



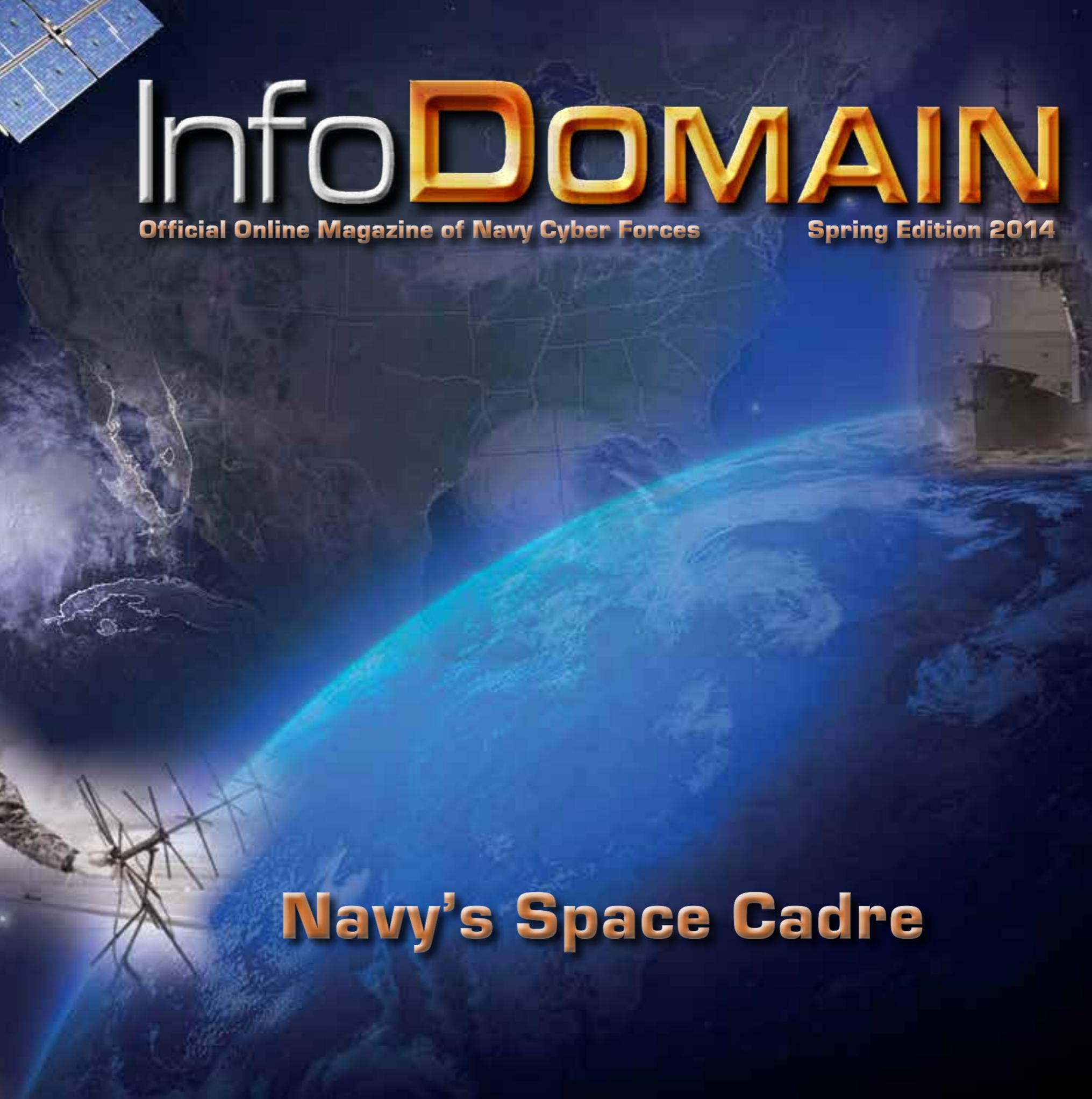
InfoDOMAIN

Official Online Magazine of Navy Cyber Forces

Spring Edition 2014



Navy's Space Cadre



- 2 **RDML Webber Addresses CYBERFOR's Newest Transition**
CYBERFOR hosts Suffolk Mayor visit and IDFOR type planning conference.
- 11 **MyDOMAIN**
Navy Space Cadre and Warfighters putting pieces together.
- 13 **Marines Look to Space During NSOC**
CYBERFOR & NETWARCOM educate Marines about space capabilities.
- 15 **Navy Process Reference Model**
The Navy's "Lego Building Set" for IT explained in detail.
- 23 **CIO's Network Tips**
Network Man reminds us not to be "The Weakest Link".
- 25 **Cyber Student Honored with Mayo Award**
LT Jason Hughes received high honor while attending NPS.
- 29 **Copernicus Awards**
Co-sponsors reconize FCC & 10th Fleet members.
- 30 **Outstanding Crypies Recognized for "On The Roof Gang" Awards**
Sailor and a Marine chosen as 2014's best cryptologists.

- | | | |
|----------------------------|-------------------------------|--------------------------|
| 4 HqtrsCYBERFOR | 9 Short Circuits | 10 Cyber Warriors |
| 17 CID Spotlight | 20 NMOC Spotlight | 26 Team Spotlight |
| 28 People Spotlight | 31 Special Recognition | 36 Diversity |

FRONT COVER: *The Navy's Space Cadre has two branches in its Officer Corps: Space Aquisitions professionals and Space Operations professionals. Satellite, Joint Space and Afloat Space Operations are just a few of the Space Cadre's missions, as well as Space Requirements Analysis. For more information and pictures of the Navy's Space Cadre see Pages 11-14. (Photo Illustration By Robin Hicks)*



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





(Standing) RDML Diane E. H. Webber, Commander, NAVCYBERFOR, addresses her staff at recent All Hands. Webber and key senior leadership gave an update on the IDFOR's pending stand up, scheduled for Oct. 1. (Photo by Jacky Fisher)

Fleet Gains from Newest Transition

From Commander, NAVCYBERFOR Public Affairs

I want to give the Cyber community, from a historical perspective, one of the major reasons why we are once again going through another transition period. Since the mid-80's the cyber battlespace has become more complex and technological advances are morphing almost faster than we can train to defend against them.

Only three disciplines predominated during the Cold War Era: cryptology - code breaking; deception; and PSYOPs (psychological operations). Today's dynamic environment has us defending more than just computers and the battle field has now reached out in to the fifth domain of warfare, cyberspace. So we need to streamline our assets

Information Dominance Forces (IDFOR) Type Command (TYCOM).

This will be accomplished by taking what we have now - cyber and C5I (Command, Control, Communications, Computers, Combat System and Intelligence) – drawing on the talents of the IDC (Information Dominance Corps) – intelligence, information warfare,

to better meet the challenges of today and those coming down the pike.

This 'realignment' should be looked upon as more of 'an alignment of functions' - man, train and equip – that currently are being performed by Navy Cyber Forces, Fleet Cyber Command/10th Fleet and three or four other commands. The end goal is to make a way for Navy Leadership to integrate information and systems requirements through a single focal point.

That single focal point will be the

oceanographers and the information professionals – and combining those assets with the space and electromagnetic spectrum cadres. There is something quite unique in building something new when its foundation is based on the rich and successful, individual histories of communities that have been established since before World War II. The IDC will take those 'individual' histories and make them 'our' histories as we meet head on the ambitious goal of standing up the newest TYCOM by the end of this year.

Navigating the turbulent waters of 'change' is challenging. But I'm confident, as is the CNO, that the task will be completed on schedule. The end result will be a single, integrated Information Dominance Community to provide relevant and effective capability as well as a highly trained workforce to meet any challenge.

The Navy stands to gain much by standing up the IDFOR. Coordinating with Fleet TYCOMs, while balancing resources and requirements, IDFOR will have the capacity to deliver qualified and ready forces and Information Dominance capability at the right time and at the best cost for mission success. I appreciate everyone staying flexible and keeping the end goal in sight. ✘



Mayor Visits NAVCYBERFOR

From NAVCYBERFOR PA Office

SUFFOLK, VA – RDML Diane E. H. Webber, Commander, Navy Cyber Forces (NAVCYBERFOR), hosted the Honorable Linda T. Johnson, Mayor of Suffolk, for an office call and a facilities tour on Feb. 25.

Johnson was accompanied by Suffolk City Manager, Selena Cuffee-Glenn, Deputy City Manager, Patrick Roberts, and Assistant Director of Economic Development, Gregory Byrd.

This was the Mayor's first visit to NAVCYBERFOR since the command relocated from Joint Expeditionary Base Little Creek - Fort Story in Virginia Beach to the Lake View Parkway complex in Suffolk last October. Among the topics discussed were the relocation efforts of NAVCYBERFOR, future opportunities for the Suffolk/Hampton Roads business communities, and community relations opportunities to partner with NAVCYBERFOR personnel.

"It is an honor to welcome the Navy Cyber Forces command to the City of Suffolk where their new base of operations will be a boon to our community's

neighborhoods, retail, dining and service industries," said Johnson. "We look forward to forging a long lasting partnership founded upon mutual support, admiration, and commitment to service.

During a gift exchange, the Mayor presented Webber with a glass peanut signifying the city's ties to the peanut industry. Byrd presented a Suffolk Welcome Basket filled with an assortment of products made by businesses located in the City of Suffolk.

In turn, the admiral gave Johnson a maritime compass, command coin and a commemorative photograph of her visit.

"We are very happy to be aboard in our new facilities and to be part of the community here in



(Standing) RDML Diane E. H. Webber, Commander NAVCYBERFOR accepts a glass peanut from the Honorable Linda T. Johnson, Mayor of Suffolk, VA. Johnson and her staff recently visited the command's new location in Suffolk, VA. NAVCYBERFOR relocated to Suffolk from JEB Little Creek - Fort Story, Virginia Beach, VA, last October. (Photo by Robin Hicks)

Suffolk," Webber said during the exchange. "It's a wonderful location, close to many amenities which our staff is excited to explore." ✂



NAVCYBERFOR Hosts Conference

(Seated -- Center) RDML Diane E. H. Webber, Commander, Navy Cyber Forces (NAVCYBERFOR) kicked off the Information Dominance Force (IDFOR) type command planning conference Feb. 10 at NAVCYBERFOR in Suffolk, VA. The conference attendees included senior advisors from Chief of Naval Operations (OPNAV), Fleet Forces Command (FFC), Commander, Naval Meteorology and Oceanography Command (CNMOC), Office of Naval Intelligence (ONI), Fleet Cyber Command (FCC) and representatives from NAVCYBERFOR directorates. Some of the topics being discussed include resources, billets and budget to be applied to the new IDFOR TYCOM scheduled to stand up Oct. 1. (Photo by Robin Hicks)

OPERATING IN NEW CYBER NORM

EDITOR'S NOTE: *The following article is taken from a Navy Live blog, Dec. 18, 2013, by then RADM Jan E. Tighe, Deputy Commander, U.S. Fleet Cyber Command/U.S. 10th Fleet.*

Why does the Navy keep enhancing the security of its networks, taking actions that at times have made things challenging for users? The answer is that we as a Navy, and as a society, are now operating in an age of constantly evolving cyber threats and network intrusion capabilities. We are operating in a new "cyber norm."

What is the new "cyber norm"? It is the reality in which we operate and requires the entire Navy team to constantly stay ahead of the adversary in the cyber arena. The Navy's network defenders must consistently and dynamically outpace the enemy, denying adversaries any benefit. As important, every user must understand their responsibility to also deny the enemy any advantage when on the network. After all, if the Navy has given you access to a keyboard, you are operating in the cyber domain.

With the stand-up of U.S. Fleet Cyber Command and re-commissioning of U.S. 10th Fleet in January 2010, the Navy recognized the need to confront a new challenge to our nation's security in cyberspace. Over the nearly four years since then, as the Navy's culture has begun to change with respect to cyber in Joint warfighting, the necessity for an active cyber defense has become more and

more apparent.

Late summer of 2013, the Navy expanded its aggressive campaign to enhance the security of its networks. Since then and moving forward, we will continually apply defensive measures and architectural hardening improvements (making the network more defensible) to strengthen the security of our networks.

In fact, it is part of this ongoing effort to improve network and cyber security that brought the Chief of Naval Operations, ADM Jonathan Greenert, to Fort Meade Dec. 17th to recognize the warfighters of U.S. Fleet Cyber Command, the warriors who have taken unprecedented network

"In January 2010, the Navy recognized the need to confront a new challenge to our nation's security in cyberspace. In the nearly 4 years since then, the necessity for an active cyber defense has become more and more apparent."

VADM Jan E. Tighe, CDR FCC/10th Fleet

maneuver measures over the past several months to increase security.

At times these network hardening actions have inconvenienced Sailors and our Navy workforce, but in balance they have been essential within this new cyber norm to supporting the Navy's vision as described in Navy Cyber Power 2020 (see footnote *1). Specifically a key goal envisioned: assuring access to cyberspace and confident command and control (C2).

These hardening actions are part of the broader Department of Defense effort to continue to develop and refine extensive capabilities to defend its networks. An example is more stringent log-in requirements, which are focused on strengthening network

and information security and minimizing exploitable vulnerabilities.

Additionally, related to the network defense measures being implemented to improve cyber security, certain Navy web applications and websites are now (or will become) accessible only from within the Department of Defense Information Network (DODIN), also known as the ".mil" domain. Sailors and Navy workforce members who experience the inability to log into an application while working outside of .mil domain should contact their local Information Assurance Manager (IAM) for details. In other words, if a Sailor finds an application they used to be able

to access from a home computer, for example, is no longer accessible there, he or she should try

from a computer connected to the DODIN or contact the IAM.

Security improvements such as these may seem inconvenient and will take time to adjust to, but these changes have been implemented to provide the increased network and cyber security necessary given the new cyber norm in which we operate, that is, they are in fact vital to defending our networks against increasingly sophisticated and determined adversaries.

Americans, our allies and our adversaries can be confident that Sailors worldwide in the Fleet Cyber Command/10th Fleet domain, the broader Information Dominance Corps, and across our great Navy are on watch 24/7/365. The vital

Official U.S. Navy Photo



VADM Jan E. Tighe

importance of network and cyber security at the individual user level, however, cannot be emphasized enough; it takes all hands being vigilant with network security to assure access to cyberspace and confident C2.

As then VADM Michael S. Rogers has said before, "we will continue to develop standards of accountability for the cyber domain, like other warfighting domains, in step with the Navy's long tradition of holding all hands responsible for their actions, cyber security is the responsibility of the entire Navy team."

Given the new cyber norm in which we operate, all hands must be vigilant. Network security starts with you.

... continued on Page 5





**1 -- Signed in November 2012 by both VADM Kendall Card, former Deputy Chief of Naval Operations for Information Dominance and Director of Naval Intelligence, and VADM Michael S. Rogers, former Commander, U.S. Fleet Cyber Command/U.S. 10th Fleet, Navy Cyber Power 2020 is the road map for success in this new era and requires U.S. Fleet Cyber Command/U.S. 10th Fleet (FCC/C10F) to continually address cyber threats, key trends, and challenges across four main areas: (1) integrated operations, (2) an optimized cyber workforce, (3) technology innovation, and (4) reforming development and execution of our requirements, acquisition, and budgeting.*

Since the November 2012 signing of Navy Cyber Power 2020, the U.S. Fleet Cyber Command and U.S. 10th Fleet team world-wide has worked tirelessly to drive toward and thus maintain these desired outcomes in the dynamic cyber arena in which we operate.

