days out. At one point during the end-to-end test with Kennedy Space Center, the MET launched, processed and distributed data from five soundings in four hours,” said AGCS(IDW/AW/SW) Eric Windell, the MET leader.

AG1(IDW/AW/SW) David Bernhard wrote an operating area forecast using the Wave Watch 3 (WW3) forecast model, the Navy Global Environmental Model (NAVGEM), and the Navy’s new weather forecast model for San Diego. NASA personnel and embarked staffs from Expeditionary Strike Group 3, Explosive Ordnance Disposal Mobile Unit 3 (EODMU3) and embarked air assets from

The members of the Mobile Environmental Team (MET) from Fleet Weather Center San Diego (FWC-SD) participated in a historic event on USS San Diego (LPD 22), Feb. 18 through 21, when they forecasted meteorological and oceanographic conditions for the Underway Recovery Test (URT) of NASA’s Orion Exploration Flight Test ONE (EFT-1).

Orion will be the next vehicle NASA uses to carry people into space. NASA plans to retrieve the vehicles and their passengers, much as the earliest generation of U.S. manned space flights, after they splash down in the ocean. However, the Orion capsule is larger than the ones from the 1960s and ‘70s, so the space agency has to develop a new retrieval method.

NASA plans to recover the capsule with an amphibious ship, by pulling the capsule into the ship’s well deck. Consequently, NASA wanted to test the ship’s ability to recover the Orion test capsule in several different sea states – calm to as much as eight- to 10-foot seas – in order to understand what was possible when the capsule actually landed from orbit. The MET’s support was the linchpin for the exercise because the MET had to locate different sea states at various places within the exercise’s Southern California operations area and directed San Diego to those areas. The MET had been involved in the nearly year-long planning process for the URT.

The MET also launched weather balloons to collect upper air soundings for both on board NASA debris

The Orion boilerplate test vehicle and other hardware are secured in the well deck of the ship in preparation for the test about 100 miles off the coast of San Diego.

Orion is the exploration spacecraft designed to carry astronauts to destinations not yet explored by humans, including an asteroid and Mars.

... continued on Page 26
Helicopter Sea Combat Squadron Eight (HSC 8) participated as well. The team also used the WW3 forecast model and NAVGEM for the long range predictions necessary for planners and decision makers.

The most critical parameter for the URT was a long-period swell and the effects it would have on the ship and capsule. Additionally, winds were a concern because of the impact on crane operations. A knuckle boom crane was used to deploy 7-meter and 11-meter Rigid Hull Inflatable Boats (RHIB) from EODMU 3, San Diego and USS Anchorage (LPD 23). The RHIBs were necessary to attach cables to the capsule to pull it into the ship’s well deck.

Windell said the plan was to carry the capsule out to sea in the well deck, put it out of the ship and then retrieve it. The URT demonstration provided extensive data on recovery methods. The relationship with the Navy and NASA will continue as NASA proceeds with developing the Orion spacecraft for deep and near space exploration.

**EDITOR’S NOTE:** Fleet Weather Center is an Echelon V command of the Naval Meteorology and Oceanography Command, which is comprised of approximately 2,500 officer, enlisted and civilian personnel stationed around the world. Naval Oceanography is the Navy’s physical maritime battlespace authority, a critical partner across the full range of DoD operations, delivering decision superiority, operational effectiveness and safety to our operational forces.

(Clockwise) Members of the Orion recovery team work to retrieve a test version of Orion’s forward bay cover, a protective shell that fits on top of the crew module, from the Pacific Ocean during an Underway Recovery Test. NASA and U.S. Navy personnel have come together on board the USS San Diego, off the coast of California, to practice the processes they’ll use to recover Orion after its splashdown following its first flight test this fall. (Official U.S. Navy Photos)
New technologies that provide better information and enhance decision-makers’ battlespace awareness can be as critical to victory as superior weapons systems.

Better information for battlespace awareness yields better decisions and enhances operational and tactical decision support to increase warfighting options.

Key pieces of physical battlespace awareness information are predictive weather and ocean forecasts that the Naval Meteorology and Oceanography Command (NAVMETOCOM) provides. Weather and ocean conditions are among the factors that dictate how radar and sonar work and how weapons systems and platforms perform. A person doesn’t have to be a military planner to understand the value of knowing what the weather and ocean conditions will be in the maritime battlespace as the battle forms. Forecasts and forecast-based operational recommendations always need to be faster, more accurate and longer range to affect operations within an adversary’s decision cycle.

“We know operational oceanography has always been a critical part of battlespace awareness, but today with the explosion of technology, Navy resources under pressure, and faced with rapidly changing geopolitical conditions worldwide, we feel a greater sense of urgency in providing our piece of the predictive battlespace awareness part of the information domain strategy,” said RDML Tim Gallaudet, NAVMETOCOM commander.

To better deliver more accurate and longer-range forecasts as part of the information dominance battlespace awareness package, NAVMETOCOM is riding a wave of technological innovation that includes increased supercomputing capability; new, more capable weather and ocean models, a variety of Unmanned Underwater Vehicles (UUVs); more sophisticated sonars and a new generation atomic clock. More advancements are on the horizon.

“The technology is making a level of environmental forecasting possible that we have never been able to do before – global ocean forecast models, fully coupled air and ocean models, models that can produce forecasts in time scales from hourly to seasonal are key to a common operational picture for operational planners and decision-makers,” Gallaudet said.

The increased computing power NAVMETOCOM leverages at the Stennis Space Center, MS, Navy Defense Supercomputing Resource Center or DSRC, one of five Defense Department supercomputer centers and already one of the most powerful supercomputer centers within the DoD, makes developing and operating more accurate weather and ocean forecast models possible. Three new systems installed in 2012, increased the center’s supercomputing processing capability nearly five times to 954 teraflops. Another addition, scheduled this year, will nearly triple the computing power to more than 2,400 teraflops.

The upgrade provides for more robust high-resolution modeling and simulation of global-scale oceanography and meteorology in support of Navy and DoD operations worldwide.

In 2012, Navy oceanographers started running the Hybrid Coordinate Model or HYCOM, the world’s first truly operational global ocean model. HYCOM was developed thanks to the more robust computing power available at Stennis. Navy oceanographers also started operating a new weather forecast model, Navy Global Environmental Model or NAVGEM, that replaced the Navy Operational Global Atmospheric Prediction System or NOGAPS, the former gold standard of Navy weather forecasting models. Ocean and atmospheric modeling efforts also have advanced through the fully-coupled Coupled Ocean/Atmosphere Mesoscale Prediction System or COAMPS®, and the COAMPS® Tropical Cyclone (COAMPS®-TC).

... continued on Page 28
Supercomputing has opened the door to even greater modeling capabilities.

“The increases in computing power that we have seen and have been promised are giving us forecasting capabilities that we never thought possible because of the complex computations required,” said Dr. Bill Burnett, NAVMETOCOM Deputy/Technical Director.

Naval Oceanography needs atmospheric and ocean data to make the models work, to develop the forecasts and to analyze the natural environment – more is better, and newer is better. Consequently, NAVMETOCOM employs an environmental data collection system among the most extensive in the world. Satellites and other sensors feed images and atmospheric and ocean data directly to the supercomputing center. The integration of data and models ensures the products provide enhanced battlespace awareness to operational decision-makers.

Unmanned underwater vehicles, including autonomous undersea gliders have become the newest data collection tools for Navy oceanographers. NAVMETOCOM has developed one of the most sophisticated systems of unmanned underwater vehicle operations in the Navy and has become recognized as the Navy’s expert in the operation of a variety of unmanned underwater vehicles. Navy oceanographers directly support a host of fleet operations using UUVs – mine warfare, safety of navigation, expeditionary warfare, anti-submarine warfare, special operations and humanitarian aid/disaster relief.

“Our Sailors have embraced this unmanned underwater vehicle technology. Their ability to understand, operate and maintain these vehicles is a big reason that we have been able to use and develop this capability,” Gallaudet said.

Navy oceanographers also direct and track a fleet of unmanned ocean gliders throughout the world that collect data leveraged for all Navy operations. The gliders, which have no independent propulsion system, are transported by ocean currents. Oceanographers at the Naval Oceanographic Office, a NAVMETOCOM Echelon IV command, monitor and send instructions to the gliders remotely via satellite.

Post-graduate-level civilian and military oceanographers provide expertise and bring years of experience and volumes of research to bear on specific issues that enhance battlespace awareness for operational decisions. Forward-deployed oceanographers have 24/7 access to reach-back cells on watch floors manned by civilian and military experts.

“Our expertise can go a long way in enhancing the battlespace awareness of the operational commander. We work very hard to give our commanders the ability to operate within an adversary’s decision cycle,” Gallaudet said.
METOC... continued from Page 28

The only part of the NAVMETOCOM portfolio that doesn’t include oceangoaphy and/or atmospheric science is the precise time and astrometry function of the U.S. Naval Observatory or USNAVOBSY, another NAVMETOCOM Echelon IV command. Both precise time and astrometry are vital in targeting, navigation and communications. On an operational level, precise time and astrometry can mean the difference in hitting the targeted building and hitting a building next door or in the next block.

The observatory was established to give Navy ships a time reference point for navigation. Ship captains could set their chronometers by the observatory, and chronometers were necessary to navigation at sea. Today the observatory remains true to its founding, but it has grown with the technology and the development of the science and as a consequence has become an asset not just for the U.S. Navy but for nation as well. The observatory operates and maintains atomic clocks that serve as the basis for the U.S. time standard and provides measurements of planets and stars, both critical for targeting and navigation.

In the past year, the observatory operationalized four Navy Rubidium Fountain Clocks that feed the master clock. Additionally, USNAVOBSY has updated the Earth Orientation Program by the operationalization of the electronic Very Long Baseline Interferometry (e-VBLI) correlation capability.

But while the tools and knowledge have gotten more sophisticated, the basic job remains the same – keep the Fleet safe and effective.

All of that environmental information is combined with other types of information to give U.S., joint and allied forces a tactical advantage that is unique in the world.

"Those other types of information, which include information from our Information Dominance partners, only enhances that tactical warfighting advantage, and we remain committed to and focused on keeping the Fleet safe and effective with our partners in Information Dominance," Gallaudet said.

COAMPS® Explained:

The Coupled Ocean/Atmosphere Mesoscale Prediction System (COAMPS®) was developed by the Marine Meteorology Division (MMD) of the Naval Research Laboratory (NRL). The atmospheric components of COAMPS® are used operationally by the U.S. Navy for short-term numerical weather prediction for various regions around the world. It represents an analysis, now cast and short-term (up to 72 hours) forecast tool applicable to any given region of the earth.

COAMPS® includes an atmospheric data assimilation system (comprised of data quality control, analysis and initialization), a Non-hydrostatic atmospheric model Component and an Ocean Model component (NCOM). Data assimilation is the method of using observations from aircraft, rawinsondes, ships, buoys, satellites and other data sources to enhance the model’s analysis. Experience has shown that the inclusion of these observations dramatically improves model skill, especially in the case of moisture fields with COAMPS®. The non-hydrostatic model formulation (no adherence to the hydrostatic assumption) allows the model to solve complicated equations associated with very small scale weather features, such as thunderstorms. The coupling of the NCOM ocean model to the atmospheric model was necessitated by the increasing awareness of the importance of the ocean and atmosphere (e.g., El Nino) to weather forecasting. In a fully coupled mode, the atmospheric and oceanic models can be integrated simultaneously so that the precipitation and the surface fluxes of moisture and momentum are exchanged across the air-sea interface.
By Cathy Willlis, CNMOC PAO

STENNIS SPACE CENTER, MS
– RDML Timothy C. Gallaudet relieved RDML Brian B. Brown as commander of the Naval Meteorology and Oceanography Command (NAVMETOCOM) in a traditional change of command ceremony held June 18 at Stennis Space Center. Gallaudet was promoted to the rank of rear admiral (lower half) just prior to the ceremony.

Brown said he felt “blessed and lucky” to have worked with the Navy’s military and civilian oceanography workforce to perform a mission so critical to the warfighting effectiveness and readiness of the Fleet and Joint forces despite personal hardships, organizational changes and challenged resources in the Navy.

“The changing nature of warfare and the demands of the information age have set us on a new path – the right path – towards fulfillment of Information Dominance for the Navy,” Brown said.

Guest speaker ADM Bill Gortney, Commander of U.S. Fleet Forces Command, acknowledged the contributions that naval oceanography makes to naval operations and Information Dominance, including developing tools and techniques for optimizing use of unmanned underwater vehicles (UUVs).

“Naval oceanography is integral to nearly everything our Navy does,” he said.

Gallaudet most recently served as the deputy oceanographer of the Navy on the Chief of Naval Operations staff in Washington, D.C.

He said that it was an honor to lead an organization that was founded by the “father of naval oceanography,” Matthew Fontaine Maury, and looked forward to the next naval oceanographic survey ship, USNS Maury (T AGS 66), becoming operational on his watch later this year.

Brown, who has been NAVMETOCOM Commander since August 2012, was nominated for promotion and transferred to Vandenberg Air Force Base, CA, in June where he will serve as Deputy Commander, Joint Functional Component Command Space, U.S. Strategic Command. He was awarded the Legion of Merit for his accomplishments during his tour at Stennis.

By Lanee Cooksey, NAVO Public Affairs Officer

Stennis Space Center, MS—CAPT A. J. Reiss assumed command of the Naval Oceanographic Office (NAVOCEANO) in a ceremony here on June 20.

Reiss relieved CAPT Paul Oosterling who retired in a ceremony following the Change of Command.

During the ceremony, Oosterling reflected on his time at NAVOCEANO and said, “You amazed me, impressed me and made me increasingly enthusiastic about my job. I can only hope I did half as much for you as you did for me. You are all amazing people, and I salute your superb service to the country!”

...continued on Page 31
Reiss . . . continued from Page 30

As a naval oceanographer, Reiss has served in a variety of sea-going and shore-based positions throughout his career. He served aboard USS McClusky (FFG-41) home ported in Yokosuka, Japan and twice deployed to the Arabian Gulf in support of Operations Desert Storm and Desert Shield.

He was Staff Meteorology and Oceanography Officer and Flag Tactical Action Officer for Commander, Carrier Group Three aboard USS Carl Vinson (CVN-70) home ported in Bremerton, WA. He later served as Executive Officer (XO) for Naval Pacific Meteorology and Oceanography Facility, Whidbey Island, WA.

Reiss reported as Operations Officer at Fleet Numerical Meteorology and Oceanography Center, Monterey, CA, in 2005 and was then named its XO. He commanded the Naval Maritime Forecast Center in Norfolk, VA, from 2008 to 2010.

Prior to being named XO for NAVOCEANO in July 2012, Reiss was Director of Navy Weather Services for Commander, Naval Meteorology and Oceanography Command (CNMOC).

At the ceremony, Reiss commented, “This day is not about us on the stage but rather about the incredible people of NAVOCEANO and the integral information you provide to Fleet warfighting. I am humbled and quite frankly amazed, to now have my name associated with so many talented people and devoted Americans. It will be my joy and great honor to serve our Navy and Nation alongside you.”

NAVOCEANO is comprised of nearly 1,000 military, civilian and contractor personnel. The command has the responsibility for supplying oceanographic products and services to all elements of the Department of Defense.

JTWC Welcomes New Commanding Officer

By LT Thai Phung, Joint Typhoon Warning Center Public Affairs

CAPT Steven P. Sopko relieved CAPT Ashley D. Evans as Commanding Officer of the Joint Typhoon Warning Center (JTWC) in a change of command ceremony held on June 5 at Joint Base Pearl Harbor-Hickam.

Dr. William Burnett, the Deputy Commander and Technical Director of the Naval Meteorology and Oceanography Command, was the guest speaker and presided over the ceremony.

“In meteorology, there are two meccas where you want to work. One of them is the National Hurricane Center... for the military side, the mecca is the Joint Typhoon Warning Center. It is an honor to be with the men and women, the group of the Joint Typhoon Warning Center and certainly, the Commanding Officer. You cannot go any higher,” Burnett said.

During his farewell remarks, Evans praised everyone at JTWC for executing their duties with efficiency and precision, inside and outside the walls every day. His farewell would not have been complete without sharing his philosophy with the command one last time: “To take care of yourself, families and shipmates; everything else is secondary.”

After Sopko assumed command of JTWC, he thanked Evans for turning over a great command and an even greater team of professionals.

“I am honored and humbled for opportunity to command an organization that has such a great history of service in the Western Pacific and Indian Ocean...I do have very high expectations for what we can accomplish in the years to come; and together, we can meet any challenge that comes our way over the next couple of years,” said Sopko.
The use of social media platforms as a means of communication has been on the rise in recent years. A recent poll conducted by the Navy Personnel, Research, Studies & Technology (NPRST) office shows that an overwhelming majority of Navy personnel use Facebook and other forms of social media to communicate.

With a majority of Navy personnel and their families using social media, it represents a key opportunity to get the word out. Social media sites enable you to more easily connect with fellow Sailors, loved ones and friends by creating a space where you can talk to them, they can talk to each other, and everyone can interact. The Navy encourages service members to share their stories of service online with the American people. The Secretary of the Navy, Chief of Naval Operations, and Master Chief Petty Officer of the Navy all participate directly in social media as part of their communication efforts. The Navy also encourages personnel to use social media to stay connected to loved ones.

But we need to be aware that there are other people listening and trying to gain information about us through these same tools. It is essential to remember that while social media sites advertise their security and privacy settings, NOTHING online (including e-mail) is fully secure. For example, Facebook groups that are run as closed groups may appear to be an excellent means to communicate with designated families and Sailors but you should not be lulled into a false sense of security that these sites could not be hacked, monitored or otherwise breeched. Once you post your pictures and documents to these sites, be very aware of the rules of ownership of those files and privacy settings. Also remember that most digital cameras and cell phone cameras geo-tag photos with location coordinates unless you turn those settings off. You may inadvertently be giving away information that you did not intend to.

All service members and their families should know about the risks when using social media networks. Sailors and their families also need to be aware that social media has no international boundaries. Even our adversaries use social media. An Internet posting by Al Qaeda in 2009 directed their followers to comb through social networking sites to look for details about service members and their families.

Protect your families by limiting, to the extent practical, detailed information about them (i.e., addresses, towns or schools). Many social sites do not let you post... continued on Page 33
anonymously (like Facebook) and your full name and photo is attached to every posting. How hard would it be for someone to figure out who your loved ones are based on your personal profile? You never know who is watching and collecting information that could be used against you or your family.

With the increased quantity and visibility of online information, it is all the more important to educate Sailors and personnel about how to maintain integrity and security online. For that reason here are some recommended best practices you and your family should consider when using social media. Also included are links to the Navy Social Media Handbook and other information on OPSEC and Navy policy. Stay safe. And see you online.

Best Practices

- Always post, tweet, blog, email or otherwise communicate with the understanding that any information you share could potentially be made public regardless of your privacy settings or intentions.
- Protect your families by limiting the amount and type of information you post about family members such as names, addresses, local towns or schools.
- Understand each of your social network’s security settings so you can make informed decisions about who is and is not able to view your information and/or photos. Remember about that geo-tagging....
- Keep classified and sensitive information safe by not discussing critical information such as ship movements, deployments, personnel rosters and weapons information.
- If you hesitate when deciding whether you should share information, DON’T post it online.

Maintain good OPSEC online

- Maintain a unique password for different accounts.
- Change passwords frequently.
- Do not link other search engines to your Facebook timeline.
- Do not register for a social media account with an official .mil/.gov email address. (unless used as an official command social media presence and approved by Commanding Officer or PAO)
- Verify friend requests before accepting. Remember, if you have foreign nationals who you have “friended”, you need to disclose that to security and during your DONCAF Security Clearance updates.
- Always assume your content can be viewed publically, regardless of your privacy settings.