To review this blog as well as past and future blogs, go to: <http://navylive.dodlive.mil/>.

CNO Establishes Information Dominance TYCOM

By Joseph F. Gradisher, Office of the DCNO for Information Dominance (N2/N6)



WASHINGTON - Chief of Naval Operations ADM Jonathan Greenert directed Commander, U.S. Fleet Forces Command (CUSFFC) to establish an Information Dominance Type Command (TYCOM).

In his March 4 memorandum to CUSFFC, Greenert wrote, "I approve the establishment of Navy Information Dominance Forces as an echelon III command under your administrative control. As the immediate superior in command, oversee the command's implementation...with an initial operating capability of Oct. 1, 2014."

The TYCOM will report directly to CUSFFC and have supporting relationships with the rest of the Navy, focusing primarily on the Navy's information environment.

Commander, Navy Cyber Forces, RDML Diane Webber will have her command re-designated as Commander, Navy Information Dominance Forces (NAVIDFOR) and will provide the initial infrastructure, resources and assets for the TYCOM.

Webber noted that the new TYCOM's mission will be to "support Combatant Commanders and Navy Commanders ashore and afloat by providing

forward deployable, sustainable, combat-ready Information Dominance forces."

Full operational capability for NAVIDFOR is expected by the end of the calendar year.

A Navy Type Command or TYCOM, coordinates the Man, Train and Equip (MT&E) functions for specific communities within the Navy. For example, Commander, Naval Air Forces exercise administrative control over aviation forces and Commander, Navy Surface Forces does the same for the surface warfare community.

NAVIDFOR will serve in that capacity for the Information Dominance Corps (IDC).

The IDC was formed in 2009 and built on the deep expertise and strengths of the officers/enlisted, active/reserve, and civilian workforce from the oceanography/meteorology, information professional, information warfare, naval intelligence and space cadre. The IDC is an inter-disciplinary corps that possesses a deep understanding of potential adversaries and the battle space, is able to accurately identify targets and brings an array of non-kinetic, offensive and defensive capabilities to the fight in the

Information Age.

According to VADM Ted N. "Twig" Branch, Deputy Chief of Naval Operations for Information Dominance (N2/N6) and the lead for the Navy's IDC, "The continuing evolution of Information Dominance as a Navy warfighting discipline demands a single, integrated TYCOM to provide relevant and effective capabilities, including a highly trained and motivated workforce. I'm confident the new NAVIDFOR will provide the Fleet and the entire Navy the ID capabilities needed to deter, fight and win within this information domain."

Previously, those MT&E functions for the various communities within the IDC were executed by OPNAV N2/N6, Fleet Cyber Command/Commander Tenth Fleet, Navy Cyber Forces, the Office of Naval Intelligence, and the Navy Meteorology and Oceanography Command.

Commander, Navy Information Dominance Forces will be based in Suffolk, VA.



U.S. Fleet Cyber Command/U.S. 10th Fleet Change of Command

From Commander, FCC /C10F Public Affairs

FORT MEADE, MD -- U.S. Fleet Cyber Command/U.S. 10th Fleet (FCC/C10F) conducted a change of command April 2 at the Frank B. Rowlett Building located at Fort George G. Meade, MD. VADM Jan E. Tighe relieved ADM Michael S. Rogers as commander in a ceremony held at fleet headquarters.

With this appointment, Tighe becomes the third commander of FCC/C10F and the first female commander of a numbered fleet in U.S. Navy history.

“It is an honor to take command of this outstanding warfighting organization and to be able to continue working with the tremendous team of uniformed and civilian professionals,” said Tighe.

Tighe has served as Deputy Commander of FCC/C10F since November 2013.

Rogers takes the reigns as Commander, U.S. Cyber Command and Director, National Security Agency/Chief, Central Security Service.

“It has been a tremendous honor and privilege to serve as your commander for the last two and a half years. Your support of the nation’s maritime strategy by effectively employing

our mission capabilities globally has been outstanding,” Rogers said. “I now pass the conn of [FCC/C10F] to VADM Jan Tighe. She is an exceptional leader, innovative thinker and stalwart warfighter who will continue our momentum of mission accomplishment and transformation.”

Tighe was promoted at the National Cryptologic Museum by Army Gen. Keith B. Alexander who retired March 28 from his position as Commander of U.S. Cyber Command and Director, National Security Agency/Chief, Central Security Service.

“I think the greatest honor and privilege I’ve had is to work with great people,” Alexander said, “and Jan Tighe, you are one of the best people that our military has across all of the Services.”

“You are exceptional in every category and you will do great with 10th Fleet, which I believe is just a stepping stone for future things for you,” Alexander went on to say.

Tighe was born in Bowling Green, KY, and raised in Plantation, FL.

Her previous tours include duty with Naval Security Group Activities in Florida, Virginia, Japan, VQ-1 and Naval Information Warfare Activity.



VADM Jan E. Tighe smiles as she assumes command of FCC/C10F during a ceremony conducted at Fleet headquarters. Tighe relieved ADM Michael S. Rogers, who takes over as Commander of U.S. CYBERCOM and Director of the NSA and Chief of the CSS. Tighe is the third Commander of U.S. Fleet Cyber Command and U.S. 10th Fleet and the first female commander of a numbered Fleet in Navy history. (Photo by MC2 David R. Finley Jr.)

She also had staff assignments on the Headquarters of the Pacific Fleet, Naval Security Group, Naval Network Warfare Command, and served as Executive Assistant to Commander, U.S. Cyber Command. Tighe commanded more than 2,800 multi-service and multi-agency personnel at the National Security Agency/Central Security Service Hawaii in Kunia.

As a flag officer, Tighe has served as

U.S. Cyber Command Deputy J3; OPNAV N2N6 Director, Decision Superiority; Naval Postgraduate School Interim President; and Deputy Commander, FCC/C10F.

Tighe is a graduate of the U.S. Naval Academy and was commissioned as an ensign (special duty cryptology) in 1984. She attended the Defense

... continued on Page 7



... continued from Page 6

Language Institute in Monterey, CA, where she studied Russian. She also attended the Naval Postgraduate School, Monterey, CA, and in 2001 was awarded a Ph.D. in Electrical Engineering and a M.S. in Applied Mathematics.

Tighe wears both the Information Dominance Warfare insignia and Naval Aviation Observer wings, which she earned while deployed as an airborne special evaluator aboard VQ-1 EP-3E aircraft in the Persian Gulf during Operation DESERT SHIELD/STORM. She is also a member of the Acquisition Professionals Community and holds a Level III Defense Acquisition Workforce Improvement Act (DAWIA) certification in Program Management.

U.S. Fleet Cyber Command serves as the Navy component command to U.S. Strategic Command and U.S. Cyber Command, and the Navy's Service Cryptologic Component commander under the National Security Agency/Central Security Service. Fleet Cyber Command also reports directly to the Chief of Naval Operations as an Echelon II command.

The 10th Fleet is the operational arm of Fleet Cyber Command and executes its mission through a task force structure similar to other warfare commanders. ✂

Official U.S. Navy Photo



By Jim Garamone, American Forces Press Service

FORT MEADE, MD -- ADM Michael S. Rogers assumed command of U.S. Cyber Command and became director of the National Security Agency and the Central Security Service during a ceremony here April 3.

He succeeds Army Gen. Keith B. Alexander, who retired last week, in all three posts. Previously, Rogers was Commander of the Navy's 10th Fleet, the service's cyber arm. He has already been confirmed by the Senate.

Michael G. Vickers, Undersecretary of Defense for Intelligence, said Rogers is the right man for the job during a challenging time, and that the NSA has been

The admiral said he had no compunction about taking the posts, "because I believe in the mission of the National Security Agency and I believe in the mission of the United States Cyber Command."

The admiral noted that for his entire naval career, he has been associated with cyber warriors and he stressed his faith in the men and women of NSA and Cyber Command.

"I believe in you," he said. "I've had the honor of working with many of you for almost my entire adult life. I love the people I've had the pleasure of serving with and I am honored to be a member of your team."

central to America's national security.

Rogers called for a moment of silence during the ceremony for "our Army teammates who are facing a great tragedy at Fort Hood."

The admiral takes the reins at a time of tremendous turmoil in the intelligence community, as thousands of documents published on Wikileaks and others released by former NSA contractor Edward Snowden detailing highly classified NSA surveillance operations have caused an uproar. Rogers alluded to that when he said friends told him, "Congratulations, I guess," when they heard of his new job.

... continued on Page 8



... continued from Page 7

Rogers stressed that the key to success in the future will be about partnerships.

“The most important partnership for all of us will be that between U.S. Cyber Command and the National Security Agency,” he said. “We need each other to execute our missions. That’s why we’re together the way we are, that’s why we have the structure, and I believe in that structure.”

Partnership must extend beyond DoD, the admiral said. The organizations must strengthen partnerships with the FBI, the Homeland Security and Justice departments and the director of national intelligence, “but even more broadly than that,” he said.

He noted that these are challenging times for the organizations. “I love challenges,” he said, “because I believe that challenge and change represents opportunity, and I love opportunity.”

The organizations have the opportunity to create “something even better, that’s focused not only on the challenges of today, but what people will need in five to 10 years to succeed,” the admiral said.

Rogers said he will squarely accept the challenge of regaining the trust of some Americans “who don’t believe us,” and he pledged to “engage in a dialogue with the citizens of our nation about what we do and why we do it.”

There has not been a discussion about the role of NSA with the public, he acknowledged. “We live in a world of great risk,” he said. “There are individuals, groups out there who, if they had their way, we would no longer exist as a nation.”

Rogers said there will be strict adherence to law and policy in the cyber world.

“There are no shortcuts here, teammates,” he said.

“Americans don’t know the specifics of what the organizations do, but they want to trust us,” Rogers added. “If we make mistakes we will stand up and hold ourselves accountable and responsible.” ✂



ShortCIRCUITS

Enlisted Cyber Master’s Degree Opportunity at Postgraduate School

WASHINGTON -- NAVADMIN 057/14 solicits enlisted member applications for enrollment in the Naval Postgraduate School’s (NPS) 12-month Master of Science in Applied Cyber Operations.

This program is one of many efforts to increase the Navy’s cyber capabilities, while building a professional cyber workforce. Selectees will have the opportunity to enhance the learning environment for all students through their background with real world network experiences in the operational environment.

Selectees will be assigned to Navy-funded education as full-time students under permanent change of station orders to Monterey, CA, with either a September 2014 or March 2015 start. As full-time students, Sailors will be required to carry a full academic load year-round. Degree requirements should be completed in 12 months and will include a capstone project.

This program is only available to active-duty and full-time support members in the Information Systems Technician (IT) and Cryptologic Technician Networks (CTN) ratings who meet the following criteria:

- Must possess a bachelor

of science degree in a relevant technical field including, but not limited to, computer science, electrical engineering, and information or engineering technology.

The degree must have been awarded by an institution of higher learning accredited by a regional accrediting agency recognized by the U.S. Department of education.

To meet NPS academic requirements, performance in technical courses, including mathematics, must be high.

The Academic Profile Code (APC) for this program is 3.44 (minimum 2.20 GPA, calculus for business/social sciences with a grade of C or better, and one calculus based physics course with a minimum grade of C). Please refer to the NPS academic catalog for specific information on calculating the APC.

- Must be an E6 or above eligible for CONUS/shore assignment between April and December 2014 for the September 2014 start or between October 2014 and June 2015 for the March 2015 start.
- Must be eligible to incur a

five-year active-duty service obligation by reenlistment or extension of enlistment prior to NPS enrollment. Selectees will be required to reenlist more than one year earlier if they are unable to satisfy the five-year obligated service requirement with an aggregate of 48 or fewer months of extensions.

An extension will become binding upon enrollment at NPS. Per Reference (a), payment of the Selective Reenlistment Bonus (SRB) is not authorized for selectees who reenlist for the purpose of meeting the obligated service requirement.

- Must be within PFA standards with no PFA failures within the last three years.
- Must have no evaluation marks below 3.0 within the last five years.
- Must hold or be eligible for a Top Secret (TS)/ Sensitive Compartmented Information (SCI) clearance. Applicants without a current TS/SCI clearance are still encouraged to apply, but should work

... continued on Page 9



... continued from Page 8

- with their Special Security Office to initiate the clearance request. Orders to NPS will not be issued until TS/SCI clearance is finalized.
- Must possess a conditional letter of acceptance. To obtain a conditional letter of acceptance, Sailors should apply to NPS at: <http://www.nps.edu/academics/admissions/applyonline/applynow.html>.
Once registered, Sailors should select applied cyber operations, curriculum number 336. Upon application submission, Sailors must arrange for submission of a sealed official

transcript to the NPS admissions office from each institution attended for all undergraduate and graduate education, as well as all Sailor/Marine American Council on Education Registry Transcripts or Joint Services Transcripts (JST).

Sailors who are not conditionally accepted will be notified by NPS via e-mail.

Upon selection, member must request (via command Career Counselor) an in-rate quota in the Career Waypoints (CWAY) system. Those members not in their CWAY window should submit a “special circumstance” application

indicating reason code of “other” and the Career Counselor will be prompted to add a note indicating selection to the Master of Science in Applied Cyber Operations program. If selected via “special circumstance” application, this program does not guarantee awarding of an in-rate CWAY quota and is not considered part of an individual’s performance indicator in the CWAY process.

Prospective applicants should contact their detailers immediately to discuss implications for their current assignments. Failure to do so may result

in the withdrawal of selection. Applications can be sent via encrypted e-mail to michael.saunders@navy.mil or mailed to:

**Deputy Chief of Naval Operations
(Information Dominance/Director of
Naval Intelligence) (N2/N6)
2000 Navy Pentagon
Washington, DC 20350-2000**

Eligible Sailors should forward a written request via their Commanding Officer.

For more information on how to properly apply for this program, refer to NAVADMIN 057/14. ✂

FY-15 Legislative Fellows Eligibility & Application Procedures

WASHINGTON – NAVADMIN 047/14 in conjunction with BUPERSINST 1560.21E, announces application procedures for the FY-15 Navy Legislative Fellows Program. Ref (a) provides background and guidance for submission of applications. Applications are due no later than April 30, 2014.

Potential fellows must have demonstrated sustained superior performance and potential for future assignments in critical billets.

Military Applicants:

Participation is limited to Unrestricted Line Officers, Restricted Line Officers and Staff Corps Officers in the permanent grades of O-3 through O-5. The selection process will focus on individual performance, promotion potential, academic and subspecialty qualifications, needs of the Navy and availability for follow-on assignment. Officers who have Permanent Change of Station orders issued will not be considered.

A year-long fellowship followed by a utilization tour makes this a minimum three-year program, for which

career timing is an important consideration. All officer applicants must contact their detailers for counseling on the career impact of participation in the Legislative Fellows Program.

Additional program information can be found at the following Website: [http://www.public.navy.mil/bupers-npc/officer/detailing/Education placement/pages/legislativeaffairs.aspx](http://www.public.navy.mil/bupers-npc/officer/detailing/Education%20placement/pages/legislativeaffairs.aspx).

Civilian Applicants:

Senior civilian employees, GS-13 and above or equivalent, interested in the Capitol Hill Fellowship Program are encouraged to contact their local civilian training officer for information on submission of applications for FY-15. Parent commands are responsible for all program costs.