Watch out for:

- Impersonations
- Accidental geo-tagging (of images or posts)
- Non-secure privacy settings
- Posting sensitive personal, operational or geographic information

Expressing your opinion online

DoD and Navy policy as well as the ethical requirements state that Navy personnel acting in their official capacity may not “Associate DoD with any partisan political campaign or election, candidate, cause or issue” (SECNAVINST 5720.44B). Service members are permitted to express your political views within certain guidelines stated in the DoD Directive 1344.10, Title 10 of U.S. Code, Sec. 888, Art. 88 and SECNAVINST 5720.44B. Keep in mind that because of your leadership position, what you say and do online may be more visible and taken more seriously than that of your personnel, even about issues that you do not intend to reflect upon your command or the Navy.

Also on a professional note, remember who you have “friended” and what you are posting. There have been examples of some folks posting questionable pictures and comments on their Facebook page perhaps forgetting they have friended a very senior person. Once it’s in cyber-land it’s there forever. That is an important lesson to pass on to your children.

More Info on Social Media Best practices:


Naval OPSEC Brief on Facebook Privacy settings: http://www.slideshare.net/NavalOPSEC/facebook-privacy-settings-updated-february-2014


The Fleet Functional Area Manager (FAM) department of Navy Cyber Forces (NAVCYBERFOR) hosted a Fleet Waterfront Applications Workshop Aug. 18-20 at the 32nd Street Base Theater in San Diego.

Gaining traction and still on a shoestring budget, FAM also hosted the three-day workshop in April at the Afloat Training Group Auditorium, Naval Station Norfolk. It was open to waterfront commands and those using afloat applications.

As with previous workshops, the itinerary for 2014’s east coast event was based on user-identified training needs on software, applications and systems as defined in the more than 1,300 Fleet Applications and Solutions Team (FAST) Fleet-wide surveys. FAST surveys allow the curriculum to be tailored-to-fit each audience based on current Fleet needs.

In this iteration, in addition to the applications curriculum, (see sidebar ‘2014 Norfolk FAST Workshop’) a ‘Cyber Day’ was added to present overviews on Host Based Security System (HBSS), Vulnerability Remediation Asset Manager (VRAM) and Assured Compliance Assessment Solution (ACAS). Those who took advantage of the ‘Cyber Day’ portion were eligible to receive Continuing Education Units (CEUs) for recertification for some COMPTIA (Computing Technology Industry Association) certifications. For more information go to http://certification.comptia.org/staycertified/ceactivities.aspx.

Military personnel, government civilians and contractors from 44 commands, afloat and shore based, comprised the audience for the Norfolk training. With an array of personnel and issues to address, critique responses were overwhelmingly positive and equally diverse.

“Real Fleet issues and solutions,” is how one attendee characterized their experience with the COMPOSE block. Another attendee said, “There is more I can do to be a better administrator,” about the eSOMS block. One attendee wrote that he learned about “…the existence of MFOM 2.0.” The workshop was well-received across the board and the critiques support the need and the desire to have them continue.

“Slow and steady,” is how John ‘Jay-T’ Toomer, NAVCYBERFOR Fleet FAM, describes FAM/FASTs progress Fleet-wide. Turnout for the Norfolk workshop was approximately 300 personnel, with many of those attending multiple sessions. “An upward trend along with visibility from senior leadership is good for any program,” added Toomer.

As FAM/FAST sees an upward trend, what hasn’t changed is the mission - to identify and address afloat deficiencies by decreasing security vulnerabilities, removing bandwidth-inefficient applications (old or redundant applications), and working with Program Offices to identify required fixes and expedite them to the Fleet. Subject Matter Experts (SMEs) from the various Program... continued on Page 35
Offices located on each coast continue to keep the training costs minimal.

A FAST visit is not an inspection. Senior leadership and key personnel are given an in-brief upon the team’s arrival – where it is reiterated, “FAST is not an inspection!” FAST works from a predetermined stationary site as well as walks around to ensure as many departments as possible are given the opportunity to ask questions or submit complaints or suggestions for improvements in afloat applications.

At the conclusion of a FAST visit, the Commanding Officer is given an out-brief outlining identified issues. FAST visits take as long as required to get everyone’s input; usually a half to a full day. It is the Sailors best opportunity to get an issue identified before pulling away from the pier. FAST works with Program Offices to address and fix identified issues.

FAST visits can be requested by any afloat command by contacting the NAVCYBERFOR Fleet FAM department at Fleet_FAM_FAST@navy.mil. Additional application support and/or training can be requested by contacting Navy 311 (See sidebar ‘Navy 311 Information’).


Navy 311 Information

“If you require assistance of any nature, anywhere and anytime contact the NAVY 311 team,” said Bob Trader, NAVCYBERFOR, Program Executive Office – Enterprise Information Systems Program Manager Warfare. “Navy 311 takes immediate action by identifying the appropriate source of support, routing each service request to that support provider, and then tracking the issue through resolution.

“Navy 311 provides 24/7/365 customer support to the Fleet and is open to all DOD employees and their family members. A response will be sent to the requester via the same contact method used,” said Trader.

Help is available and here’s how to access it:
- Phone: 1-855-NAVY311 (1-855-628-9311)
- DSN: 510-NAVY311 (510-628-9311)
- Email: Navy311@navy.mil (unclassified) and Navy311@navy.smil.mil (classified)
- Navy message: NAVY THREE ONE NORFOLK VA
- Text: Type Navy311@navy.mil into the TO line of text message
- Chat: Via Navy311 website or mobile phone
- Sailor 2.1: A SPAWAR CAC-enabled self-help website is accessible at: https://sailor.nmci.navy.mil/Authentication/LoginForm.cfm

Ken Brown, NAVCYBERFOR Fleet FAM/FAST, interviews ABH3 Marc P. Elacio, USS Theodore Roosevelt (CVN-71), Air Operations Department, during a recent FAST visit.
EDITOR'S NOTE: Information on this page and the next was provided by NCTAMS LANT, DET Hampton Roads. Contact Information, as well as milestones in making rank from E2 to E6 are available here. It is intended to be used as a “Road Map” for Cyber Warriors to excel in their rating.

NAVAL COMPUTER AND TELECOMMUNICATIONS AREA MASTER STATION ATLANTIC DETACHMENT HAMPTON ROADS

REFERENCE SITES

1D Resources for Cyber Warriors
**NCTAMS LANT DET HAMPTON ROADS**
**SAILOR ROAD MAP**
**“HOW WE BUILD GREAT SAILORS”**

<table>
<thead>
<tr>
<th>36 MONTHS</th>
<th>ADVANCED TO E5</th>
</tr>
</thead>
<tbody>
<tr>
<td>PQS:</td>
<td>TRAINING PERSONNEL</td>
</tr>
<tr>
<td>EIDWS:</td>
<td>QUALIFYING PERSONNEL, SITTING BOARD &amp; CONDUCTING TRAINING</td>
</tr>
<tr>
<td>COLLATERAL:</td>
<td>COMPLETELY REQUISITIONED, COLLATERAL REISSUE TRAINING DATE</td>
</tr>
<tr>
<td>CPO 365:</td>
<td>ATTENDED AS REQUIRED</td>
</tr>
<tr>
<td>SCHOOL:</td>
<td>SCHOOLS: BACHELOR DEGREE COMPLETED (TECHNICAL DEGREE RECOGNIZED)</td>
</tr>
<tr>
<td>VOLUNTEER:</td>
<td>VOLUNTEER: LEADING ROPHERS &amp; COMMAND EVENTS</td>
</tr>
<tr>
<td>24 MONTHS</td>
<td>ADVANCED TO E4</td>
</tr>
<tr>
<td>PQS:</td>
<td>TECHNICAL PERSONNEL</td>
</tr>
<tr>
<td>EIDWS:</td>
<td>QUALIFYING PERSONNEL, SITTING BOARD &amp; CONDUCTING TRAINING</td>
</tr>
<tr>
<td>COLLATERAL:</td>
<td>COMPLETELY REQUISITIONED, COLLATERAL REISSUE TRAINING DATE</td>
</tr>
<tr>
<td>CPO 365:</td>
<td>ATTENDED AS REQUIRED</td>
</tr>
<tr>
<td>SCHOOL:</td>
<td>SCHOOLS: NATIONAL DEGREE COMPLETED (TECHNICAL DEGREE RECOGNIZED)</td>
</tr>
<tr>
<td>VOLUNTEER:</td>
<td>VOLUNTEER: LEADING ROPHERS &amp; COMMAND EVENTS</td>
</tr>
<tr>
<td>18 MONTHS</td>
<td>ADVANCED TO E3</td>
</tr>
<tr>
<td>PQS:</td>
<td>DIVISIONAL PERSONNEL</td>
</tr>
<tr>
<td>EIDWS:</td>
<td>QUALIFIED</td>
</tr>
<tr>
<td>SCHOOL:</td>
<td>AUTHORIZED AFTER 18M IN PQS AND E4</td>
</tr>
<tr>
<td>VOLUNTEER:</td>
<td>VOLUNTEER: CALLED AND RECOMMENDED</td>
</tr>
<tr>
<td>12 MONTHS</td>
<td></td>
</tr>
<tr>
<td>PQS:</td>
<td>DIVISIONAL PERSONNEL</td>
</tr>
<tr>
<td>EIDWS:</td>
<td>QUALIFIED</td>
</tr>
<tr>
<td>SCHOOL:</td>
<td>AUTHORIZED AFTER 12M IN PQS AND E4</td>
</tr>
<tr>
<td>VOLUNTEER:</td>
<td>VOLUNTEER: CALLED AND RECOMMENDED</td>
</tr>
<tr>
<td>9 MONTHS</td>
<td>ADVANCED TO E3</td>
</tr>
<tr>
<td>PQS:</td>
<td>DIVISIONAL PERSONNEL</td>
</tr>
<tr>
<td>EIDWS:</td>
<td>QUALIFIED</td>
</tr>
<tr>
<td>SCHOOL:</td>
<td>AUTHORIZED AFTER 9M IN PQS AND E4</td>
</tr>
<tr>
<td>VOLUNTEER:</td>
<td>VOLUNTEER: CALLED AND RECOMMENDED</td>
</tr>
<tr>
<td>6 MONTHS</td>
<td></td>
</tr>
<tr>
<td>PQS:</td>
<td>DIVISIONAL PERSONNEL</td>
</tr>
<tr>
<td>EIDWS:</td>
<td>QUALIFIED</td>
</tr>
<tr>
<td>SCHOOL:</td>
<td>AUTHORIZED AFTER 6M IN PQS AND E4</td>
</tr>
<tr>
<td>VOLUNTEER:</td>
<td>VOLUNTEER: CALLED AND RECOMMENDED</td>
</tr>
<tr>
<td>3 MONTHS</td>
<td></td>
</tr>
<tr>
<td>PQS:</td>
<td>DIVISIONAL PERSONNEL</td>
</tr>
<tr>
<td>EIDWS:</td>
<td>QUALIFIED</td>
</tr>
<tr>
<td>SCHOOL:</td>
<td>AUTHORIZED AFTER 3M IN PQS AND E4</td>
</tr>
<tr>
<td>VOLUNTEER:</td>
<td>VOLUNTEER: CALLED AND RECOMMENDED</td>
</tr>
</tbody>
</table>

**REQUIRED**
1. PERSONNEL QUALIFICATIONS STANDARDS (PQS)
2. ENLISTED INFORMATION DOMINANCE WARFARE SPECIALIST (EIDWS)
3. COLLATERAL (CP455)
4. CHIEF PETTY OFFICER (CP430 & 454)

**INFORMATION ASSURANCE TECHNICAL/MANAGER LEVELS**

<table>
<thead>
<tr>
<th>IA/IT LEVEL 1</th>
<th>IA/IT LEVEL 2</th>
<th>IA/IT LEVEL 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAP</td>
<td>G2G</td>
<td>G2G</td>
</tr>
<tr>
<td>G2G</td>
<td>DCS</td>
<td>DCS</td>
</tr>
<tr>
<td>DCS</td>
<td>CAP (or Associate)</td>
<td>CISSP</td>
</tr>
</tbody>
</table>

**DIVISIONAL PERSONNEL QUALIFICATION STANDARDS (PQS)**

<table>
<thead>
<tr>
<th>COMMUNICATION SUPPORT ACTIVITY</th>
<th>TECHNICAL CONTROL FACILITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>GSA</td>
<td>C2S</td>
</tr>
<tr>
<td>NAVS</td>
<td>C2S</td>
</tr>
<tr>
<td>COMM</td>
<td>C2S</td>
</tr>
<tr>
<td>GSA</td>
<td>C2S</td>
</tr>
</tbody>
</table>

**COMMUNICATIONS/TECHNICAL/ENGINEERING**

<table>
<thead>
<tr>
<th>COMMUNICATIONS/TECHNICAL/ENGINEERING</th>
</tr>
</thead>
<tbody>
<tr>
<td>COMMUNICATIONS/TECHNICAL/ENGINEERING</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

**COMMISSIONING/SPECIAL PROGRAMS**

<table>
<thead>
<tr>
<th>COMMISSIONING/SPECIAL PROGRAMS</th>
</tr>
</thead>
<tbody>
<tr>
<td>COMMISSIONING</td>
</tr>
<tr>
<td>NAVY</td>
</tr>
</tbody>
</table>

**For a copy or to recommend changes please contact:**

[Contact Information]

**FOR A COPY OR TO RECOMMEND CHANGES PLEASE CONTACT**

[Contact Information]
BIG Awardee Inspires Young & Old

By George D. Bieber,
NAVCYBERFOR Public Affairs

Navy LT Duane L. Motley, Flag Secretary, Staff Executive Officer (XO) of Troops and Assistant Chief of Staff (ACOS) Admin for Navy Cyber Forces (NAVCYBERFOR), was named as one of 13 DOD military and civilian recipients of the Blacks in Government (BIG) Meritorious Service Award for 2014.

“He’s a superstar,” said his supervisor, CAPT Danielle Barrett, NAVCYBERFOR’s Chief of Staff. “He has the responsibility, accountability and autonomy of an Officer-in-Charge and executes those duties with extraordinary results.”

“He similarly excelled in academics earning his Bachelor’s degree in his off time, community outreach events, and is a mentor and role model of the highest caliber,” Barrett added. “LT Motley understands mission needs, teamwork and promotes success in others.”

Many of Motley’s shipmates feel he significantly improves the mission effectiveness of NAVCYBERFOR and its subordinate commands. As XO of Troops, he focused on process improvements, enhancing all command programs, personnel readiness, and quality of life at the command, resulting in improved generation of Information Dominance force readiness worldwide.

Motley’s direct personal involvement and leadership in significant command programs include: Command Managed Equal Opportunity Program, Sexual Assault Prevention and Response Program, Fitness Enhancement Program, Multicultural Committee, and the Planning Board for Training. His direct hands-on involvement has led to exceptional improvements and set the standard for excellence in the Fleet.

“I feel very appreciated and honored to be recognized by my command for my efforts,” said the 38-year-old Motley, who has been at NAVCYBERFOR since June 2013. “I like to help everyone. That’s just who I am.”

As the Flag Secretary and ACOS for Admin, Motley meticulously reviewed all staff processes, innovatively employing efficiencies that improved the quality and timeliness of services and deliverables to senior leadership. According to that same leadership, Motley’s actions directly contributed to enhancing the command’s support to operational forces in the areas of information dominance, network operations and C5I (Command, Control,
Command’s ‘Superstar’ Shines in Vegas

NCTAMS LANT’s own, LCDR Tripp, receives special award

By Jacky Fisher, NAVCYBERFOR Public Affairs

LCDR Yolanda M. Tripp, Assistant Operations Officer (OpsO), Naval Computer and Telecommunications Area Master Station Atlantic (NCTAMS LANT), was awarded one of 13 Meritorious Service Awards presented by Blacks in Government (BIG) for her exceptional role model example as a Navy officer and mentor to both Sailors and those in her community.

Tripp reported to NCTAMS LANT December 2011 and recently transferred to Navy Information Operations Command Georgia. But the legacy she leaves behind will serve the Navy for years to come and illustrates her well-deserved selection for this award.

During her tour as Assistant OpsO, a department larger than most commands consisting of 475 officers, Sailors and civilians, employees excelled under her charge. “Professionalism, mentorship and a laser focus on mission excellence are her hallmarks,” said CAPT Kelly Aeschbach, Commanding Officer, NCTAMS LANT.

The stats speak to Tripp’s unparalleled technical expertise and desire to encourage and instill upward mobility for those who served under her - 95 percent retention rate; 40 Basic and Intermediate qualified Information Professional Officers; 210 Enlisted Information Dominance Warfare Specialist (EIDWS) qualifications; and 190 Information Assurance (IA) certifications leading to the DOD $200,000 in contracting costs to develop similar training.

Officers; 210 Enlisted Information Dominance Warfare Specialist (EIDWS) qualifications; and 190 Information Assurance (IA) certifications leading to 120 Navy Enlisted Classification (NECs) designations. All this training reflected well on her Sailors performance records and in their wallets. Sailors under Tripp’s charge received in excess of more than $100,000 in re-enlistment bonuses.

As the Training Officer, Tripp identified and tackled a training deficiency by developing and implementing a seven-week Training Academy for command personnel. Using 21 subject matter experts, Tripp spearheaded the development of 57 podium-base lectures tailored in three functional areas to rapidly train personnel for mission execution. Her initiatives dramatically improved qualifications of her five watch teams and Sailor advancement rates leading to an unprecedented 200 command Sailors advancing in rate during FY13 and FY14. Tripp’s effort was shared with the Department of Defense to improve Navy schoolhouses and resulted in saving the DOD $200,000 in contracting costs to develop similar training.

Active in the community and grounded in her faith, Tripp also served as the Sixth Mount Zion Baptist Church Scholarship Ministry Chairperson that focused on financial support for graduating high school seniors to further their education. This committee awarded $30,000 to 30 minority students enabling them to attend Historically Black Colleges and Universities throughout the Tidewater area. Through her direct guidance, 23 of those 30 students were accepted into the Norfolk State and Hampton University Reserve Officer Training Corps program.

“She’s a superstar,” said Aeschbach. “Her ability to motivate others to excel coupled with her unmatched dedication to service in the Navy and the nation make LCDR Tripp the ideal candidate for this award.”
In 1969, the Rolling Stones’ lead singer, Mick Jagger belted out one of the band’s biggest hits, “You Can’t Always Get What You Want.” In 2014, LT Jimmy J. Pavelka, Navy Cyber Forces’ (NAVCYBERFOR) N432, took the tune’s popular reply, “...But if you try sometimes, well you might find...You get what you need!” to the next level.

Pavelka has served 16 of his 26 years in the Navy as an Interior Communications Technician until he was commissioned Nov. 1, 2005. Since becoming a Limited Duty Officer (LDO) as an Electronics Materials Officer (EMO), Pavelka sought educational opportunities to not only improve his career, but those of his fellow LDOs, which in turn benefits the entire Navy.

“Until recently, the Web-enabled version of the Joint Professional Military Education’s (JPME) Phase I training was only open to regular commissioned officers,” said the Springfield, OH, native. “Apparently the Community Managers at BUPERS had a restriction, for whatever reason, that prevented LDOs from attending the highly sought after course at the Navy War College.”

“The distinction was that as an LDO, I was not seeking to do a residency course in Rhode Island but asking to get enrolled in a distance learning version of the course to do on my own time after work,” said Pavelka. “This version of the course was zero cost and a win/win situation for everyone involved. I was just asking for an opportunity.”