Questions concerning department of the Navy civilian participation should be directed to Ms. Janet Evans at (202) 685-6493 or via e-mail at janet.m.evans@navy.mil. A description of the program can be found at: <https://www.portal.navy.mil/donhr/>

trainingdevelopment/pages/chfp.aspx.

Upon notification, selectees must be available to report to Washington, DC, no later than November 2014 for an orientation program, followed by a full-time one-year assignment to a congressional member’s office. During the Fellowship, officers will be assigned to the Office of Legislative Affairs for administrative purposes. The one-year Fellowship is typically followed by a utilization tour of at least two years in length in a legislative-related assignment on a senior headquarters staff. Upon execution of orders, fellows agree to serve on active-duty for three years following completion or termination of the Fellowship.

Points of contact are LCDR Natalia Henriquez, Navy fellows program manager, Office of Legislative Affairs, at (703) 697-2885/ DSN 227 or via e-mail at natalia.henriquez@navy.mil; and LCDR Angelin Graham, Pers-440 at (901) 874-4056/DSN 882 or via e-mail at angelin.graham@navy.mil. ✂



How To CLIMB LADDER OF SUCCESS -- WITH HANDS-OFF APPROACH

CTI1 April Mule steps back to gain time to properly manage her Department

Story and Photo by MC1 Leeanna Shipp, NCWDG Public Affairs

WASHINGTON, DC - Cryptologic Technician (Interpretive) 1st Class April Mule, a Lafayette, NY native, is the Leading Petty Officer (LPO) of the Target Analysis and Intelligence (TA&I) department at the Navy Cyber Warfare Development Group (NCWDG). She is in charge of Cryptologic Technician Collection (CTR), Intelligence Specialists (IS) and Cryptologic Technician Interpretive (CTI), which makes her unique.

There are 20 first class petty officers in her department and she is only one of three CTI's and the only LPO in her rate. She spends most of her day managing administrative tasks. As a Division LPO, she was able to be very involved with the mission and Sailors around her. Now, as Department LPO she has had to take more of a hands-off approach; something that took a little getting used to.

"Taking a step back as the Department LPO was a personal adjustment for me. I am use to being operational and always on the go," said Mule. "Now there's less time to be hands on because I have to manage my Sailors administratively more so than and operationally."

The LPO position is a grooming position for Chief. Having good communication and trust between the LPO, Leading Chief Petty Officer (LCPO), and Department Head is essential to running a department smoothly.

"I am confident that my Department Head has a good pulse on the department. There is constant

communication between me, the LCPO and our Department Head. We all keep each other up to date throughout the day," said Mule.

There is a different level of trust given at the LPO position. Because being an LPO is grooming her for



CTI1 April Mule, N2 (Target Analysis and Intelligence) Department LPO, discusses the organization of one of her divisions with the T3 Division LPO, CTR1 Raymond Donato.

Chief, Mule is treated as such and given a different level of trust that involves not only the administrative side of the house, but also in how she manages her Sailors and Division LPOs.

"It is interesting to see how the Chief's Mess and Wardroom work together. Before I was Department

LPO, I was not able to see the decision making process first hand," said Mule.

She is a very direct LPO. If there is an issue, she gets it out in the open as soon as possible to address and solve the problem at the lowest level. She has learned to be less reactive and more proactive. Instead of reacting right away when something needs to be squared away she pulls her Division LPOs aside to figure out the problem and come up with a solution as a group.

"Every department relies on TA&I, so we have to run as efficiently as we can to be able to fulfill not only our mission, but to support the other departments in their mission," said Mule.

She came from a command that was able to use a prototype piece of equipment NCWDG developed and now she is helping to develop that future software and equipment.

"Being stationed at NCWDG gives me a sense of heritage," she said. "To be a part of what we are doing now, knowing that what we are building and testing will be used in the future, I can say I was a part of that."

Without analysis of information collected from all sources, the NCWDG wouldn't be where it is today. The Target Analysis and Intelligence Department plays a huge role in the command's mission of research, development and operational analysis. This department provides focused intelligence support for information operations and is the backbone of the command. ✂



Navy Space Cadre ^{And} Warfighters Putting Pieces Together

By CDR Adam "Tito" C. DeJesus, NAVCYBERFOR N13/N17

As the Space Cadre Readiness Officer for Navy Cyber Forces, I am frequently asked the question: "What is the Navy Space Cadre, and what do they do for the warfighters?" This article outlines the need for space professionals in the Navy and describes some of the major functions of the Navy Space Cadre.

Prior to the 1957 launch of Sputnik I, there were no satellites. Navy ships communicated via wireless Ultra High and High Frequency (UHF and HF) radios, mostly by voice or Morse code. Intelligence and surveillance activities were performed by submarines and aircraft, which were vulnerable to attack and could not get close to the sovereign territory of other nations. We predicted weather using balloons, aircraft and scientific guesses. We navigated the oceans by dead reckoning in daylight and by the stars at night.

Over the past 60 years the Navy has come to rely on the significant operational and tactical advantages afforded by our national assets in space. Satellites allow us to see and talk over the horizon and around the world. Digital communications via satellite provide high data rates and high security. We can look into our adversary's territory without putting lives at risk. We can see a third of the planet at once from geosynchronous orbit and spot hurricanes thousands of miles away. We can fly a pilotless airplane around

the world and know its position to within a yard or two.

To most of us in the Navy, it seems that the United States has mastered the space domain: just look what we can do! But we tend to take our space capabilities for granted. We tend to think they have always been there for us, and that they will always be there for us. If asked, "What would you do without those satellites to help you," we tend to think it is someone else's problem. Fact is, it is a problem that we have to address in order to stay ahead of our potential adversaries. Just as militaries throughout history have fought for control of the land, sea and air, we must be prepared to fight for control of space.

While it's true that we don't fight "in" space, the 21st century is rapidly becoming an era where national and non-traditional forces are fighting "over" space. Jamming of satellite signals including Global Position System (GPS) and satellite communications (SATCOM) is a growing threat. The recent increase in the number of orbiting satellites is causing congestion of critical orbital regimes. As foreign countries build and launch satellites in greater numbers, with more and more advanced capabilities, U. S. ships, aircraft, submarines, and ground forces are no longer free from foreign space-based surveillance. The Navy is particularly dependent on space to support information transport, missile warning and precision navigation and targeting; and where the Navy used

... continued on Page 12

enjoy an operational advantage because no one could observe us unexpectedly, satellite proliferation means we can be watched wherever we go.

So, it's clear we need to know what's at stake in the space domain. We need to know what we can do, how we can best utilize the capabilities that are up there. We also need to know what the enemy can do, and how they will use their satellites to their own advantage, or how they can turn our dependence on space into a disadvantage. More than ever, we need space expertise in order to effectively operate in and through the space domain.

The Navy Space Cadre has this expertise. Navy Space Cadre personnel have the knowledge and skills that will enable us to maintain the tactical and operational advantages we enjoy through space. There are two branches of the Navy Space Cadre Officer corps: Space Acquisitions professionals and Space Operations professionals.

Space Acquisitions accounts for 40 percent of the Space Cadre officer billets in the Navy. These officers are embedded in Navy and National satellite engineering offices, performing a variety of functions from requirements development, to satellite construction, to testing, launch and on-orbit evaluation. They work alongside government and contract engineers who prepare satellites for their missions in space. Most importantly, they ensure that the satellites built and launched with taxpayer dollars provide the maximum benefit to all the services, including the unique requirements of the Navy. Without Navy Space Acquisitions professionals, satellite designers would not be able to build systems that can integrate with Navy surface and air systems.

The other 60 percent of the Space Cadre is aligned to Space Operations, which encompasses anything our military does to employ satellites for military missions. Navy Space Operations professionals combine their experience of traditional Navy missions

with extensive knowledge of space capabilities.

While it's impossible to describe all of Navy Space Operations in a few pages, here are a few of the major categories: Satellite Operations, Joint Space Operations, Afloat Space Operations and Space Requirements Analysis.

Satellite Operations

The Navy has operated a wide array of satellites over the past 60 years, necessitated by the Navy's unique requirements for beyond-line-of-sight communications, over-the-horizon surveillance, and precision navigation. This traditional mission continues at the Naval Satellite Operations Center (NAVSOC) at Point Mugu, CA. As USSTRATCOM -- designated Satellite Control Authority, NAVSOC is responsible for the safe operation of these satellite constellations, which provide essential narrowband communications to tactical forces around the world. **(For more about what NAVSOC does, see LCDR Arvizo's story on Page 13).**

Joint Space Operations

The Air Force performs the bulk of the work needed to support military space missions, but all space assets must be shared jointly by all the services. For this reason, a contingent of Navy Space Cadre officers is embedded in the Joint Space Operations Center (JSpOC) at Vandenberg Air Force Base, where they provide situational awareness to satellite operators and military commanders on what's "going on" above the earth. They also serve as the clearinghouse for Joint Force Commanders to request space support based on current operational requirements. When the Navy has a particular need for space capabilities, the Navy contingent at JSpOC understands the unique requirements of the mission.

Afloat Space Operations

Navy Space Operations officers provide insight into Navy mission planning and execution, ensuring that afloat commanders understand the advantages and disadvantages of working with space-based resources. They evaluate tactical and operational plans and point out vulnerabilities that must be mitigated; they generate requests for information (RFIs) and request space support when necessary to ensure commanders make decisions based on the best possible information. With highly specialized training and knowledge, a Navy Space Operations officer knows where to go to maintain the Navy's advantage in space.

Space Requirements Analysis

Navy Space Cadre Officers abound in Navy and Joint Service functional staffs including OPNAV, Strategic Command, Navy Cyber Forces and Fleet Cyber Command. Here, they translate Navy and Joint capability gaps into actionable solutions that can be provided by satellites currently on-orbit, or more long-range solutions that will drive the performance of the next generation of military spacecraft. These more senior Space Cadre officers also produce the overarching Navy and Joint policies that drive space readiness, manpower, and training. They look years down the road to anticipate what the future of the Navy, and of space, will be like.

Being a part of the Space Cadre means specializing in complex topics like physics, engineering, technology and the electromagnetic spectrum—all of which have unique characteristics when it comes to space. The Space Cadre member at a particular command or on a particular planning team brings insight that will not be afforded by anyone else. As important as space is to the Navy, so important is this expertise. Now that space is an essential part of naval operations, we can't afford to take it for granted. ✂



Naval Satellite Operations Center

Underway With The Fleet,
Supporting the Joint Warfighter

By LCDR Adrian Arvizo, NAVSOC

Realizing that many of the satellites operated by NAVSOC have been on-orbit well beyond their design life, and that geosynchronous orbit is increasingly congested, careful maintenance and monitoring is required. NAVSOC's team must be prepared to take immediate action if a problem occurs to ensure a satellite does not become stranded on-orbit, posing a danger to other geosynchronous satellites as they drift. For this reason, the NAVSOC team takes every precaution to maneuver dying satellites out of their geosynchronous orbit before it is too late. This process of decommissioning a satellite is known as "super-syncing"; an example which occurred with UFO-5, when it suffered a major anomaly in October 2012.

Previously, UFO-5 (launched in May 1995) provided UHF and EHF satellite communications to Joint warfighters in the NORTHCOM and SOUTHCOM areas of responsibility. The on-orbit anomaly caused a loss of command and control, and forced NAVSOC to attempt an immediate recovery. Luckily, the NAVSOC team was able to recover and regain control of the satellite in a timely manner, however it could no longer be considered reliable. This failure mandated "super-sync" of the satellite, in order to prevent stranding it on-orbit. Upon obtaining concurrence/approval from the Joint Functional Component Commander for Space (JFCC-Space), Fleet Cyber Command / Commander TENTH Fleet (FCC/C10F), U.S. Army Space and Missile Defense Command / Army Forces Strategic Command (USASMDC/ARSTRAT), and Naval Network Warfare Command (NNWC), NAVSOC rapidly executed the "super-sync" operation.

The first "super sync" step was turning off the UHF and EHF payloads. Thrusters were then fired to increase the orbit beyond geosynchronous orbit into a "graveyard" orbit. Lastly, upon arrival in the "graveyard" orbit, the remaining propellant was expelled from the spacecraft, and all systems were turned off. With UFO-5 safely out of geosynchronous orbit, NAVSOC relocated another satellite into the same location, continuing to provide critical satellite communications to NORTHCOM and SOUTHCOM users. ✎



Marines Look to Space During NSOC Training

By Cpl. Lena Wakayama, Okinawa Marine Staff

CAMP KINSER, Okinawa, Japan

— U.S. service members participated in the Naval Space Operations Course (NSOC) supported by Navy Cyber Forces (NAVCYBERFOR) and Naval Network Warfare (NAVNETWARCOM) instructors Jan. 27-29 at Camp Kinser.

The term space refers to the expanse beyond the earth's atmosphere and the capabilities that exist through satellites that orbit the planet.

"The intent of the course is to raise the overall awareness of the range of space capabilities that exists to support warfighters," said John Herron, one of two NAVNETWARCOM NSOC instructors. "It improves their use of those space capabilities and their understanding of potential vulnerabilities."

The students in the course came from a variety of military occupational specialties from all four services and had little knowledge on the topics of space operations, space research and development.

"The main thing the class (entails) is baseline knowledge as far as the fundamentals of how space works," said Marine Capt. Andy Novario, the other NAVNETWARCOM NSOC instructor. "Essentially this course is meant to form a baseline of knowledge because the Marine Corps is in the early stages of understanding of how space can help the warfighter."

NSOC is a three-day course and is unique in the Department of Defense, according to Navy LT Jeff Covington, an instructor from NAVCYBERFOR's N82. Covington went on to explain that the mobile course allows the training team to teach about space operations to service members who may not be able to travel back to the U.S.

"We are willing to travel around, which makes it easier, especially here in the (Pacific Command area of operations)," said Novario. "We made it so that we have three or four

... continued on Page 14



... continued from Page 13

instructors that travel out here, which is much more cost efficient than sending 20 people back to the States.”

The course was created for Navy Carrier Strike Groups, but there is a Marine on staff and a section in the handbook dedicated to Marine operations, according to Maj. Brian C. Anderson, the III Marine Expeditionary Force space operations officer.

“We talked about tailoring to Marine operations because not everything we do (involves naval warfare),” said Anderson. “Communications are a big deal to command and control the forces during an amphibious operation. Going from ships to objectives gives us unique problems.”

The course also covered other topics that can affect space communication capabilities in relation to the students’ needs.

“We tailor the course to the interest or concerns of the students,” said Herron. “We’re constantly updating all of the presentations that we use.”

This evolution of the course included a practical application exercise in the afternoon of the final day, allowing the students to apply the knowledge they learned during the course to a planning scenario.

“When they’re doing a normal planning scenario, they can see where they have been leaving things out,”

said Herron. “They can see what (they) should be considering, what they hadn’t thought of, and how that will change the scenario and their plan.”

The continued Marine Corps involvement with NAVCYBERFOR and NAVNETWARCOM is very important to the future success of this program, according to Anderson.

“There is a space (Marine Air-Ground Task Force) and a Space Plans Branch at Headquarters Marine Corps,” said Anderson. “It’s a long-term goal to have them continue to influence the course. That way, when the Marine

“Essentially this course is meant to form a baseline of knowledge because the Marine Corps is in the early stages of understanding of how space can help the warfighter.”