According to Pavelka, a Navy message went to the Fleet and Pavelka along with several other NAVCYBERFOR LDOs became the first group to get the “green light” to be enrolled in Naval War College’s Web-enabled JPME Phase I program.

“After many emails and phone conversations with CDR (Ken) Demick, Information Professional Officer Community Manager and Susan Piekarski, Strategy & Warfare Administrative Assistant at the War College, we were successful,” said Pavelka. “Without their support and that of my NAVCYBERFOR Chain of Command reaching out to all the stakeholders to make this happen, I would not be enrolled in the course today. I owe a lot to NAVCYBERFOR’s leadership and CDR Demick at BUPERS.”

“As a graduate of the Naval War College,” added Menard, “I believe that Joint Professional
Military Education’s Phase I program is essential to the professional growth of every officer to include Limited Duty Officers. As LT Pavelka’s mentor, it was important to support his efforts and provide him with the guidance he needed in order to gain acceptance into the program.”

Professor Tim Garrold, Fleet Seminar Program Manager, provided everyone with the background on how the program had become unavailable to LDOs and Warrant Officers nearly three years earlier. According to Garrold, BUPERS had made the call and Pavelka was the first one to seek this educational opportunity since then.

Pavelka not only broke new ground for acceptance into the once-exclusive Web-enabled program, but proved that persistence pays.

Dr. William D. Ferree, Manager, Web-enabled Programs, NWC, sent Pavelka a letter prior to accepting him into the JPME Phase I program, describing the criteria being geared toward senior officers serving in Naval and Joint assignments.

“Even though there were some obstacles and road blocks,” added Pavelka, who currently serves as NAVCYBERFOR’s Cruiser-Destroyer (CRUDES) Action Officer and EMO, “I kept questioning the process and qualifications until the eventual approval for my enrollment came in.” In his Theater Security Decision Making (TSDM) class, there are several LDO’s from around the Fleet who have joined the program.

Being an Army brat, Pavelka learned early in life from his father, a retired master sergeant, that if you wanted something bad enough you kept trying and that the word “no” was more of a deterrent than a complete surrender when seeking a goal.

Hence, the now newly-enrolled JPME Phase I student has not only lived up to his father’s advice and others, but Pavelka has obtained what he and the Navy needs... an educated LDO who not only serves the Navy as a more rounded Navy officer, but the joint service community as well.

“I guess the Stones did say it best,” concluded Pavelka, “If you try... you get what you need.”

**EDITOR’S NOTE:** For more information on qualifications and enrollment into the Naval War College’s Web-Enabled Programs, see article below; accessible at www.public.navy.mil/BUPERS-NPC/OFFICER/Detailing/JOINTOFFICER/Pages/JPME.aspx.

---

**Joint Professional Military Education (JPME)**

To be excepted for the “in-residence” military programs, officers must provide NPL PERS-45J with their official JPME completion letter/diploma for all accredited programs to receive the respective Additional Qualification Designators (AQD) (JPME I - JS7, JPME II - JS8). Send documentation for all distance learning programs to the appropriate email address below. Documents are processed daily.

**AC and FTS:** Mill_PERS-45J_JPME@navy.mil  
**SELRES:** Mill_RC_JQS_Manager@navy.mil

The AQD will be entered in the Joint Manpower Information System and Officer Assignment Information System within 30 days. Documentation will then be forwarded to PERS-313. It may take an additional 60 days for the AQD to reflect on the officer’s Officer Summary Record (OSR) and Officer Data Card (ODC).

Availability is extremely limited with all in-residence JPME programs. Accordingly, work through your detailer (and only your detailer) to obtain a quota.

Per Title 10, Joint Professional Military Education (JPME) must be completed in sequence; Phase I followed by Phase II. Direct Entry Waivers (DEW) are only authorized by the Joint Staff on a strict case-by-case basis, with a compelling reason for attending Phase II prior to completing Phase I. Additionally, per Title 10, no more than 10 percent of a JPME II class may be attending under a DEW. Accordingly, it is advisable to begin joint education as soon as possible. Officers may enroll through distance learning at the Naval War College as a LT or other junior service colleges as a LCDR. Per NAVADMIN 136/10, completion of JPME Phase I is now a requirement for assuming URL CDR command.

JPME Phase I can be completed either through an “in resident” course or through distance learning. All of the intermediate service colleges offer distance learning via some of the listed links (See JPME on page 43). Distance Learning through the Air University Air Command and Staff College (AU ACSC) is accredited for JPME I. However, distance learning through the Air War College (the Air Force Senior College) is not accredited for JPME I.

JPME Phase II is available for CDRs and CAPTs at National Defense Universities (Joint Forces Staff College - Joint Advanced Warfighting School, Industrial College of the Armed Forces, and National War College) and all of the senior service colleges. These are all “in resident” courses, but be forewarned; because of Title 10 requirements, the

... continued on Page 43
IDC Warrior Adds Elite Program To Resume

By Jacky Fisher, NAVCYBERFOR Public Affairs

Intelligence Officer (IO), CDR(sel) William D. Richmond will leave his current position as Officer in Charge, Fleet Intelligence Detachment Washington, D.C. (FID DC OIC) this November for Capitol Hill as one of 16 Fellows selected for the 2015 Navy Legislative Fellows program. The lone Information Dominance Corps (IDC) selectee, Richmond will learn which Congressional office he’ll be assigned after a three-week orientation this winter.

A native of La Crosse, WI., Richmond appreciates the magnitude of responsibility that goes with this opportunity. “I am representing not only the Navy and the Intel community,” said Richmond, “I also represent the newest warfare community, the IDC. It’s an honor on all accounts.”

Office of Legislative Affairs (OLA) places Fellows in the office that best fits their background and experience. As a 15-year career Navy IO with two degrees, a Bachelors in International Relations/Russian and a Masters with a focus on Economics, the options of congressional office assignments Richmond is qualified to support spans the gamut.

Duties as FID DC OIC required Richmond to be responsible for preparing 100 personnel for deployment with eight Carrier Strike Groups and six Amphibious Readiness Groups. With his background in Navy Intelligence, Richmond thinks he would be a good fit to work with any sitting Members of Congress serving on the Armed Services or Intelligence Committees. “Maybe I will end up assisting the personal staff of a Member on one of the Select Committees on Intelligence,” Richmond said. “Regardless of where I’m assigned, this is a great opportunity to experience a higher level decision-making process.”

Richmond is the second IO and only the third IDC candidate to be selected in more than a decade.

“The Fellows program has existed for many years,” said LCDR Natalia Henriquez, the Navy Legislative Fellows program manager. “As it has grown over the years, we have found that Fellows bring a valuable perspective to Capitol Hill offices, but they also learn a tremendous amount, ultimately bringing that knowledge back to the Navy during their utilization assignment.”

Expanding his knowledge of Congressional affairs was the motivation behind Richmond’s application for this prestigious program. According to Richmond, “Being a Legislative Fellow will afford me the opportunity to duly represent the Navy in policy-making processes both during and after my time working in a Congressional office.”

Richmond’s options for an O5 milestone follow-on tour are many as he anticipates taking his Navy career “as far as possible.”

Richmond adds, “Regardless of the tour, as a senior officer I will be in a position much closer to the national level. The familiarity with Congressional affairs I glean from this program will prove invaluable in understanding and communicating the national decision-making processes that directly affect the future units to which I will be assigned.”

...continued on Page 43
NDUs may incur a joint tour obligation upon graduation. If you’re interested in attending contact your detailer. Officers who are already a JQO and attend one of the NDUs you must, by law, go to a Joint Duty Assignment List tour upon graduation. OSD waivers are only approved on a strict case by case basis.

The JFSC also offers four, 10 week, Phase II classes per year for LCDRs - CAPTs. Attendance is competitive due to limited seating. If you would like to attend please contact your detailer.

Reserve Component Officer School Information

Advanced Joint Professional Military Education (AJPME) is a 40 week blended learning course for Reserve Component (RC) officers (grades O-4 to O-6) that is similar in content to the in-residence JFSC Phase II. AJPME satisfies the educational requirement for qualification as JQO level III (RC officers only). Quotas are obtained through CNRFC N7.

The AJPME link is: http://www.jfsc.ndu.edu/schools_programs/ajpme/default.asp

The CNRFC N7 JPME page can be accessed here (login required): https://private.navyreserve.navy.mil/3447B/n7/pme/default.aspx

Email AC & FTS: Mill_PERS-45J_JPME@navy.mil

SELRES: Mill_RC_JQS_Manager@navy.mil.

JPME Schools Information

**JPME Matrix**
Matrix of JPME Options

**JPME I International military colleges**
JCS memo for international military colleges that are eligible for JPME I equivalent credit

**National Defense University (NDU)**
Industrial College of the Armed Forces, National War College and Joint Forces Staff College (JAWS, JCWS and AJPME)

**Naval War College**
Navy Intermediate and Senior Schools

**Marine Corps University**
USMC Intermediate (CSC) and Senior (MCWR)

**Air Force Intermediate**
Air University Air Command and Staff College

**Air Force Senior**
Air War College

**Army Intermediate**
Army Command and General Staff College

**Army Senior**
Army War College

Cyber Warrior . . . continued from Page 42

I’m fortunate to be assigned to the Fellowship program,” Evans said. “It’s both a competitive and unique opportunity to glean experience outside the Corps while representing the Corps. I’m sure we can learn from each other.”

Evans has more than 18 years in the Corps. He spent the first five years in the Intelligence field before accepting a commission as a Communications Officer. Trading his uniform for a suit and tie, Evans will keep his work ethic intact. “I’ll do my job the best I can, contribute to the mission, and mentor when needed.”
Multi-service AFPs were offloaded in Belize to support SPS14 missions in July.

IT2 Gains Sea Legs Aboard USS Ponce

IT2 Christian J. Troutner, formerly assigned to Navy Cyber Forces’ Facilities IT Department, is now on board the USS Ponce (AFSB(I)-15) as an Individual Augmentee (IA).