Corps requests it, it’s not just Navy Cyber and Naval Network Warfare funding it. There is a service driven.”

component to it that is According to Logan Maynard, another instructor from NAVCYBERFOR’s Colorado Det., the training with the Okinawa Marines was one of the most involved group of students that he has seen as a NSOC Instructor. Covington echoed Maynard’s feelings about the Marines.

“Normally courses are focused on informing the Fleet that space is more than just a transport layer for satellite communications, as that is what most of the Navy sees as it as,” said Covington.

“The Marines have a different take



on it. They seemed to have more of an understanding that space capabilities are game changers when it comes to planning operations.”

After the course, the four NSOC instructors stayed on island as subject matter experts for a planning event that the Marines held to make sure

they understood the capabilities and vulnerabilities they had just been taught.

“Overall, I believe it was a rewarding experience for both the instructors as well as the Marines, Navy, Army and Air Force students that were able to attend the course,” concluded Covington.

Photo Illustration by Michael J. Morris



Navy Process Reference Model

The Navy's "Lego® Building Set" for IT

By LCDR James L. Fisher, FCC/10th Fleet

Everyone is undoubtedly familiar with the Lego toy dynasty, either through personal experience, through the eyes of the millions of children who regularly leave them on the floor for you to step on (in the middle of the night), or on the big screen with the recent release of *The Lego® Movie* to theaters in February.

You should recall that Legos consist of colorful interlocking plastic bricks and an accompanying array of gears, mini-figures and various other parts that can be assembled and connected in a million ways to construct such objects as vehicles, airplanes, buildings, and even working robots.

While definitely not as colorful, the Navy Process Reference Model (NPRM) has been developed by the Navy IT Service Management Office (ITSMO) to assist commands in the "construction" of their IT services with interlocking processes that support measurable quality targets and requirements.

The achievement of quality IT service is a product of measureable and repeatable processes that underpin end-to-end service delivery to the customer. Just like the plumbing that brings water into your home: you're not really concerned with any of the technical infrastructure, pressurization, and desalinization or purification technology behind the wall or in the ground. What you're after is water on demand – whenever you open the tap.

You're not buying a pipeline, a meter, a pumping station timeshare, or any of the parts in the water infrastructure. You're buying a complete end-to-end service – water in exchange for a set fee per gallon. It's up to the specialists who offer the water contract to deliver as promised so that you can use the water as you need it, when you need it and in the amount you need it. Operationally speaking, that's Command and

Control, better known as C2.

The Information Technology Infrastructure Library (ITIL) was developed by the UK Office of Government Commerce (OGC) to codify the processes defined for IT that were being performed by the vast majority of global organizations who built end-to-end IT service delivery models with them. The OGC looked at the best of these processes and developed the ITIL Lifecycle to give a "Lego® Building Set" of best practices to IT organizations. These interlocking IT processes perform specific activities and tasks in a predictable and repeatable way by taking the input provided specifically for that process and producing and delivering their work

“... in this business, we need to be able to talk to how those processes we're working on now for the Enterprise Service Management are core to the (IT) capability just as (they are) for nuclear warfighting capability.”

RDML Diane E. H. Webber

products to other processes in turn.

Since ITIL is a framework, that is, it is a nominal set of processes considered to be necessary for all IT organizations, and is not prescriptive, the Navy ITSMO leveraged ITIL and added processes and components from ISO/IEC-20000, COBIT and others, to produce the NPRM. The NPRM contains 34 interlocking IT processes – everything from Access Management to Workforce Management – that define inputs, outputs, controls, roles, responsibilities, and tool and skill recommendations. The processes are grouped according to the ITIL Lifecycle Phase they are most closely associated with: Strategy, Design, Transition or Operations (although Continual Service Improvement (CSI) is also a distinct ITIL Lifecycle Phase, the NPRM incorporates CSI principles within each process and

does not treat CSI separately). A chief distinction of the NPRM is the incorporation of the COBIT-5 Governance model which emphasizes the Evaluate, Direct, and Monitor (EDM) activities necessary for Government oversight and control of its own, or vendor-managed infrastructure.

The NPRM version 1 was published in 2013, and is now undergoing a yearly review to ensure it remains current with international standards and industry best practice guidelines. Since its publication, the NPRM has provided a solid foundation upon which Navy Organizations can construct or improve IT infrastructure and enterprise management... but something was missing.

Enter the Process Capability Assessment Model and Tool (PCAT). While the NPRM provides the 'building block' processes that support the construction of IT services, the PCAT helps organizations objectively quantify the quality of their process performance, and by extension, the quality of their service delivery. A few axioms are applicable here: "You get what you inspect, not what you expect" and "If you can measure it, you can manage it." There are many more, but these two management maxims drive home the point: if you don't measure the quality of your processes and services, you don't really know if you're actually delivering what the customer expects.

At the June 2013 Defense Enterprise Service Management Consortium, RDML Diane E.H. Webber, then Deputy Commander Fleet Cyber Command, spoke to the need for "nuclear-like accountability" in the design, operation and improvement of Enterprise IT and noted that . . .¹

The Admiral's remarks emphasized how, from 1942 on, ADM Hyman Rickover, widely acclaimed father of

... continued on Page 16



... continued from Page 15

the nuclear Navy, viewed the entire nuclear program; not as individual pieces of capability (design, implementation, training, operation, sustainment, et al), but as a complete strategic asset that delivered warfighting capability and demanded “zero-defects” through a holistic inspection, training, certification and review continuum² – a record that stands to this day.

While admittedly not “nuclear-like” in its rigor (at least not yet), the PCAT nonetheless fosters an enterprise approach to IT service quality, taking a holistic view of process capability and performance through five lenses: Performed, Managed, Established, Predictable and Optimized. The model provides the assessment criteria – the tool provides an ability to capture process performance metrics and assess capability against the five dimensions (levels) of capability using a Microsoft Excel spreadsheet that automatically calculates assessment input and provides a graphic depiction of capability. If the NPRM can be likened to a Lego building set, the PCAT is almost certainly the tachometer strapped to the Formula-1 racing car you built with it.

Together, the NPRM and PCAT are a powerful combination available to IT Service Management (ITSM) stakeholders who desire to apply proven best practice framework design into their enterprise, with the added benefit of Continuous Performance Improvement (CPI) tooling that gives them an objective performance ‘snapshot’, gap identification, and a way forward for improvement.

The NPRM is available for download on the ITSMO portal at <https://usff.portal.navy.mil/sites/fcc-c10f/cio/1/ITSMO/default.aspx>.

Stakeholders can request a process-specific PCAT tool from the ITSMO through the ITSMO Service Request System: <https://usff.portal.navy.mil/sites/fccc10f/cio/1/ITSMO/Lists/ITSMOServiceRequestSystem/NewForm.aspx>

***Note:** Access to the ITSMO web portal requires a Navy Forces Online (NFO) account. Email itsmo@navy.mil for instructions on obtaining a NFO account. ✂



¹ RDML Diane E.H. Webber, June 18, 2013, Defense Enterprise Service Management Consortium, Ft. George Meade, MD., retrieved from <https://www.milsuite.mil/video/watch/newvideo/5874>

² Ibid

CID Instructor Wins 2013 NETC SOY

Story & Photo by Gary Nichols, CID Public Affairs

PENSACOLA, FL – The Naval Education Training Command (NETC) announced Dec. 12, 2013, that a Center for Information Dominance (CID) Instructor was the NETC 2013 Sailor of the Year (SOY).

CTR(IDW/AW/SW) James R. Lee Jr., an instructor at the CID Learning Site (LS) San Diego, was selected from among more than 8,000 Sailors within the NETC domain for the prestigious recognition.

Lee said that being selected as the CID SOY was a huge honor because it represented the organization that really laid down the foundation for everything he had accomplished in his naval career.

“I am extremely proud to represent the Center for Information Dominance Domain,” Lee said. “Being selected as a NETC finalist is more recognition than anyone could ever ask for.”

Lee said he was surprised and humbled that he was selected for the NETC SOY from among such a distinguished group of Sailors.

“I was shocked to be picked as the Naval Education Training Center’s Sailor of the Year, because the other nominees are all Sailors of the very highest caliber,” he said.

Lee said that throughout his naval career he had received training, mentorship and guidance from top-notch instructors, and that is what prompted him to ask for duty as a Navy instructor.

“I wanted to take the time in my career to reciprocate by providing my shipmates in the fleet the same level of training, mentorship and guidance I received,” Lee said.

One of the mentors Lee said he is most grateful to is CID LS San Diego Training Director CTTCS(IDW/SW) Mayra Kohlmann, who has been his mentor during his tour at San Diego.

“I definitely owe a lot to her,” Lee said. “The entire time I worked for Senior Chief Kohlmann she set a high standard for the work environment. I’ve learned and have grown exponentially from working with and for her this

past year, and trying to meet the standards she set for us has pushed me to be a better all-around Sailor.”

Lee is the course lead for the Maritime Cryptologic Systems of the 21st Century “C” school and the department Leading Petty Officer for the Information Warfare Department. He also is the Petty Officer Association President. While there he also earned a certification in human resources.

He was recently selected for assignment to Tactial Information Operations Support Activity One in Coronado, CA.

“The Information Dominance Corps (IDC) produces extremely well-versed, motivated and talented Sailors,” CID CMC(AW/SW) Travis P. Brummer said. “Petty Officer Lee is a great example of the remarkable Sailors we see at every level within the IDC community at the Schumacher Submarine Learning Center, TRIDENT Training Facility, Kings Bay, GA.

“I looked at these Sailors, and thought to myself, ‘Wow, I’m glad I’m not



CTR1(IDW/AW/SW) James R. Lee Jr.

competing with them,’ Brummer said. He had some very tough competition, but Petty Officer Lee definitely broke out.”

San Diego “Cyber Sites” Consolidate

By LTJG Jacqueline Humburg, FITC Public Affairs

SAN DIEGO – The Fleet Intelligence Training Command (FITC) and Center for Information Dominance Learning Site San Diego (CIDLSSD), two San Diego-based training commands for Information

Dominance-related fields, have consolidated effective Jan. 14, 2014.

The new combined command will be officially renamed the Center for Information Dominance Unit

San Diego (CIDUSD) later this year.

The consolidation of FITC and CIDLSSD is a

... continued on Page 18



Congressman Miller Praises Grads Who “Undoubtedly Saves Lives...”

By CID Unit Corry Station Public Affairs

PENSACOLA, FL – Florida Rep. Jefferson B. “Jeff” Miller attended a Joint Cyber Analysis Course (JCAC) graduation ceremony at the chapel on board Corry Station Jan. 27.

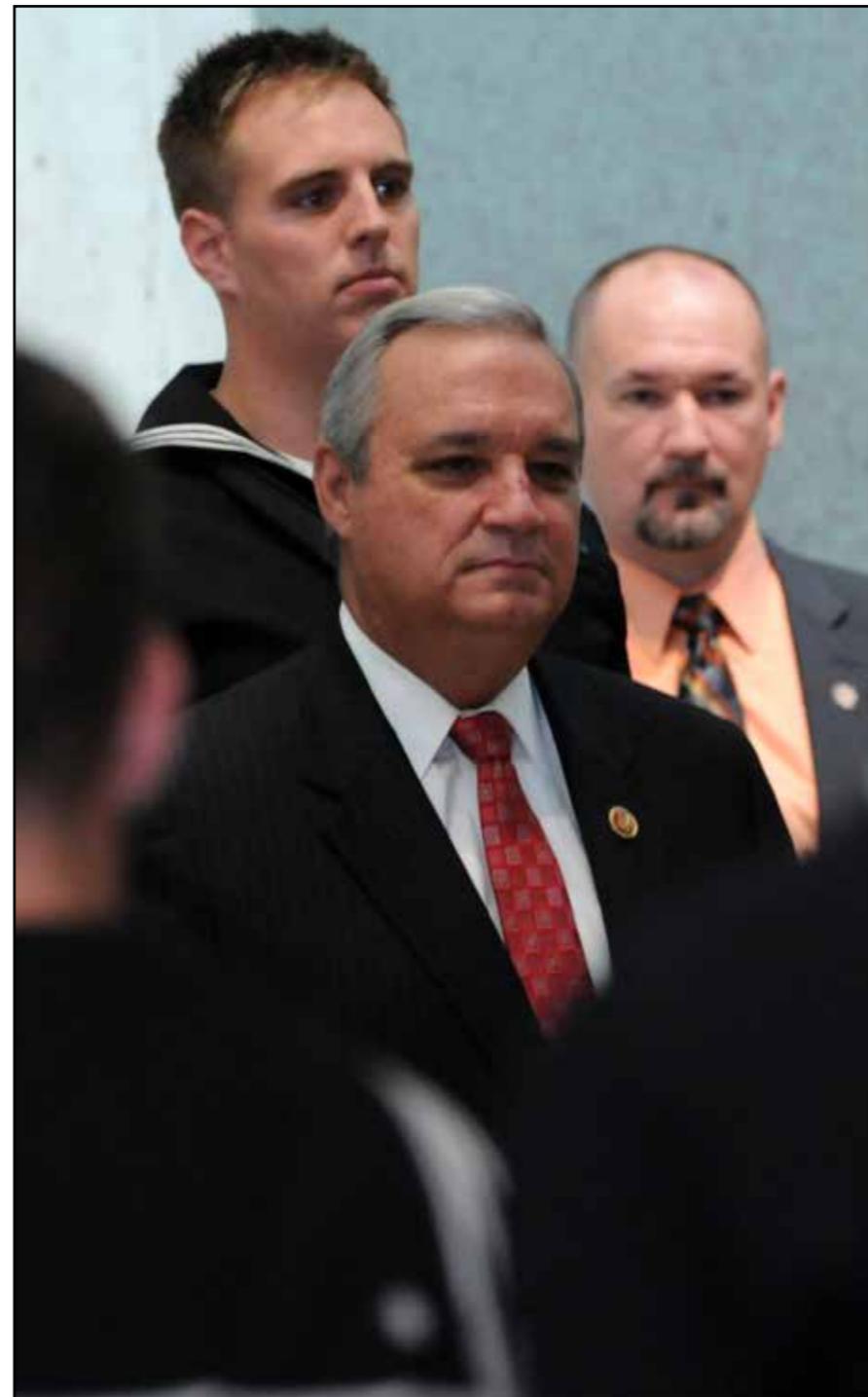
Miller, who serves as chairman of the Veterans Affairs Committee, the House of Armed Services Committee and the House Permanent Select Committee on Intelligence, congratulated 18 JCAC students for successfully completing the demanding course of instruction.

Though a familiar visitor to Corry Station, this was Miller’s first graduation. He noted how impressed he was by each graduate. He also remarked how vital the work was that each graduate would soon be undertaking to help defend the nation’s computer networks.

“You are going to spearhead the defense of this threat with the technical skills you have acquired over the last six months in this course,” Miller said. “You’re also going to help our armed forces defend their networks against our adversaries. The skill set required for this important mission does not come easily.”

The JCAC is taught at the Navy’s Center for Information Dominance (CID) Unit Corry Station. CID Unit Corry Station delivers Navy and joint forces training in information operations, information warfare, information technology and cryptology. JCAC is a program designed to take individuals who have minimal computer experience and make them proficient in cyber analysis within six months. The course, which is divided into 10 modules, covers 25 topics ranging from computer fundamentals to programing to forensics methodology and malware analysis.

... continued on Page 19



Congressman Jefferson B. Miller at the Joint Cyber Analysis Course graduation ceremony at Corry Station’s chapel on Jan. 27.

... continued from Page 17

logical outcome stemming from the Information Dominance Corps (IDC) concept, which emphasizes collaboration between the Intelligence, Information Warfare, Information Professional, Meteorology/Oceanography and Space Cadre disciplines. FITC previously focused on Intelligence training whereas the expertise of CIDLSSD lay in Information Operations and Information Technology.

“The missions of our commands have been – and will remain – to provide the best possible training to the Fleet enabling them to prevail across the full spectrum of military operations,” FITC Commanding Officer Cmdr. Miriam Smyth said. “The consolidation of these two commands is a unique opportunity to optimize the development and delivery of IDC training.”

For more information on the Fleet Intelligence Training Command, visit the FITC information page on CANTRAC: https://app.prod.cetars.training.navy.mil/cantrac/pages/rpt_vol1.html?uic=43662.



... continued from Page 18

Class Advisor, Army Sgt. 1st Class Charles Martinez, said JCAC is very challenging due to the demanding curriculum and heavy workload. “JCAC students receive 27 college credits for this course, which means they are learning more than a year of college in only six months. “Unlike most Navy training, which focuses on a Navy-specific mission, JCAC is geared toward intense joint training that focuses on a larger, national mission of protecting and defending the nation’s cyber networks.

JCAC graduates will be capable of providing computer (network and infrastructure) analysis and technical solutions to produce Computer Network Operations (CNO) effects in support of national intelligence requirements.

Citing a recent poll among defense leaders, Miller said a cyber attack is the single greatest threat to the United States today, with terrorism coming in a distant second. “Our nation depends on what you do today and what you are about to do,” he said.

Martinez said the job of the CID Unit Corry Station instructors is to help train the JCAC students to defend and protect the infrastructure of the United States.

“Defending the country’s networks is really important,” Martinez said. “For example, we don’t want someone hacking into air traffic control and making an airplane crash. That’s what we’re trying to defend against.”

Class Leader, Marine Corps Gunnery Sgt. Julianna Graham, a 13-year veteran of the Corps, said the JCAC course was tougher than she had anticipated. “It was definitely one of the more difficult courses that I have ever taken,” Graham said. “It was extremely high paced and challenging. “That sentiment was echoed by Honor Student Cryptologic Technician Networks Seaman Craig Jennings , who had an impressive final grade point average of 96.94 percent.

“It was definitely challenging and fast paced,”

Jennings said. “However, it is within reach of anyone if they are willing to study hard.”

“I believe that there is a great future here at the Center for Information Dominance Unit Corry Station,” Miller said. “We are continually turning out students who are going to all four corners of the globe and protecting Americans from our adversaries. Soldiers, Sailors, Airmen, Marines and Coast Guardsmen in the field depend on the integrated systems and networks that you are going to defend. Your performance and technical knowledge will undoubtedly save lives.”

Miller concluded his visit by personally handing out diplomas and shaking the hands of each graduate. “I’m proud of each and every one of you,” Miller said. “I’m honored that you answered your nation’s call to join the armed services and in fact are taking this very important undertaking seriously. I wish you all the best in your future endeavors and again add my congratulations on completing this very rigorous and tough course.” ✂



Congressman Miller congratulates one of 18 Joint Cyber Analysis Course (JCAC) students from CID Unit Corry Station for successfully completing a demanding six month course of instruction. (Photos by Gary Nichols)

EDITOR'S NOTE: *CID Unit Corry trains approximately 8,000 service members each year. With a staff of 300 military and civilian instructors, CID Unit Corry Station oversees the development and administration of 35 courses of instruction.*



Pathfinder Visits Guatemala as Part of OSPS

USNS PATHFINDER (T-AGS 60) visited Puerto Santo Tomas de Castilla, Guatemala on Feb. 5, as part of the U.S. Southern Command's (USSOUTHCOM) Oceanographic Southern Partnership Station. The mission was led by Giovanni Morris, Senior Naval Oceanographic Office Representative, with a crew of civilian surveyors who conduct the collection and processing of data.

Multiple activities took place during the visit, including daily tours for civilian, military and academic institutions; subject matter expert exchanges in hydrography, geodesy/tides and nautical charting; and a reception aboard PATHFINDER hosted by CAPT Marc Eckardt, Deputy Hydrographer of the Navy, representing USSOUTHCOM, Commander, U.S. 4th Fleet and Commander, Naval Meteorology and Oceanography Command. ✕



(Above) Eric Villalobos (extreme right) of the Naval Meteorology and Oceanography Command conducts a tour of USNS PATHFINDER for Guatemalan naval officers during a reception on the ship as part of Oceanographic Southern Partnership Station during the ship visit to Guatemala.

(Left) Eric Villalobos (center) of the Naval Meteorology and Oceanography Command explains the data collection and analysis system on USNS PATHFINDER for Guatemalan naval officers during a reception on the ship as part of Oceanographic Southern Partnership Station during the ship visit to Guatemala.



DeWitt Relieves Scott as Reserve Commander

CAPT Theresa DeWitt relieved CAPT Carven Scott as Commanding Officer of the Naval Meteorology and Oceanography Reserve Activity (NMORA) Headquarters Unit 0282 in a traditional change of command ceremony at Stennis Space Center, on Dec. 6, 2013.

RDML Brian Brown, commander of the Stennis-based Naval Meteorology and Oceanography Command, spoke at the ceremony.

NMORA Headquarters Unit 0282 serves as headquarters for and directs the activities of the Naval Meteorology and Oceanography reserve forces.

Scott is Chief of the Environmental and Scientific Services Division with the National Weather Service Alaska Region in his civilian job.

DeWitt serves as the Deputy Chief, Staff Resources for Human Capital and Contracts with the U.S. Joint Staff. ✂



RDML Brian Brown, NMOC Commander, congratulates CAPT Theresa DeWitt, CO of NMORA Headquarters Unit 0282, on assuming command. Looking on is CAPT Carven Scott, outgoing CO of NMORA.



The newest class of Naval Oceanography officers are: (front row, l-r) LTJG Natasha Reid, ENS Megan Ryan, ENS Michelle Weaver, ENS Shunika Hamilton, (second row, l-r) ENS Raymond Landato, LT Matthew Geistfeld, ENS Erin Harvanek, ENS Christopher Wilson, ENS Ted Jacobs, LTJG William Zinicola.



STENNIS SPACE CENTER, MS -- AG2 Dustin Brashears briefs Master Chief Petty Officer of the Navy (MCPON) Mike Stevens on unmanned underwater vehicles used in mine warfare operations during Stevens' visit to the Naval Oceanography assets at Stennis Space Center on Dec. 10, 2013. Brashears is a Sailor with the Naval Oceanography Mine Warfare Center.





Dr. Bill Burnett (r), Deputy/Technical Director of the Naval Meteorology and Oceanography Command (NAVMETOCOM), welcomes (r-l) Dr. Ellen Stofan, National Aeronautics and Space Administration (NASA) Chief Scientist; Dr. Gale Allen, NASA Deputy Chief Scientist; and Duane Armstrong, NASA Stennis Space Center Chief of Applied Science; to the Naval Oceanographic Office (NAVOCEANO) at Stennis Space Center. NAVOCEANO is a subordinate command of NAVMETOCOM, also based at Stennis.

Naval Oceanography's SOYs

Senior and Junior Sailors of the Year were named for the Naval Oceanography commands at Stennis Space Center. Pictured Right to Left are:

AG1 Lisa Sherry, NAVOCEANASWCEN's Senior Shore SOY

AG1 Brittney Waddell, NAVOCEANO's Senior Shore SOY

AG1 Brandon Husted, NAVOCEANMIWCEN's Senior Shore SOY

AG1 Kirk Hying, NAVOCEANASWCEN's Sea SOY

LS1 Alejandro Ozornio, FLTSURVTEAM's Sea SOY

AG2 Elizabeth Tran, NAVOCEANMIWCEN's Junior SOY

IT3 Dominic Ellis, NAVOCEANO's Junior SOY

AG2 Corey Brigner, FLTSURVTEAM's Junior SOY

AGAA Jason E. Moore, NAVOCEANMIWCEN's Blue Jacket of the Year.

(Not pictured - AG2 Bradley Wendeln, NAVOCEANASWCEN's Junior SOY)

Senior Sailors received the Navy and Marine Corps Achievement Medal. Junior Sailors received a Flag Letter of Commendation. 🏆



CIO's Network Tips



DO NOT BE THE WEAKEST LINK . . .

By Carlos Parter, Fleet Cyber Command

Throughout the year, these Network and Cyber Security Tips series addressed real world issues and topics that we face, day in and day out. Of all the topics presented, one theme resonated throughout; you, the end user, are the first line of defense for protecting the Navy's networks, the information exchanged on them and our shared mission.

Good user behavior can help protect our networks from unauthorized access and malicious coding. Bad user behavior, whether caused by malicious intent, carelessness or lack of effective training, can help the adversaries find a way into our networks and open the door to unauthorized access to critical data. Not only must we govern ourselves, but it is paramount to be alert and aware of the security related actions of those around us in the workplace.

If we are going to stay ahead in this cyber warfare, we must be vigilant, focused and undeterred to report to appropriate personnel when you see something wrong or out of place. Just like in football, the best defense is an even better offense. So, go on the offensive and take control of your part of our shared cyber landscape. Do a self-assessment of your user behavior. Where there are deficiencies, find the tools to correct them. No matter how many times it is stated or how you package the idea, the bottom line is the Navy needs you to take on a level of greater personal accountability.

Would you leave the doors of your home open at night? Would you leave your credit card access number, bank account access numbers, online banking passwords, etc. in the open for easy access by unauthorized users? How important is the security of our nation? With this in mind, wouldn't you want to ensure you are doing your part in protecting our vital

information? Lax security could cause grave damage to our national security. Taking personal ownership in information security is not just a good idea, but it is your duty to your nation, your family and your co-workers.

In the last year's series of Information Domain articles, the following topics were discussed: electronic spillage, records management and malicious code. Each topic concluded with a reference to the Navy Network

“Network man says: the human element is our first line of defense; you can be our strongest or weakest link.”

Discipline Navy Telecommunications Directive (NTD) as a checklist for ways users could effectively monitor their personal behavior and best contribute to the security posture of our networks and protection of the Department of Defense's classified information.

Another important piece of documentation is the System Authorization Access Request Navy (SAAR-N), OPNAV 5239/14 (Rev 9/2011). Where the Navy Network Discipline NTD provides guidelines for user behavior, the SAAR-N provides a legalistic approach to what expectations are placed on the end user when granted access to the Navy's information system resources.

Highlights from 2013

According to the Symantec Internet Security Threat Report released in April 2013, the following 2012

highlights are provided:

- 42 percent increase of targeted attacks
- 5,291 new vulnerabilities
- 604,826 average number of identifies exposed per breach
- 30 billion estimated global email Spam per day
- 23 percent of malware attacks via email used a link to a web page (13 percent decrease from 2011)
- 58 percent increase in mobile malware attacks

Top 5 Industries attacked:

- Manufacturing – 24 percent
- Finance, Insurance & Real Estate – 19 percent
- Services – Non-Traditional – 17 percent
- Government – 12 percent
- Energy/Utilities – 10 percent

The 2013 report will be released spring 2014.

. . . continued on Page 24



... continued from Page 23

According to Verizon's 2013 Data Breach Investigations Report (available at <http://www.verizonenterprise.com/DBIR/2013/>), in 2012 there were over 47,000 security incidents reported world-wide (not counting Russia or China, which did not participate). Of the 47,000, there were 621 confirmed data disclosures and at least 44 million compromised records.

From a September 2013 Lowell Sun report, the Lowell Housing Authority (LHA) could be forced to repay the federal government more than \$11.4 million because of deficiencies discovered during a federal audit with regards to its handling of major renovation projects and improper procurement procedures. The executive director of LHA described the problem as poor record keeping and pledged the LHA would spend the next two-to-six months working to produce the documentation to justify the use of force-account labor. This report highlights the importance of good records management. Due to poor records management, LHA risked losing \$11.4 million in federal support, lost \$272, 598 in potential revenue, and had \$52, 212 of unsupported over-costs. Poor records management could carry a high price tag.

Malicious Code

We, as users, should not take security of our networks lightly. When you receive an email from a known or unknown source, you should be careful before opening any attachments; consider the risks. Not only should you be careful to scan external media at work but you should be doing the same at home. Malicious codes are an infestation that can be controlled as long as the users maintain proper user discipline when using both DoD networks and commercial networks. Protecting your personal data is as important as protecting the data you are entrusted with in the work place.

Records Management (RM)

An office with files scattered and stacked on top of file cabinets and in boxes, creates an inefficient working environment. The same applies to electronic records. One of the key issues caused by improper RM, relates to

cost. For example, the available storage space is limited; therefore, command history files could be inadvertently deleted or difficult to locate. Acquiring additional storage space is a temporary solution that eventually becomes cost prohibitive. Dependent on the number of users, a command may require anywhere from 100 gigabytes to a terabyte of share drive space.

Electronic Spill

Data spillages are unacceptable. They pose a risk to vital trade secrets in the business world, and in the Navy networks, they equate to a loss of control of classified information. Data spillages can degrade operational readiness and negatively impact national security. They are most often caused by human error, which shows a lack of information security discipline.

“Stay safe and remember, protecting our networks and information is dependent on each of us making the right decisions!”

User Discipline

Good user discipline on the network is an “all hands” responsibility. Simple disciplinary action, without consideration of what other factors may have contributed to the situation, is not considered an acceptable response to a security incident. Maintaining a high level of security awareness at all levels in the chain of command is a must. Information security discipline is reinforced when commands complete annual security and information assurance awareness training. It is imperative that we use this annual training time to refresh our minds and re-adjust our focus on information security. Additionally, the following statements are included on page three of the SAAR-N that all Navy network users sign:

I understand that to ensure the confidentiality, integrity, availability and security of Navy Information

Technology (IT) resources and information, when using those resources, I shall:

- Safeguard information and information systems from unauthorized or inadvertent modification, disclosure, destruction, or misuse.
- Protect Controlled Unclassified Information (CUI), to include Personally Identifiable Information (PII) and classified information to prevent unauthorized access, compromise, tampering, or exploitation of the information.
- Protect authenticators (e.g., Password and Personal Identification Numbers (PIN)) required for logon authentication at the same classification as the highest classification of the information accessed.
- Protect authentication tokens (e.g., Common Access Card (CAC), Alternate Logon Token (ALT), Personal Identity Verification (PIV) and National Security Systems ((NSS) tokens, etc.) at all times. Authentication tokens shall not be left unattended at any time unless properly secured.
- Virus-check all information, programs and other files prior to uploading onto any Navy IT resource.
- Report all security incidents including PII breaches immediately in accordance with applicable procedures.
- Access only that data, control information, software, hardware, and firmware for which I am authorized access by the cognizant Department of the Navy (DON) Commanding Officer, and have a need-to-know, have the appropriate security clearance. Assume only those roles and privileges for which I am authorized.
- Observe all policies and procedures governing the secure operation and authorized use of a Navy information system.
- Digitally sign and encrypt e-mail in accordance with current policies.

... continued on Page 25



... continued from Page 24

- Employ sound operations security measures in accordance with DOD, DON, service and command directives.

The bottom line is that most vulnerabilities to our networks are largely preventable. The value and importance of proper discipline and user behavior cannot be over emphasized.