Currently homeported in Manama, Bahrain, Troutner is one of the ship’s primary tech controllers. “I’m here to support the ship and crew making sure we can communicate during the Laser Weapon System (LaWS) installation,” said Troutner.

The Ponce is being converted into a test bed to deploy the first ever LaWS. The laser gun will destroy drones, small boats and other air or sea-borne threats.

“Being an IA is a unique experience,” added Troutner. “You see the Fleet from a different perspective than you normally would.”

Though he’s only been at sea since July 22, Troutner feels that if a Sailor has the opportunity to do an IA, he or she should jump at it.

He is scheduled to complete his tour with the Ponce by mid-April 2015, however, plans could change as early as October should he be selected to attend the Seaman to Admiral program.

“All I’m waiting on now is my package results from Pensacola,” said Troutner. “I’m hoping for the best. We’ll just have to wait and see what happens.”
DEFENSE SUPERIOR SERVICE MEDAL
CAPT Chad Asey, NIOC Maryland
CAPT Kathleen Creighton, NCTS Bahrain
CAPT Larry Flint, FLTCYBERCOM FT Meade
CAPT Kevin LeRette, NAVCYBERFOR Suffolk

DEFENSE MERITORIOUS SERVICE MEDAL
CDR Brady Babcock, CSG Key West
LT Sarah Beatty, NIOC Maryland
LCDR Douglas Bradshaw, NIOC Maryland
CDR Pablo Breuer, USCYBERCOM
CTTC Michael Burrnasser, NIOC Georgia
CTRC Eric Carter, NIOC Maryland
CDR Ann Casey, NIOC Maryland
CTNC John Collins, NIOC Maryland
CTRC Lesley Conn, NIOC Maryland
CDR Calvin Foster, USCYBERCOM
LCDR Christopher Fraser, USCYBERCOM
CTTC Bradley Glisan, NAVWARSSYSCOM
CTNC Daniel Gray, NIOC Maryland
CTTC Jeremia Hall, NIOC Colorado
CDR Michael Holland, USCYBERCOM
ITC David Istvan, NIOC Georgia
LCDR Dustin Johns, NIOC Maryland
LCDR Stephen La Bash, NIOC Maryland

MERITORIOUS SERVICE MEDAL
LCDR Paige Adams, NCDOC
LCDR Lane Askew, NAVSOC
CW3 Richard Aubin, NIOC Georgia
CDR John Bandy, NIOC Hawaii
CMDCM James Barnes, NIOC Texas
CTRCM Amber Betts, NIOC Pensacola
CDR Damian Blassey, NCDOC
CDR Stacy Bowman, NAVCYBERFOR Suffolk

JOINT SERVICE COMMENDATION MEDAL
CTN2 Tyler Anderson, NIOC Maryland
LTJG Diana Barron, NIOC Maryland
LTJG David Barsis, NIOC Georgia
CTT2 Christopher Bernheisel, NIOC Colorado
CTT1 Ryan Berton, NIOC Colorado
CTN1 Eric Bokin, NIOC Maryland
CTN2 Valeria Bokay, NIOC Maryland
LT Derrick Brooks, NIOC Maryland
CTT1 Ernie Chavez, NIOC Colorado
CTT1 Paul Christopher, NIOC Maryland
CTN2 Bradford Collier, NIOC Maryland
CTN2 Vincent Crusan, NIOC Maryland
CTNC Shawn Dencklau, NIOC Maryland
LT Gretchen Dowdy, USCYBERCOM
IT2 Taylor Downs, SUSLA Korea
LTJG Doran Duhart, NIOC Maryland
CTT1 Christopher Durrett, NIOC Colorado
CTJ2 Joshua Dyer, NIOC Maryland
CTNC Ryan Earle, NIOC Maryland
LT Amanda Eckert, NIOC Maryland
CTT1 Aaron Edson, NIOC Maryland
CTT1 Matthew Ekker, NIOC Maryland
IS1 Kayla Faust, USCYBERCOM
CTB1 Benjamin Fawkes, NIOC Maryland
CTT1 Robert Fox, NIOC Maryland
CTT2 Brandon Galbraith, NIOC Maryland
LCDR Douglas Gray, NIOC Maryland
LCM3 David Hargrave, NIOC Maryland
CTT1 Eric Haigh, NIOC Colorado
CTT2 Patrick Haughney, NIOC Maryland
LT Christopher Heywood, NIOC Maryland
CTT1 Bryan Hoeft, NIOC Maryland
CTN3 Brittany Holloway, NIOC Georgia
CTR2 Jonathan Horwath, NIOC Maryland
CTC Eric Jetmir, NIOC Maryland
CTCJ Michael Joseph, NIOC Maryland
CTT2 Christopher Kenna, NIOC Maryland
CTT1 Joshua Kehoe, NIOC Maryland
CTT2 Joshua Keller, NIOC Georgia
CTT2 Samuel Knight, NIOC Georgia
CTT1 Sean Kontogiannis, CST 20 Afghanistan
A NAVY AND MARINE CORPS COMMEMORATION MEDAL

Lcdr Paige Adams, NCDOC
CTR Anthony Addair Jr., NIOC Maryland
CTR Joshua Adee, NIOC Georgia
LT Ashley Adewuyi, NCWDG
CTC Michelle Albin, NIOC Maryland
CTN1 William Aldridge, NIOC Pensacola
CT12 Michael Alexander, NIOC Georgia
CT11 Anthony Allen, NIOC Hawaii
IT1 Isaac Aaron, NCTAMS PAC
CTN1 Terrance Barnes, NIOC San Diego
Lcdr Anthony Barks, NCTAMS PAC
Yncs Patricia Arnold, NCTAMS PAC
Lcdr John Barkley, NCWDG
IT2 Curtis Barnes, NIOC San Diego
Lcdr David Barnes, FLTCYBERCOM
C1r1 Michael Barnes, NIOC Pensacola
C1r1 Charles Barns, NCTAMS PAC
C1r1 Brittany Bean, NIOC Maryland
Yncs Melanie Beasley, NCTAMS LANT DET Hampton Roads
C1r11 Joshua Beemer, NIOC Georgia
C11 Terena Beltz, NIOC Digby
CTTN5 Aspen Bentley, NIOC Georgia
L1tg6 Matthew Bernard, NIOC Maryland
LT Jesse Bird, NCWDG
L1tg6 Jeremy Blanchette, NIOC Bahrain
C1r11 Tandre Bodine, NIOC Maryland
C1r11 Allan Bollinger, NIOC Pensacola
C1r11 Joseph Bosser, NIOC Maryland
C1r2 Brandon Box, NIOC Maryland
C1r1 James Brashfield, NCWDG
C31 Lindale Brooks, NCWDG
IS3 Larry Brown, NIOC Pensacola
IS1 Samuel Brown, NCTAMS PAC
C1r11 Terrance Brown, NCTAMS PAC
Lcdr Bradley Brown Jr., NIOC Whidbey Island
LT Alyson Bulis, NCOS Norfolk
C1r2 Lukas Bunning, NIOC Maryland
LT Jared Burgess, FLTCYBERCOM FT Meade
L1tg6 Evita Burks, NCTAMS LANT
L53 Nassir Burks, NIOC Fairfax
C1r2 John Burroughs, NIOC Maryland
ICTC Alcario Bustamante, NCDOC
C1r1 David Cabacuna, NIOC Whidbey Island
C1r2 Timothy Callim, NCTS Bahrain
IS2 Jena Calloway, NCOS Norfolk
BU2 Ryan Canny, NIOC Sugar Grove
CTTC Bryon Carter, NIOC San Diego
CTNC Michael Carroll, NCDOC
C1r1 Ryan Causey, NIOC Maryland
C111 Brian Chalfant, NIOC Hawaii
Yn2 Naomi Chaney, NCTAMS PAC
C1r1 Dustin Chapman, NIOC Colorado
ICMC Cherise Chase, NCTAMS PAC
C1r2 Zhan Chen, NIOC Salt Lake City
C111 Andrew Chesser, NIOC Georgia
Lcdr Robert Clarady, NAVYCYBERFOR Suffolk
Cec Lyndarryl Clark, NCTS Bahrain
C1r1 Amanda Clarke, NIOC Sugar Grove
C1r1 Mario Clay, NIOC Bahrain
C1r1 Van Clinton, NIOC Maryland
C1r1 Santos Colon Jr., NIOC Georgia
IS2 Joshua Columbo, F/A17 Norfolk
C1m1 Nicholas Cordier, NAVYCOMCOM Norfolk
ICS Michael Craig Sr., NNWC Suffolk
C1r1 Tracy Culbert, NCTS Cialis
CTC1 Jessica Cummins, FLTCYBERCOM FT Meade
LT Andrea Curry, NIOC San Diego
C1r11 Ryan Custer, NAVYCYBERFOR Suffolk
C1r1 Tracy Culbert, NCTS Cialis
C1r1 Jessica Cummins, FLTCYBERCOM FT Meade
Lcdr Gary Daniels, NIOC Maryland
CE1 Alpedro Danieli, NIOC Bahrain
C1r2 Matthew Darby, NIOC Bahrain
C111 Gregory Davis, NIOC Pensacola
ITCM Orlando Davis, NCTAMS LANT
CTR Bartholomew Dewey, NIOD Alice Springs
CTNCS Rafael Del Valle, NIOC Norfolk
LT Amanda Deo, NAVYCYBERFOR Suffolk
C1r1 Yeray Diaztorres, NIOC Maryland
EMC Shelton Dickerson, NIOC Cialis
C1r1 James Dinette, NIOC Norfolk
IS1 Richard Dix, NIOC Pensacola
C1M1 Christopher Duffey, NIOD Groton
C1r1 David Duggar, NIOC Pensacola
CT11 Anna Duncan, NIOC Georgia
CTC Timothy Duncan, NIOD Kaneohe Bay