The following guidelines (along with adhering to the SAAR-N user agreement), found in the Fleet Cyber Command "Navy Network Discipline Quick Tips User Guide," should assist in minimizing the risk of to our networks:

- Safeguard Information and Information Systems from unauthorized or inadvertent modification, disclosure, destruction or misuse. Protect Controlled Unclassified Information (CUI), Personally Identifiable Information (PII), and classified information to prevent unauthorized access, compromise, tampering or exploitation of the information
- Report all security incidents, including PII breaches, to your Command Information Assurance Manager (IAM) immediately in accordance with applicable procedures
- Access ONLY the data, controlled information, software, hardware, and firmware for which you are authorized access, have a need-to-know, and have the appropriate security clearance. Assume only those roles and privileges for which you are authorized
- Employ sound operations security measures IAW DOD, DON, Navy and Command directives. ✂



**“Do not
be the
weakest
link!”**

Cyber Student Honored With Mayo Award

Story & Photo by Amanda D. Stein

NPS Cyber Systems and Operations student LT Jason Hughes has been presented with the VADM Richard W. Mayo Award. The Mayo Award, named for the first commander of the Naval Network Warfare Command, is presented annually to an Information Professional (IP) junior officer who demonstrates vision, innovation and exceptional performance in information technology (IT) and operational command, control, communications and computers (C4).

“LT Hughes was selected for the award over his peers in the Information Professional community worldwide,” said NPS Senior Intelligence Officer CAPT Jennith Hoyt after formally presenting Hughes with his certificate. “This shows what an exceptional officer LT Hughes is, and I know he will continue to be an instrumental leader in the Information Dominance community and the Navy.”

Hughes joined the Navy more than 18 years ago, and started as a Fire Control Technician, but says he spent most of his Navy career in positions some way related to information technology and C4, including teaching IT “C” Schools.

For Hughes, continuing education has been a personal commitment, having dedicated free time during his 2010 commissioned tour to earning an academic certificate in Information Systems Technology through NPS’ distance learning program.

When the chance presented itself for Hughes to attend NPS full-time for his master’s degree, he jumped at the opportunity. Although only one month into his studies at NPS, Hughes says he looks forward to bringing his unique experiences in IT and C4 to the cyber conversation.

“You look across, not just military, but federal government as well, and no one really has the

clear direction for how we proceed in cyber,” said Hughes. “That means it’s important for leadership to bring people together with diverse opinions and backgrounds to work to develop these solutions.

“I think you’re going to find a lot of people who bring different things to the table. And some people who turn out to be true leaders and visionaries in cyber, may not even have a background in cyber. And that’s what’s interesting about the Information Professional Community,” he added.

“You’ve got people of quite diverse backgrounds all coming into this community, and they all bring interesting strengths and different ways of looking at things.” ✂

EDITOR’S NOTE: *Guidance for the VADM Richard C. Mayo CY13 nominations is provided in NAVMSG DTG 081127ZAPR14.*

(Below) NPS Cyber Systems and Operations student LT Jason Hughes, left, is presented with the VADM Richard W. Mayo Award by CAPT Jennith Hoyt, NPS senior intelligence officer. (Official U.S. Navy Photo)



Full Steam Ahead for Next-Generation Shipboard Network in '14

By George I. Seffers, SIGNAL magazine staff

U.S. Navy officials expect to award a full-deployment contract for a new shipboard network this spring, and they plan to install the system on nine ships this year. The network provides commonality across the fleet, replacing multiple aging networks, improving interoperability and driving down costs. The Common Afloat Networks and Enterprise Services (CANES) program represents a new business model for delivering capability to the fleet, Navy officials say. The program consolidates five legacy networks into one, which enhances operational effectiveness and provides better quality of life for deployed sailors. The approach allows the fleet to streamline logistics support, training and operating procedures. Additionally, CANES offers a common computing environment with continual hardware and software upgrades. Navy officials expect to update software every two years and hardware every four years. Furthermore, minor insertions will be executed on four-year cycles and major insertions on eight-year cycles to reduce obsolescence.

Dave Wegmann, director of maritime command and control within Northrop Grumman's Information Systems

sector, headquartered in McLean, VA, acknowledges that 2014 is a big year for the program. "This is a very important year for CANES with all the ship sets that we'll be delivering. The Navy's got its at-sea operational evaluation scheduled for this year. That's an important milestone leading up to the program's full-deployment decision, so it's a very important year," Wegmann says.

CANES also reduces known cybersecurity vulnerabilities, Navy and industry officials say. For example, the regularly scheduled technology refresh cycle enables the fleet to better keep up with security threats. Wegmann lists three additional ways it improves the Navy's cybersecurity posture.

"Go back to the concept of CANES reducing the number of individual legacy networks into a more modern, robust, single system. Just the technical fact of combining these historically stovepiped systems into a more modern architecture by itself helps to improve the security posture. You've got that benefit right off the bat," Wegmann maintains. "We're also fielding the most modern commercial off-the-shelf products. So, you've got an upgrade in your security posture right there. Also,

you've got this single CANES system that is common and scalable across all the different ship classes. The security features are common, so the crew training and their understanding of the cyber capabilities of the ship will increase over time."

Additionally, network standardization eliminates up to 642 known legacy configurations, according to information provided by the Navy's Space and Naval Warfare Systems Command public affairs office. CANES also allows the Navy to better meet rapidly changing warfighter requirements and it improves data, transport, voice and video services and systems management.

And the system allows efficient insertion of next-generation command and control, intelligence, surveillance and reconnaissance capabilities. "The future of maritime command and



Forward deployed in Yokosuka, Japan, the USS McCampbell was the first ship to complete the CANES installation process in November 2012.

Official U.S. Navy Photo

control becomes enabled by software updates and upgrades versus having to go physically onto the ship and install more hardware. In that respect, it's going to speed up the fielding of new mission capabilities and also save costs," Wegmann contends.

Last November, the Navy completed installation of CANES on the USS MCCAMPBELL, the first ship to complete the process. The ship is forward deployed in Yokosuka, Japan. The MCCAMPBELL conducted sea trials in early October 2013 to validate how CANES would function

... continued on Page 27



... continued from Page 26

in an operational environment and received positive feedback, Navy officials say. The Navy's first installation of CANES aboard the Arleigh Burke-class guided missile destroyer USS MILIUS began in December 2012. Installation is ongoing at various stages aboard eight guided missile destroyers, two carriers and one amphibious assault ship.

"The whole purpose of the CANES program is to consolidate these legacy programs and to create a common, modernized and robust computing environment to run the many applications for the ships' missions," Wegmann maintains.

"CANES is really a step forward on a local area

network afloat that merges those domains in the local area network infrastructure. One substantiation of that would be a converged C2ISR common operating picture, so operators are looking at a screen and can see both kinds of data with a point and click," emphasized Wegmann. ✂

NIOC Georgia Wardroom Makes a Difference by Serving Meals

By CTT3 Robert A. Hartland, NIOC Georgia Public Affairs

AUGUSTA, GA -- Officers from Navy Information Operations Command Georgia (NIOC GA) served meals to the hungry Jan. 4, 2014, during a volunteer service event in Augusta, GA.

The NIOC GA Wardroom and Golden Harvest Food Bank, a non-profit, charitable organization that operates the Master's Table Soup Kitchen, organized the volunteer effort.

"Without groups volunteering it would probably be impossible to serve all of the people who pass through the kitchen each and every day," said Daniel Saucier, chef of Master's Table Soup Kitchen.

At the Master's Table facility there are usually 300 people seeking meals daily. The soup kitchen is open 365 days a year and it takes more than 30 volunteers per day to operate.

"Almost every day there are groups such as the NIOC GA Wardroom or individuals who come and work at the kitchen," Saucier said.

Volunteers help prepare and serve the meals, greet guests and take on special tasks.

The majority of guests at Master's Table are not homeless. Whether from losing a job or struggling with medical bills, the truth is that most guests simply cannot afford to pay for food, according to Saucier.

"After seeking out an opportunity to help those hungry within our own community, I reviewed a list of



available volunteer opportunities that fall under the umbrella of Golden Harvest Food Bank," said LCDR Scott Brown who led the organizational effort for NIOC GA.

"We then offered the invitation to volunteer to other military members we work with and some of our family members," said Brown. "We hope to continue with helping to feed the hungry within our community in the future."

No matter who walks through the doors, every guest has a unique story to tell. For this reason, Master's Table encourages all its volunteers and visitors to sit down with a guest for a few minutes to listen.

"Serving a simple meal gives a hungry person hope that they can make it through another day," said Brown.

"Giving back to those who can't provide for themselves or for their family by serving them a meal helps all our volunteers see that with each plate served, it does make a difference," Brown went on to say.

In the past 31 years the program has grown to a 6,200 square foot facility with an organic community garden and indoor seating for 152 guests. ✂





Sailor Aides in Auto Accident Rescue

IS2 Justin L. Mickelson, a Maritime Domain Awareness Analyst assigned to the Fleet Intelligence Adaptive Force in San Diego was recently driving on Rosecrans Avenue, heading towards Naval Base Point Loma, San Diego, when he witnessed a single cab white pickup get hit by an SUV and roll over in the opposite lane.

The truck came to a stop on its driver's side pinning the driver in the vehicle. Mickelson stopped his car in the left hand turn lane, got out and ran over to the rolled over truck. He asked the driver if he was hurt and he told Mickelson his arm was really hurting but that was it.

At this point the truck began to smoke from the engine, and two other males and Mickelson couldn't roll the truck back over. However, the young Sailor was able to get the other two males to help him pop the jammed shut passenger side door loose on the truck.

When they finally got the door to open, the 22-year-old Mickelson hopped up on the truck along with a second male and they pulled the injured man out of the vehicle and carried him over to the sidewalk where they sat him down and tried to keep him calm. Ladies from a nearby nail salon brought the injured man some water and paper towels to help try and stop the bleeding from his arm and hand. About two minutes after the rollover had happened police and ambulances showed up, at that point the Stanwood, WA native asked the police if they needed anything else and headed off to stand his watch.

"I guess my hope is that someone would do the same for me if I was ever in that same situation," said Mickelson. ✂



IS2 Justin L. Mickelson

Official U.S. Navy Photo

PENSACOLA, FL -- (Left) Chief petty officers from the Center for Information Dominance (CID) Headquarters on board Corry Station hoist the national ensign during morning colors on April 1, to commemorate the 121st birthday of the Chief Petty Officer. 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. (Photo by Gary Nichols)





Co-Sponsors Recognize FCC/10th Fleet Members

From Commander, Fleet Cyber Command / 10th Fleet Public Affairs

FORT MEADE, MD -- Three U.S. Fleet Cyber Command/U.S. 10th Fleet (FCC/C10F) members were selected as recipients of the Copernicus award, which is presented annually to Sailors, Marines, Coast Guardsmen, and civilians who excel in Command, Control, Communications and Computers (C4I) and information technology jobs.

The award is co-sponsored by Armed Forces Communications and Electronics Association (AFCEA) International and the U.S. Naval Institute (USNI).

C10F winners are LT Ryan N. Haag, NIOC, Georgia; CTR1(IDW/NAC) Matthew James Strauss, NIOC Whidbey Island; and LCDR Gilbert A. Yarbrough, NCTS Station, Bahrain.

The Copernicus award was established in 1997,

named for the Copernicus Architecture that was used as the blueprint for the future C4I structure of the Navy, according to AFCEA.

You can view the C10F and all 2013 Copernicus Award winners' citations (for actions performed during FY 12) at AFCEA's award website: <http://www.afcea.org/awards/copernicusaward.htm>.

FCC is an Echelon II command reporting to the Chief of Naval Operations for administrative and service related matters. It serves as the (1) Navy Component Command to U.S. Strategic Command and U.S. Cyber Command, providing operational employment of the Navy's cyber, network operations, information operations, cryptologic, and space forces and (2) Navy's Service Cryptologic Component commander to

the National Security Agency/Central Security Service.

C10F is the operational arm of FCC and executes its mission set through the same maritime warfighting organizations and mechanisms that the Navy uses in other warfighting domains. That is, C10F is a three-star numbered fleet that provides operational oversight and uses its Maritime Operations Center to execute command and control over its assigned forces and subordinate Task Forces.

The backbone of this cyber capability is a motivated work force of uniformed and civilian teammates, such as those receiving the 2013 Copernicus award, who are the foundation of the Navy's efforts in the cyber domain. ✂



Outstanding Crypies Recognized

2014 On the Roof Gang Winners

From Commander, NAVCYBERFOR Public Affairs

VADM Michael S. Rogers, Commander, U.S. Fleet Cyber Command/U.S. 10th Fleet, announced the Navy and Marine Corps 2014 On The Roof Gang (OTRG) winners. The Navy OTRG winner was CTTTCM(IDW/SW/AW) Samuel R. Olmstead, Navy Information Operations Command (NIOC) Denver, CO and GySgt. John F. Kirk IV, Delta Company, Marine Cryptology Support Battalion, Fort Gordon, GA, was the Marine Corps winner.

"Throughout my cryptologic career I have been fortunate to have had the opportunity to work with some of the most talented and professional Sailors I have ever known. And it's these Sailors who truthfully raised my game and made me the CT that I am today," said Olmstead. "In short, the OTRG award isn't mine, it was earned by all the shipmates that I have served with across the years."

Kirk also felt honored "both personally and professionally" receiving the OTRG award. He too recognized he did not do it alone. "It elevates the respect I already have for the many Marines I have served with who have spent time mentoring, teaching and molding me to be a solid SIGINT (Signals Intelligence) Marine," said Kirk.

"I have learned a great deal about my job and myself by absorbing as much of that wisdom as possible. I challenge all of the young Marines out there in this field to go out and aggressively seek the knowledge and mentorship of the many great men and women of the Intel Community."

CAPT Danelle M. Barrett, NAVCYBERFOR Chief of Staff, acknowledged the honor of just being nominated for this prestigious award. "I wanted to call out the outstanding performance by our nominee, Senior Chief Gallardo, for all her tremendous contributions to Navy Information Warfare. We are very proud of all she has done."

"This nomination was never about me, it's a reflection of the Sailors I've worked with and all the mentors that have guided me throughout my career," said Gallardo. "I was extremely humbled to even be considered."

Rogers noted the competition was "particularly keen" this year. He also extended congratulations to the following stellar nominees: ✂

- CTRCM(IDW/SW) Brent L. Baty, NIOC Texas
- CTRCS(SW/AW) Brandon A. Drake, SPAWARSCEN Atlantic
- CTICS(IDW/SW) Kasey M. Gallardo, NAVCYBERFOR
- CTNCM(IDW/SW) Lance S. Johansen, NIOC Hawaii
- CTRCS(IDW/SW) Dan L. Leonard, Commander, 7th FLEET
- CTRCS(IDW/SW/AW/NAC) Brian P. Mueller, NIOC Whidbey Island
- CTRC(IDW/SW) Wynoka M. Munlyn, USS Dwight D. EISENHOWER
- CTTCS(IDW/SW/AW) James E. Northrop, USS George WASHINGTON
- CTRC(IDW/NAC/PJ) Alexander C. Ollison, NIOC Yokosuka
- CTICS(IDW/AW/NAC) Heather N. Stokes, NIOC Maryland



Official U.S. Navy Photo

CTTTCM(IDW/SW/AW)
Samuel R. Olmstead



Official U.S.M.C. Photo

GySgt John F. Kirk IV

OTRG History

Between the years 1921 and 1927, U.S. Navy and Marine Corps personnel taught themselves to break Japanese code and passed these skills informally to many of their contemporaries. The value of the information extracted was recognized, and under the auspices of OP20G, the former Office of the Director of Naval Communications. Formal training was subsequently developed and implemented in 1928. Until 1941, this activity took place in a specially constructed block house on the roof of the old main Navy building in Washington, D.C., called the "On-the-Roof" Gang (OTRG). Since 1983, the OTRG award has recognized cryptologists who exemplify leadership, initiative, resourcefulness and dedication, and personify the highest traditions established for cryptologic excellence.



Cryptologic Technicians are Leading the Way

EDITOR'S NOTE: *The following article is taken from a Navy Live blog, April 18, 2014, by VADM Jan E. Tighe, Commander, U.S. Fleet Cyber Command/Commander U.S. 10th Fleet.*

Today, five of the Navy's finest Sailors were honored during the 2013 Navy Shore Sailor of the Year Ceremony held at the Pentagon. Each one of these outstanding Sailors earned the right to be considered for the esteemed title of Shore Sailor of the Year and each exemplifies the Navy's Core Values of Honor, Courage and Commitment.

Two of the five Sailors from this remarkable group of finalists share the Cryptologic Technician Collection or CTR rating – CTRs are experts in intercepting signals. The two nominees are:

CTR1(IDW/SW/AW) James R. Lee, Jr., nominated by the Center for Information Dominance (CID) Detachment San Diego and currently with Navy Special Warfare Command.

CTR1(IDW/SW) Patricia H. Madigan, Navy Information Operations Command (NIOC) Hawaii. NIOC Hawaii is a subordinate command of U.S. Fleet Cyber Command and comprises Task Force 1070 of the U.S. 10th Fleet.

I had the distinct pleasure of meeting both CTR1 Lee and CTR1 Madigan today during the ceremony. They well represent the Navy and CT community!

Their nominations also speak volumes about their personal commitment to excellence and the outstanding professionals who make up the U.S. Navy's 10th Fleet team and Information Dominance Corps.

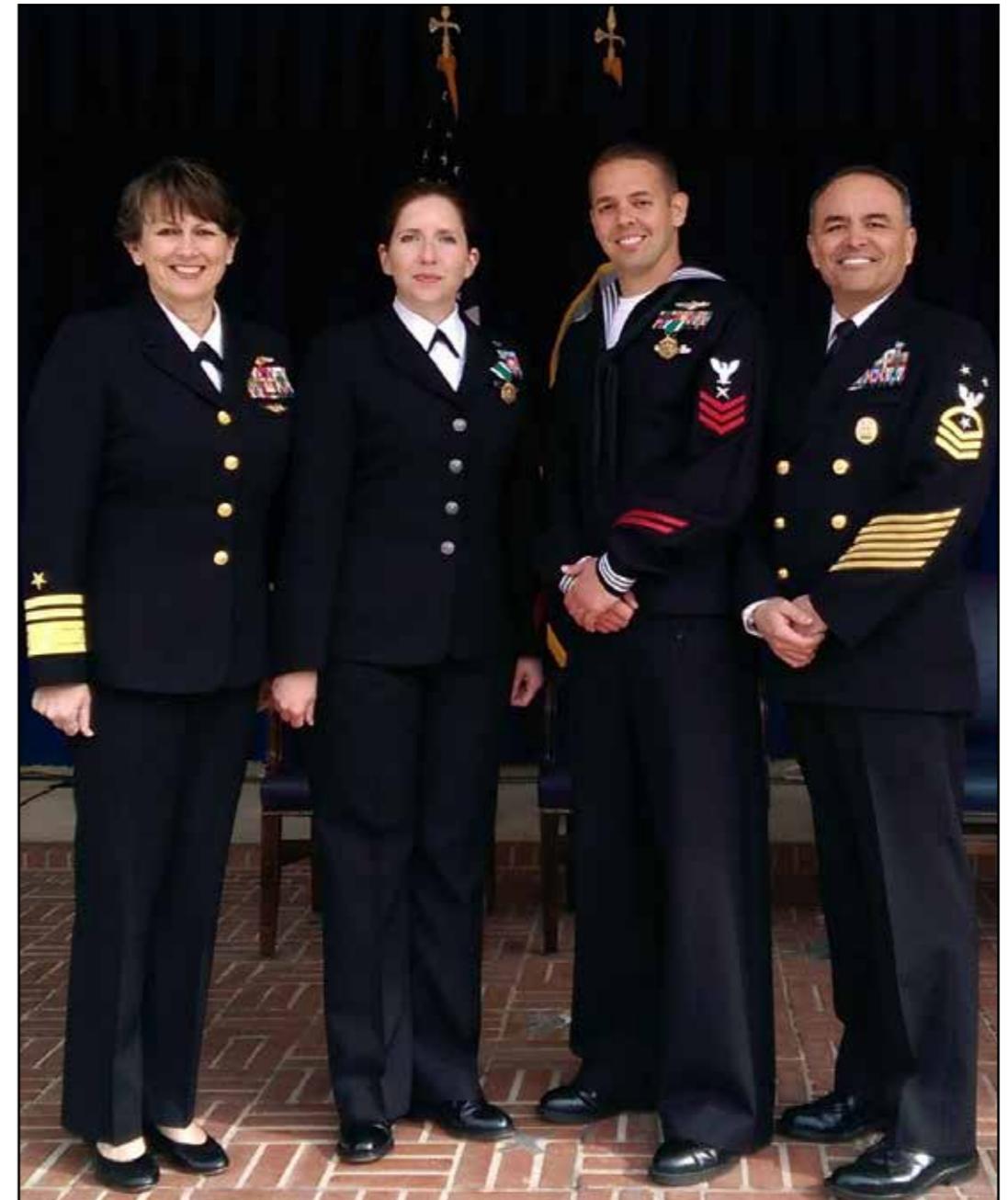
Moreover, it is an honor to note that CTR1 Madigan was selected as the 2013 Shore Sailor of the Year!

CTR1 Madigan is an outstanding leader who will continue to serve our Navy and country very well, and with even greater responsibility, as she will be meritoriously promoted to Chief during a ceremony on May 22 at the U.S. Navy Memorial in Washington, DC. ✕

EDITOR'S NOTE: Additional background from Navy.com about CTRs: ... their primary responsibility is to collect, analyze, and report on communication signals using computers, specialized computer-assisted communications equipment, video display terminals and electronic/magnetic tape recorders.

CTRs are also assigned duties as fusion analysts – a role that involves taking intelligence data from multiple sources, effectively 'piecing together the puzzle,' and generating a coherent intelligence product report to be used by decision makers.

If you are interested in learning more about CTRs and other Information Dominance Corps jobs in the U.S. Navy, go to: <https://www.navy.com/careers/information-and-technology/cryptology.html>.



(Left to right) VADM Jan E. Tighe, commander FCC/C10F; CTRC(IDW/SW) (select) Patricia H. Madigan; CTR1(IDW/SW/AW) James R. Lee, Jr.; and CMDCM FCC/C10F Jon R. Taylor pose following Madigan's announcement as the Navy's 2013 Shore SOY. (Official U.S. Navy Photo)



NAVCYBERFOR Senior Chief Takes 2014 Cryptologic Support Excellence Award

Commander, U.S. Fleet Cyber Command has announced that CTMCS(IDW) Ricky L. Pottebaum is the winner of the 2014 Award for Cryptologic Support Excellence (ACSE). This is an annual award recognizing Navy and Marine Corps personnel for their superior accomplishments in cryptologic support functions.

The award will be formally presented to Pottebaum on May 15, 2014, at the annual reunion of the U.S. Naval Cryptologic Veterans Association in Mobile, AL. Pottebaum is stationed at Navy Cyber Forces in Suffolk, VA and was selected from a field of 11 other outstanding nominees. ✂



CTMCS(IDW) Ricky L. Pottebaum



WASHINGTON -- CTR1(IDW/SW) Patricia H. Madigan receives a Navy-Marine Corps commendation medal from Vice Chief of Naval Operations, ADM Mark E. Ferguson III after winning the 2013 Navy Shore Sailor of the Year (SOY) competition at the Pentagon. The Navy Shore SOY program was established in 1972 to recognize Sailors who represent the best of the Navy by demonstrating both professional and personal dedication above and beyond their peers. This year's competition was among 5 first class petty officers representing shore commands across the entire Fleet. (Photo by MC1 Thomas L. Rosprim)

Special RECOGNITION

NCVA Seeks Members

If you have ever served or are serving in the U.S. Navy's cryptologic or cyber warfare organizations, the U.S. Naval Cryptologic Veterans Association (NCVA) would like you as a member.



NCVA is an organization of current and former officer and enlisted military (from all branches) and civilian cryptologic/cyber personnel who served or are serving in the Navy's cryptologic/cyber organizations. Their primary focus is preserving their rich cryptologic history and maintaining contact with those with whom they've served.

Their uniqueness is founded in the pioneering spirit of our oldest WWII and Cold War members, and in the cutting edge service of today's Navy's cryptologic and cyber warriors. In recognition of service and contributions to their heritage, the NCVA is offering a free one-year membership to all active duty personnel, which is renewable each year as long as the person remains on active duty.

The only stipulation is that the person agrees to take delivery of our flagship publication the "CRYPTOLOG" via a download from our Password Protected Directory (PPD) on the NCVA website. Once they have applied for the active duty membership, they will need to contact the webmaster to set up your PPD account.

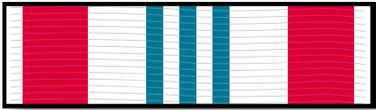
More information is available on their website at <http://www.usncva.org/> or from their Public Affairs Officer via email at pao@usncva.org or via USPS at NCVA PAO, Box 66, Gouldsboro, ME, 04607. ✂





LEGION OF MERIT

CAPT David Bailey, FLTCYBERCOM
CAPT Daniel MacDonnell, COMTENTHFLT
CAPT John MacMichael, Jr., NCTAMS PAC
CAPT George Snider, NR NAVCYBERFOR OPS



DEFENSE MERITORIOUS SERVICE MEDAL

CTI1 Mohammed Adawi, NIOC Maryland
CTI1 Joshua Devore, NIOC Georgia
CTRC Michael Hernandez, NIOC Texas
CTIC John Jordan, NIOC Maryland
CTTC Frakelia Leonard, NIOC Maryland
CTRC Randy McKnight, NIOC Texas
CWO2 Adam Morrison, NIOC Texas
CTI1 Laura Catherine Olack, NIOC Maryland
CTRC Keli Patterson, NIOC Hawaii
CTIC Dennis Phillips, NIOC Maryland
LCDR Eduardo Salazar, NIOC Maryland
CTTC Matthew Saxton, NIOC Colorado
CTRC Ivan Toney, NIOC Maryland
LT Robert Virden, SUSLA Korea
CTRC Eric Webb, NIOC Maryland



MERITORIOUS SERVICE MEDAL

ICDR Eugene Bailey, NCTS San Diego
YNCM Gerald Burgess, NIOC Texas
CDR Theodore Burke, NIOC Norfolk
CAPT James Butler, NR NIOC Texas
LCDR Bobby Carmickle, NCTAMS LANT DET
Hampton Roads

CDR John Delaere, FLTCYBERCOM
CDR Robert Flickinger, FLTCYBERCOM
LCDR Randal Fuller, NCTS Guam
CDR Carl Sullivan, NR NIOC Tacoma
CDR Allen Williams, NAVCYBERFOR Suffolk



JOINT SERVICE COMMENDATION MEDAL

CTN2 Reesha Alexander, NIOC Maryland
CTNC Bernard Armer, NIOC Georgia
IT3 Stacey Ayers, Yokota Air Base
CTN2 Sarah Baalbergen, NIOC Hawaii
CTRC Matthew Barr, NIOC Texas
CTN1 Robert Battocletti, NIOC Maryland
CTRC Brandon Beaudoin, NIOC Maryland
CTI1 Rachel Brown, NIOC Georgia
CTI1 Justin Carter, NIOC Maryland
CTT1 Dustin Chapman, NIOC Colorado
CTN2 Katherine Christensen, NIOC Maryland
IT2 Casey Clydesdale, NIOC Maryland
CTR2 Brooke Comer, NIOC Maryland
LTJG Christopher Crabtree, Yokota Air Base
LTJG James Dells, NIOC Maryland
CTRC Daniel Farnsworth, NIOC Georgia
CTR2 Jose Galvan, NIOC Maryland
CTRC Miguel Garcia, Jr., NIOC Menwith Hill
CTN2 Ian Gentry, NIOC Maryland
CTM2 Andrew Gibson, NIOC Hawaii
CTT1 Christopher Gillen, NIOC Maryland
CTN2 Caleb Golchert, NIOC Maryland
CTR2 Gene Griffin, NIOC Maryland
CTI1 Drew Hawthorne, NIOC Georgia
YN1 Lillie Hernandez, NIOC Maryland
CTR1 Raul Herrera, NIOC Maryland
CTI2 John Hubbell, NIOC Georgia
CTI2 Nicholas Iverson, NIOC Georgia
CTMC William Knehr, NIOC Georgia
CTI2 Eric Lampi, NIOC Georgia
CTN2 Charles Lee, NIOC Texas
CTI2 Jared Lewis, NIOC Hawaii
CTN2 Brian Maroney, NIOC Georgia
CTN1 Michael McCall, NIOC Maryland
LTJG Justin Monroe, NIOC Maryland
CTN1 Kevin Montoya, NIOC Maryland
CTR1 Justin Mullins, NIOC Maryland
CTI2 Jennie Murch, NIOC Georgia

CTI1 Jennifer Murphy, NIOC Maryland
CDR Glenn Murray, NIOC Georgia
CTI2 Peter Musser, NIOC Hawaii
CTR2 Ericka Newland, NIOC Hawaii
CTN2 Lashay Pettis, NIOC Georgia
CTI1 Lindsey Phillips, NIOC Georgia
CTN1 Joshua Porter, NIOC Texas
CTI2 Michael Pounds, NIOC Georgia
CTR2 Raquel Ramos, NIOC Maryland
CTR1 Patrick Roark, NIOC Maryland
CTN1 Alexander Robinson, NIOC Maryland
CTI1 Charles Rose, NIOC Texas
CTI1 Jacqueline Saenz, NIOC Georgia
CTR2 Daniel Saldivar, NIOC Maryland
CTI2 Brianna Sanden, NIOC Hawaii
CTR1 Kendell Shinmori, NIOC Colorado
CTI1 Jason Sikora, NIOC Maryland
CTR1 Terri Siler, NIOC Misawa
LTJG Phillip Smith, NIOC Hawaii
CTT1 Nicholas Southwell, NIOC Georgia
CTI1 Justin Sumner, NIOC Hawaii
CTN2 Leesa Tarter, NIOC Maryland
CTRC Sean Temples, SUSLA Korea
CTR2 Miari Thornhill, NIOC Maryland
CTN1 Marissa Viaene, NIOC Hawaii
CTN1 Nathan Vidal, NIOC Maryland
CTN2 Mark Watkins, Jr., NIOC Georgia
CTR1 Gilbert Webster, NIOC Menwith Hill
LS1 Shane Weems, NIOC Hawaii
LT Daniel Whitaker, NIOC Maryland
LT Joshua Williams, NIOC Hawaii