CT12 Samuel Knight, NIOC Georgia
CT11 Sean Kontogianis, CST 20 Afghanistan
IT2 Justin Lacleuse, NSUSLA Korea
ITC Alan Lawley, SUSLO London
Cttc Son Le, NIOC Colorado
CT11 Christopher Lieder, NIOC Colorado
CTN2 Damon Lockard, NIOC Maryland
CT11 Jason Loftin, NIOC Maryland
CTR1 Corey Mahoney, NIOC Georgia
CT11 Mark Martel, NIOC Maryland
CTR2 Michael Martinez, NIOC Georgia
CTN2 Carlos Martinez, NIOC Texas
CTT2 Justin Mays, NIOC Colorado
ITG6 Ismail McCowin, NIOC Maryland
CT11 Justin McKeithan, NIOC Georgia
CTT2 Trevor McMahon, NIOC Colorado
LT Jonathan Meckes, NIOC Colorado
L1tg8 Kenneth Mercer, NIOC Maryland
C1r2 Scott Mikkelson, NSUSLA Korea
IT2 Reuben Miles, SUSLA Korea
CTTT1 Jared Miyashiro, NIOC Colorado
CTT1 Anthony Oubre, NIOC Colorado
C1r2 Benjamin Parker, NIOC Maryland
C1n1 Sarah Palyo, NIOC Maryland
CT11 Michael Perry, NIOC Colorado
IT2 Joshua Pickron, NIOC Maryland
IT1 Stephanie Porcelli, NIOC Maryland
CT11 Terrance Price, NIOC Maryland
C1r1 Matthew Ramos, NIOC Menwith Hill
C1r1 Derek Radko Jr., NIOC Texas
C1r2 Danielle Roberts, NIOC Maryland
C1r2 Jesse Roberts, NIOC Maryland
C112 Ryan Roberts, NIOC Maryland
LT Jonathan Sahim, NIOC Maryland
CTN2 Gustavo Sanchez, NIOC Maryland
CTN1 Jesse Sanchez, NIOC Maryland
CTN1 Alan Savage, NIOC Maryland
LT James Schall, USCYBERCOM
CT11 Nicholas Scharrs, NIOC Colorado
CTN1 Matthew Schwarz, NIOC Maryland
CTN1 Jeffrey Sells Jr., NIOC Maryland
CTN2 Annette Sherman, NIOC Maryland
IT11 Jamie Smith, NIOC Maryland
CTN1 Derek Stevens, NIOC Georgia
C1r2 Matthew Stevens, NIOC Georgia
CTN2 Perry Stewart, NIOC Maryland
IS1 John Stout, USCYBERCOM
CTTT2 Tyler Stull, NIOC Maryland
C1r2 Michael Sundberg, NIOC Maryland
CTN2 Levi Terry, NIOC Maryland
CTT11 John Thompson, NIOC Texas
C1r117 Justin Tropp, NIOC Colorado
C1r1 Jason Umel, NIOC Georgia
CTR11 Lean Upton, NIOC Maryland
CT11 Guy Vanderkamp, NIOC Maryland
CTN1 Wayne Villars, NIOC Georgia
C1r12 Christopher Werman, NIOC Maryland
CT12 John Wesselos, NIOC Maryland
C1r2 Dylan Winston, NIOC Georgia
C1r11 Jason Winters, NSUSLA Korea
L1tg6 Joseph Wissler, NIOC Maryland
C1r21 John Zinser, NIOC Maryland
JOINT SERVICE ACHIEVEMENT MEDAL

CTI2 Brandon Almquist, NIOC Georgia
CTR2 Benjamin Alteme, NIOC Maryland
CTM3 Athena Anderson, SUSLA Korea
CTR3 Henny Arndt, NIOC Misawa
CTR2 India Ballinger, NIOC Maryland
CT12 Dennis Barrett, NIOC Georgia
CTI2 Kelly Bedard, NIOC Hawaii
LCDR Victor Belanger II, NIOC Maryland
IT3 Denver Bello, NIOC Misawa
IT3 Daniel Benko, NIOC Misawa
CTT2 Aspen Bentley, NIOC Georgia
CTM2 Matthew Boggs, SUSLA Korea
CTN3 Brandi Bowser, NIOC Maryland
CTI2 Mallory Box, NIOC Georgia
CTR3 John Bradshaw, NIOC Maryland
CT12 Patrick Brasel, NIOC Georgia
CTR3 Kyle Bray, NIOC Georgia
CTI1 Michael Briggs, NIOC Georgia
CTR2 Toccara Brooks, NIOC Maryland
CTR3 Corie Brown, NIOC Maryland
CTN3 Austin Butts, NIOC Maryland
CTR1 Willie Cabarrus, NIOC Maryland
CTN3 Isabella Cabarrus, NIOC Misawa
CTR3 Jessica Carroll, NIOC Maryland
IT3 Jesse Casler, NIOC Maryland
CTR3 Omar Chavez, NIOC Maryland
CT12 William Collins, NIOC Georgia
CTN1 Joseph Dean, NIOC Maryland
CTR2 Bryan Espinosa, NIOC Georgia
CTI1 Charles Farrington, NIOC Colorado
IT2 Brian Ferguson, NIOC Hawaii
CTI2 Matthew Finch, NIOC Georgia
CTM3 Benjamin Flores, NIOC Maryland
CTN3 Corey Foulds, NIOC Maryland

IT2 Randy Gardner, NIOC Maryland
CTI2 Andrew Gillen, NIOC Georgia
CTI1 Kellynn Goraczkowski, NIOC Maryland
CTI2 Champagne Green, NIOC Georgia
CTM3 Jess Urrutia, NIOC Maryland
CTN2 Carlton Harris, NIOC Maryland
CTR3 David Hawkins, NIOC Hawaii
CTI1 Jared Hess, NIOC Hawaii
CTI2 Noah Hibbler, NIOC Georgia
CTI1 Noah Hightower, NIOC Colorado
CTT2 Tiffany Hood, NIOC Colorado
CTR2 Michelle Hubenak, NIOC Georgia
CTR2 Amber Ivac, NIOC Georgia
CTN1 Thomas Jack, NIOC Maryland
CTI2 Richard Jackson, NIOC Hawaii
CTI2 Emily Jennings, NIOC Georgia
CTI2 Kristopher Jensen, NIOC Georgia
CTR2 Meredith Johnson, NIOC Maryland
CTI3 Michael Johnson, NIOC Hawaii
IT3 Zachary Jones, SUSLA Korea
IT3 Anthony Kail, NIOC Maryland
CTI2 Benjamin Kight, NIOC Texas
CTI2 Elizabeth Kingsland, NIOC Georgia
CTI2 CHGA James Kinney, NIOC Georgia
CTN1 Matthew Koss, NIOC Maryland
CTN2 Gianni Laban, NIOC Maryland
IS2 Jeffrey Lambert, USCYBERCOM
CTR2 Andrew Languille, NIOC Colorado
CTI2 Iza Lara, NIOC Misawa
CTI2 Amy Lavelle, NIOC Georgia
IT3 Omri Losh, NIOC Maryland
CTI1 Eddie Little, NIOC Georgia
CTN2 Michael Loberger, NIOC Maryland
CTI2 Kennan Locher, NIOC Maryland
CTI3 Valerie Madison, NIOC Georgia
IT2 Robert Magee Jr., NIOC Georgia
CTR2 Matthew Manley, NIOC Maryland
CTN1 Frederick Marshall, NIOC Georgia
CTN2 Jacob McCauley, NIOC Maryland
CTI2 John McCormick, NIOC Maryland
CTI2 Michael McGraw, NIOC Georgia
CTN2 Mark McKinney Jr., NIOC Georgia
IT2 Bryan McNair, NIOC Maryland
CTN2 Mario Medina, NIOC Maryland
CTI2 Sean Miller, NIOC Colorado
CTI2 Ryan Mills, NIOC Georgia
CTR3 Herschel Moore, NIOC Misawa
CTI2 Bradley Murphy II, NIOC Georgia
CTI3 Matthew Murphy, NIOC Hawaii
CTI2 David Murray, NIOC Georgia
CTN2 Dane Nelson, NIOC Maryland
IT3 Ashton Ockert, NIOC Hawaii
CTR2 Michael Odio, NIOC Georgia
IS3 Anthony Odom, NIOC Maryland
CTI3 Charles Pearman, NIOC Hawaii
CTN3 John Posey, NIOC Hawaii
CTI2 Colby Prichard, NIOC Georgia
CTT2 Tiffany Priestley, NIOC Maryland
CTT2 Samantha Purkins, NIOC Hawaii
CTN2 Nicholas Reinter, NIOC Georgia
CTR3 Richard Rengifo, NIOC Maryland
CTI2 Tyler Robinson, NIOC Maryland
CTI2 Krissa Santhi, NIOC Georgia
CTN2 Brent Savage, NIOC Maryland
CTM3 Michael Schmer, NIOC Hawaii
CTR2 Robert Schonberger, NIOC Texas
CTN2 Brice Self, NIOC Maryland
CTR2 Rebekah Serna, NIOC Misawa
CTT5 Jaylan Seymour, NIOC Georgia
CTI2 Christopher Setzer, NIOC Georgia
CTR2 Richard Sheehan, NIOC Maryland
CTN2 Sean Simmon, NIOC Maryland
CTI3 Bryce Slaughter, NIOC Maryland
IT2 Douglas Smith, NIOC Maryland
CTR2 Steven Smith, NIOC Maryland
CTI2 Clayton Snider, NIOC Georgia
CTN2 Ryan Snyder, NIOC Georgia
CTI2 Dallas Steiden, NIOC Georgia
CTR2 Evan Stewart, NIOC Georgia
CTI3 Robert Suesserman, NIOC Maryland
CTN3 Gregory Taggart, NIOC Maryland
CTN1 Nicholas Thill, NIOC Maryland
CTI1 Ryan Thomason, NIOC Maryland
CTI2 Natalie Tobey, NIOC Georgia
CTR2 Judith Torres, NIOC Maryland
CTI2 Paul Tutino, NIOC Georgia
CTN3 Harry Vargas, NIOC Maryland
CTI2 Luke Walker, NIOC Maryland
CTN2 Brittany Washington, NIOC Maryland
CTN2 Bradley Vomocil, NIOC Georgia
CTI2 Daniel Wells, NIOC Georgia
CTI2 Christopher Whempner, NIOC Maryland
CTN2 Octavia Wilkinson Jr., NIOC Maryland
CTN2 Luke Willadsen, NIOC Maryland
CTI2 Hannelore Willeke, NIOC Georgia
CTI2 Natalie Wood, NIOC Georgia
CTI2 Robert Wong, NIOC Hawaii
MA2 Iran Yamaguchi, NIOC Hawaii
CTM3 Matthias Zahn, NIOC Maryland

IT1 Leonar Ablian, NCTAMS PAC
IT3 Evan Abrahamsen, NCTS Bahrain
CTI1 Brian Achilles, NTS Bahrain
LSCS Ramon Alcantara, NCTS Naples
CTR1 Philip Alexander, NIOC Texas
LS1 Stephen Alexander, NCTAMS PAC
CTR1 Raymond Alford, NIOC Menwith Hill
CTM5 Athena Anderson, NIOC Seoul
IT2 Marquis Anderson, NCTS San Diego
IT2 Raney Anderson, NCTAMS LANT
IT1 Angel Arcegieta, NIOC Bahrain
IT1 James Argiro, NCTAMS LANT NMC DET Norfolk
CTR1 Anthony Ashby, NIOC Texas
CTI1 Christopher Auenen, NIOC Georgia
IT2 Cody Babino, NIOC Naples
IT1 Matthew Bach, NWNC Suffolk
IT1 Pablo Baez Jr., NCTS Naples
IT2 Antonio Banks, NIOC Maryland
CTN1 Nancy Baptiste, NIOC Pensacola
IT2 Andrew Barker, NCTAMS LANT
CTI2 Londyn Barrett, NIOC Georgia
CTN1 Samuel Barton, NIOC Pensacola
IT3 Jason Baugh, NAVYCYBERFOR Suffolk
LT Christopher Beaumont, NIOC Sugar Grove
IT1 Leonilo Bernal, NIOC Bahrain
IT2 Timothy Birdette, NCTAMS LANT DET Hampton Roads
CTI1 Daniel Blake, NIOC Hawaii
CTN2 Tyler Bleau, NIOC Pensacola
IT2 Abdul Borders, NIOC Norfolk
IT2 Elizabeth Bourquin, NCTAMS LANT DET Hampton Roads
IT3 Alan Bowman, NCTS Naples
IT2 Jacob Breault, NCTS San Diego
CTR2 Serge Brotous, NIOC Maryland
CTI2 Brooke Brewer, NIOC Norfolk
ET1 James Brickey, NCTAMS PAC
CTM1 Robert Brillhart, NIOC Groton
CTM3 Aaron Brindley, NIOC Yokosuka
ITC Bobbie Brinkley, NIOC Norfolk
IT1 Lindale Brooks, NCWDG
IT1 Bridgett Broussard, NCTS San Diego
LS2 Kendra Brown, NCTS Bahrain
CTI2 Jordan Burghoff, NIOC Georgia
CTN2 Derek Burnett, NIOC Pensacola
IT2 Kodzi Byers, NCTS Far East
LS1 Michael Cainion, NCTS Naples
CTR1 John Caldwell, NIOC Hawaii
MC3 Ivanne Campbell, NIOC Maryland
CTN1 Tamela Caples, NIOC Norfolk
IT1 Rogerio Cardosoconcalve, NWNC Suffolk
IS2 Matthew Carlson, NIOC Georgia

NAVY AND MARINE CORPS ACHIEVEMENT MEDAL

CTI1 Seth Watkins, NIOC Whidbey Island
LT Candas Watson, NCTS Bahrain
CWO3 Jessica Weeks, NIOC San Diego
CTIC Bailey White, NIOC Hawaii
MAC Levi White, NIOC Georgia
LCDR Craig Wightman, NIOC Hawaii
IT1 Rose Williams, NAVCOMTELSTA Sicily
CTTC Timothy Wood, NIOC Norfolk
LT Kenneth Yates, NCTS Far East
LS1 Levi Zimmerman, NIOC Bahrain
LT Antonio Zubia, NIOC San Diego

Summer Edition 2014
Special Recognition

MILITARY OUTSTANDING VOLUNTEER SERVICE MEDAL

IS2 Jenae Calloway, NIOC Norfolk
IT1 Charefa Edwards, NCTS Bahrain
IT1 Eboni Gatson, NCTS Bahrain
IT1 Dwayne Gordon, NCTAMS LANT DET Rota
CTN2 Nicholas Hardy, NIOC Pensacola
ITC William Heitsman, NNWC Suffolk
IT2 Justin Houser, NCTAMS PAC
LCDR Darrell Keller Jr., NIOC Norfolk
CTT1 Rodney Martin, NIOC Georgia

ITC Simone Odom, NCTS Bahrain
YN2 Samandra Otey, NIOC Maryland
YN1 David Parham, NCTS Bahrain
CTR1 Derek Raulston, NIOC Texas
IT1 Robert Rydl, NCTAMS LANT
LS2 Reneerose Solis, NIOC Misawa
CTN2 Ryan Swoboda, NIOC Texas
ET2 Ricky Wallen, NCTAMS LANT
LSC Felicia Wells, NIOC Maryland
CTT1 Jason Winters, NIOC Seoul

CIVILIAN LENGTH OF SERVICE AWARDS

Ruth Fox, NAVCYBERFOR Suffolk - 30 Years
Christina Louzonis, NAVCYBERFOR Suffolk - 20 Years

Rashita Morris, FLTCYBERCOM FT Meade - 20 Years
Sandra Anderson, NAVCYBERFOR Suffolk - 10 Years
Richard Cecconi, NAVCYBERFOR Suffolk - 10 Years
Maurice Edgington, NAVCYBERFOR - 10 Years
David Jackson, NAVCYBERFOR Suffolk - 10 Years
Willam Krump, NAVCYBERFOR Suffolk - 10 Years
Mark Lanni, FLTCYBERCOM FT Meade - 10 Years
Allen Morrison, NAVCYBERFOR Suffolk - 10 Years
Rafael Negron, FLTCYBERCOM FT Meade - 10 Years
Todd Newell, Jr., NAVCYBERFOR Suffolk - 10 Years
Dwayne Paul, NAVCYBERFOR Suffolk - 10 Years
Donald Scott, FLTCYBERCOM FT Meade - 10 Years
Lorie Vann, FLTCYBERCOM FT Meade - 10 Years
Mariza Watson, FLTCYBERCOM FT Meade - 10 Years
Kevin Williams, NAVCYBERFOR Suffolk - 5 Years
Barbara Materna, FLTCYBERCOM FT Meade - 5 Years
Jason Watson, FLTCYBERCOM FT Meade - 5 Years

(Left to right) Tim Lawlor, AFCEA Hampton Roads Civilian Cyber Professional of the Month for July 2014 poses with, LCDR Doug Vanderlip (AFCEA HR President). Lawlor was recognized for his outstanding performance as the Navy Cyber Forces Lead for Intelligence Systems Modernization & Readiness. He was also selected as NAVCYBERFOR’s Senior Civilian of the Month for August.

NAVCYBERFOR DET San Diego -- IT1(IDW/SW) Winora Whatley was recently awarded a NAM by RDML Diane E.H. Webber, Commander, NAVCYBERFOR. Whatley is working on her Bachelors at Vincennes University online. She was the detachment’s JSOY two years running (2012-2013) and has been in the Navy 13 years. She is enroute to Kadena AFB Okinawa, Japan.
IW Officer Salutes Forerunners
‘Remembering . . . those who came before us’

By MC2 David Finley, U.S. Fleet Cyber Command/U.S. 10th Fleet Public Affairs

APT Joseph John Rochefort was a major figure in the U.S. Navy’s development of cryptologic and intelligence capabilities from 1925 to 1947. He headed the Navy’s then fledgling cryptanalytic organization in the 1920’s and “. . . provided singularly superb cryptologic support to the U.S. Fleet during World War II, leading to victory in the Pacific,” as the award message noted.

At the end of his career (1942-1946), Rochefort successfully headed the Pacific Strategic Intelligence Group in Washington, DC. Many feel Rochefort wrote a critical chapter in the Navy and nation’s history in both the Cryptologic and Intelligence communities. And they believe that without superb Sailors and professionals such as this, the intelligence community would not be the same today.

In 1986, Rochefort posthumously received the Presidential Medal of Freedom for his contribution during the Battle of Midway.

Today, IW officers, born from naval cryptology, are directly involved in every aspect of naval operations, deploying globally to support Navy and joint military requirements.

IW warfighters execute the full spectrum of cyber, cryptology, signals intelligence, information operations, computer network operations (exploit, defend, attack) and electronic warfare missions. They operate afloat and ashore and serve at the National Security Agency, the Pentagon, Navy Information Operations Commands and regional cryptologic centers across the globe.
"OUR FLAG"

This isn’t just material.
This isn’t just a rag.
This represents our Country,
And it’s called our American Flag.

A lot of people fought for it,
and gave their lives for you.
They are all proud servicemembers,
who honor the Red, White and Blue!

So when you see someone in uniform,
Go up and shake their hand.
And let them know how proud we are,
that they are protecting our land.

When our Troops are serving and
very far from home,
Write them a letter or send them a package,
to let them know they’re not alone.

Those who fought and gave their lives;
they’re our Brothers, Sisters, Husbands and Wives.
These are the Soldiers, Sailors, Airmen and Marines,
who are keeping us free!

So you see my friends, the American Flag,
actually belongs to you and me!

SSG Thomas K. Barnes Jr.
U.S. Army
LOOK FOR US ON THE WEB

www.cyberfor.navy.mil
or
www.facebook.com/USNavyCyberForces