NAVY AND MARINE CORPS COMMENDATION MEDAL

LTJG Scott Aaron, NIOC Maryland
CTI1 Ghathe Alkhalaf, NIOC Georgia
CTRC Kimberly Allen, NIOC Whidbey Island
LT Rodney Arthur, NIOC Maryland
LTJG John Bardenhagen, NAVCYBERFOR FIAF DET
San Diego
LCDR David Barnes, FLTCYBERCOM
ITCM Eugene Bartholomew, Jr., NCTAMS LANT
NMCI DET Norfolk
LCDR Valeret Bass, NAVCYBERFOR FIAF DET
Pearl Harbor
CTR1 Kyle Beccue, NIOC Maryland

CTR2 Stephen Bittman, NIOD Digby
LT Christopher Bjornnes, NIOD Groton
LT Ezra Blanche, NIOC Bahrain
LCDR Theodore Bohl, NIOC Norfolk
LCDR Robert Boyce, FLTCYBERCOM
ITC Christopher Brown, NAVCYBERFOR Suffolk
ITC Rachel Brown, NCTAMS PAC
LTJG James Brown, Jr., NIOC Maryland
CTIC Christopher Calder, NIOC Hawaii
CTRC Dawn Carlton, NIOC Norfolk
ITCS Gregory Carter, NCTAMS PAC DET Puget Sound
CTNC Dave Collins, NIOC Georgia
LTJG Brian Crawford, NIOC Georgia
IS1 John Cruse, NAVCYBERFOR FIAF DET Norfolk
CTRC Nakia Davis, NIOC Georgia
CTIC Hillary Deems, NIOC Georgia
IT1 Nathan Detandt, NCTAMS LANT DET Rota
CDR Gregg Dewaele, FLTCYBERCOM
LT Jonathan Dieter, NCTS Naples
CTN1 Dessamba Diop, NDCOC
CTR1 Adam Duncan, NIOD Digby
CWO3 Angela Elder, NCTS Bahrain
CDR David Filanowicz, FLTCYBERCOM
CDR Ethan Gibson, FLTCYBERCOM
CTR1 Michael Graham, NIOC Bahrain
LT Eric Hayden, Jr., NIOC Texas
CTR1 William Hemming, NIOC Georgia
CTRC Tabitha Henry, NIOC Maryland
CDR Damen Hofheinz, FLTCYBERCOM
CTIC Amos Hoover III, NIOC Georgia
ITCM Lisa Ingram, NCTS Bahrain
CTN1 Kelli Keisel, NIOC Maryland
ITC Duane King, NMCSO PAC Honolulu
IT1 Neal King, Jr., NDCOC
ITC Nichole Knight, NCTS Bahrain
CTRC Alexis Lund, NIOC Hawaii
FCC Shawn Lynn, NCTAMS LANT
LCDR Njuguna Macaria, NAVCYBERFOR Suffolk
CTNC Allyn Malventano, NIOC Texas
ITCS Randall Mand, NAVCYBERFOR Suffolk
LCDR Joseph Maxwell, FLTCYBERCOM
CTI1 Sean McCue, NIOC Georgia
CTTC Tilisa McCullers, NIOC Norfolk
ITC Alisha McElhaney, NNWC Suffolk
ITC Tywandia McLean, NNWC Suffolk
LT Cody Mortensen, NCTAMS LANT
CTR1 Allyn Morton, NIOC Maryland
YN1 Jackie Murphy, NIOC Texas
LCDR James Ogden, NAVCYBERFOR Suffolk
ITC Derrick Owens, NCTAMS LANT
HM1 Josemaridennis Pascual, NIOC Georgia
LT Patrick Payte, NAVSOC



ITC Leroy Rhem, Jr., NCTAMS PAC
LCDR Darren Rice, FLTCYBERCOM
YNC Teresa Roberson, NCTS Bahrain
ITC John Robertson, NNWC Suffolk LT William Runge, Jr., NR NIOC ST Louis
LT Griffin Saving, NIOC San Diego
ITC James Shupe, NCDOC
CTTCS Michael Sipes, NIOC Norfolk
CTTCS Eddie Smith, NIOC Norfolk
LT Sol Snyder, NAVSOC
ETC Erik Stanland, NCTS Bahrain
CTRC Matthew Strauss, NIOC Whidbey Island
ITC Thomas Surratt, Jr., NCTS Naples
CTI1 William Tavery, NIOC Maryland
LT Anthony Thomas, NAVCYBERFOR Suffolk
CDR Vincent Tionquiao, FLTCYBERCOM
CTTC Alicia Tuft, FLTCYBERCOM
CTICS David Ure, NIOC Bahrain
CWO4 Danny Walton, NCTS Naples
CTR1 Scott Wegner, NIOC Maryland
CTIC Nathan Wells, NIOC Texas
IT1 Larry Wilson, NCTS Naples
IT1 Stephen Winborn, NAVCYBERFOR Suffolk
CDR Karen Wingert, NR NNWC Suffolk
LT James Wolff, NR NAVCYBERFOR OPS



JOINT SERVICE ACHIEVEMENT MEDAL

CTN1 Byran Adamic, NIOC Maryland
IT2 Bradley Alspaugh, SUSLA Korea
CTR3 Stuart Ament, CJTF-Horn of Africa
CTI2 Daniel Beardsell, NIOC Maryland
CTR2 Justin Behzad, NIOC Misawa
CTR3 Keith Blum, NIOC Misawa
CTM2 Alice Bruley, NIOC Hawaii
LTJG Forrest Bush, NIOC Maryland
CTR1 Kristopher Caldwell, NIOC Maryland
CTT2 Mitchell Carpenter, NIOC Hawaii
CTN3 Richard Clark, NIOC Hawaii
CTTC Scott Cooper, NIOC Hawaii
CTR2 Cody Cox, NIOC Georgia
CTI2 Christine Crisostomo, NIOC Maryland
YN2 Nicholas Dimercurio, SUSLA Korea
IT3 Kiara Dominguez, NIOC Hawaii
CTR2 Jazmine Elahee, NIOC Georgia
LT Jordan Fox, NIOC Maryland
CTI3 Jacqueline Frisina, NIOC Hawaii

CTI1 John Gann, NIOC Hawaii
CTI2 Joseph Glass, NIOC Hawaii
MA3 Matthew Green, NIOC Hawaii
CTI3 Amiebrae Harmon, NIOC Hawaii
CTR3 Brittany Hernandez, NIOC Hawaii
CTN3 Derek Hockman, NIOC Maryland
CTN3 James Honea, NIOC Maryland
CTI2 Christopher Johnson, NIOC Georgia
CTN3 Jessica Jolly-Ricouard, NIOC Maryland
CTN2 Nathan Kehn, NIOC Maryland
IS2 Tami King, NIOC Hawaii
CTI2 Jasmine Loran, NIOC Texas
CTN3 Serena Mansfield, NIOC Maryland
CTN2 Bryan Martin, NIOC Georgia
CTN2 Cody Martz, NIOC Texas
CTR2 Erin McDermott, NIOC Colorado
LTJG John McMurray, NIOC Maryland
CTR3 Emily Nelson, NIOC Maryland
CTI2 Anthony Pace, NIOC Georgia
CTI2 Ryan Park, NIOC Georgia
IT2 Cheyenne Patty, NIOC Maryland
CTR2 Richard Pearse, NIOC Hawaii
CTR1 Matthew Perezluha, SUSLA Korea
CTR3 Christopher Puleo, NIOC Sugar Grove
CTI1 Aaron Pyle, NIOC Georgia
MA3 Kristopher Rakes, NIOC Hawaii
CTI1 Adam Richardson, NIOC Georgia
CTT2 Nicole Richardson, NIOC Colorado
IT3 Andrew Rowland, NIOC Maryland
CTR1 Patrick Sherlock, NIOC Maryland
EO2 Gary Slack, NIOC Maryland
CTR1 Rodney Slusher, NIOC Misawa
IS3 Steven Spires, NIOC Maryland
CTN2 Levi Terry, NIOC Maryland
CTN1 Nicholas Thomas, NIOC Maryland
LTJG John Thurmond, NIOC Maryland
CTI2 Jeremiah Ulrich, NIOC Hawaii
CTR2 Charles Ulveling, NIOC Maryland
CTN3 Dara Valdez, NIOC Maryland
CTR2 Jorden Washburn, NIOC Georgia



NAVY AND MARINE CORPS ACHIEVEMENT MEDAL

IT1 Omar Abdi, NNWC Suffolk
YN3 Alexander Adams, NCTS Sicily
CTI1 James Agee, NIOC Georgia

CTI1 Leah Agee, NIOC Georgia
CTN2 Layton Aho, NCDOC
CTI1 William Alexander, NIOC Bahrain
CTR2 Pamela Alford, NIOC Pensacola
CTIC JohnMark Allen, NIOC Hawaii
IT2 Bradley Alspaugh, NIOD Seoul
ITC Dyonisha Anderson NCTAMS PAC
CTR2 Angel Aquino, NIOC Pensacola
LTJG Jermaine Armstrong, NAVCYBERFOR FID Washington
LS1 Jonathan Azarcon, NCTS Bahrain
ET2 Theo Bailey, NCTS San Diego
CTR2 Charles Bain, NIOC Bahrain
CTTSN Carrie Baity, NIOC San Diego
ITCS Labrina Banks, NCTAMS LANT DET Norfolk
IT2 Jennifer Barnthouse, NCTS Sicily
CTI1 Amy Bates, NIOC Bahrain
CTN3 Charles Batts, NIOC Maryland
CTM3 John Beasley, NIOC Hawaii
IT2 Dennis Bellamy, NCTS Sicily
ITC Andre Belser, NCTAMS LANT
IT1 Joseph Bentley, NNWC Suffolk
ET1 Nicolas Betz, NCTAMS LANT DET Rota
IT1 Edward Blevins III, NCTAMS LANT DET Souda Bay
IT2 Jennifer Blower, NCTS Bahrain
CTI1 Jason Bonsell, NIOC Georgia
IT2 Daniel Boseman, NCDOC
IT2 Toni Boyd, NCTAMS LANT
CTI2 Caroline Brewer, NIOC Texas
ETC Aaron Britt, NCTAMS LANT
CTI2 Gabriel Brown, NIOC Georgia
IT2 Matthew Brown, Jr., NCTAMS LANT DET Souda Bay
IT3 Roderick Brown, Jr., FLTCYBERCOM
LT Kathryn Buikema, NIOC Maryland
CTT2 Matthew Bullock, NIOC Hawaii
CTN3 Austin Butts, NIOC Maryland
IT3 Nathan Campbell, FLTCYBERCOM
ITC Allan Capps, NCTS Sicily
IT1 Oliver Carlin, NCTS Guam
IT2 Cody Carlson, NCTS Guam
LTJG David Carroll, NR COMTENTHFLT
IS2 Gwen Cernecarl, NAVCYBERFOR FIAF DET San Diego
BMC Cherise Chase, NCTAMS LANT
CTI2 Richard Clark III, NIOC Georgia
ITC Michael Cloutier, NNWC Suffolk
IT2 Jill Cody, NCTS Naples
CTN3 Zachary Coker, NIOC Maryland
CTM1 Brenden Collins, NIOC Yokosuka
IT2 Christina Cooper, NCTAMS PAC
IT3 Blake Cotton, NCTAMS LANT DET Rota
CTM3 Ryan Crosby, NCTAMS LANT DET Hampton Roads
IT1 Jonathan Cunha, NCTS FE DET Diego Garcia

YN1 Mark Cutler, FLTCYBERCOM
CTN2 Emily Dabruzzo, NIOC Hawaii
YN2 Anthony Dagle, FLTCYBERCOM
IT1 Omar Daly, NCTAMS LANT NMCI DET Norfolk
HM1 Patrick Daly, NIOC Misawa
ET1 Timothy Davis, NCTS San Diego
CTI2 Krista Delap, NIOC Hawaii
CTT2 Sarah Diaz, NNWC Suffolk
CTI2 Lorena DiazMejias, NIOC Maryland
CTN3 Paul Diediker, NIOC Pensacola
IT2 Neil Dizon, NIOC Norfolk
CTT1 Jahun Dugger, NIOC Maryland
IT3 Glenn Dunkirk, NCTAMS LANT
SW1 Riley Edwards III, NCTS Bahrain
CTM2 Russell Ekin, NCTS Guam
IT3 Kimberly Erler, NCTS San Diego
IS2 Frantz Exantus, NIOC Pensacola
CTN1 Jeremy Farr, NIOC Pensacola
CTT2 Justin Farris, NIOC Georgia
CTI1 Eduardo Ferriol, NIOC Maryland
LS2 Christopher Figueroa, NIOC Maryland
ITC Randal Foss, NCTAMS PAC
ET1 Katherine Foster, NCTAMS LANT
CTN3 Tyrone Francis, Jr., NIOC Maryland
LTJG John French, NIOC Hawaii
LS2 Thomas Friedman, NCTS Bahrain
CTN2 Andrew Galens, NCDOC
CTI1 Ryan Gallagher, NIOC Maryland
IT2 Mary-Colleen Garr, NCTS San Diego
CTI2 Erin Gebhart, NIOC Georgia
CTR3 Joshua Gober, NIOC Maryland
LT Robert Gonzalez, NCTAMS PAC
IT3 Matthew Greene, NCTS Far East
IT3 Michael Grubbs, NCTS Naples
IT3 Mario Gutierrez, Jr., NCTAMS LANT
IT1 Raquel Hadley, NAVCYBERFOR Suffolk
IT1 Scott Halton, NCTS Naples
ENS Jon Hammond, NCTS FE DET Diego Garcia
CTR2 Jon Harperslaboszew, NIOC Hawaii
CTM1 Justin Hatfield, NIOC Yokosuka
CTR3 Jeffrey Hendershot, NIOC Colorado
CTN3 Pricilla Henderson-Starr, NIOC Maryland
CTN2 Patrick Henry, NIOC Norfolk
IT2 Brenda Hernandez, NAVCYBERFOR Suffolk
IS2 Evan Hill, FLTCYBERCOM
CTTC Nicholas Howlett, NIOC Georgia
CTR2 Christopher Huls, NIOC Pensacola
EM2 Jomi Jack, NCTS Sicily
IS3 Ebony Jackson, NAVCYBERFOR FID Fallon
IT1 Paul Johnson, NCTS Bahrain
CTN3 Jessica Jolly-Ricouard, NIOC Georgia
CTNC Aimee Jones, NIOC Hawaii



IT1 Justin Jones, NCTAMS LANT DET Hampton Roads
ET1 Colby Karaim, NCTS Sicily
ITC Giles Kawahara, NCTAMS LANT
ET1 Anna Keown, NCTS San Diego
IT1 Jabir Kesler, NCTS Jacksonville
IT3 Chantel King, FLTCYBERCOM
LT Ryan Klint, NIOC San Diego
CTI2 Nikolaus Klutch, NIOC Georgia
IS2 Derreck Koch, NAVCYBERFOR FIAF DET San Diego
IT1 Joseph Kornegay, NCTAMS LANT
CTR3 Jeffrey Kryman, NIOC Georgia
CTM2 Nathan Kuhn, NIOC San Diego
ET3 Jasmin Lamanna, NCTAMS LANT DET Hampton Roads
CTR1 Brandy Lambert, NIOC Norfolk
ENS Krystina Landry, NIOC Maryland
CTR2 Andrew Languille, NIOC Colorado
CTI1 Kelly Larsen, NIOC Georgia
CTI3 Dustin Ledbetter, NIOD Seoul
YN1 Mark Lentz, Jr., NCTS Bahrain
LT John Leo, NIOC Norfolk
CTR3 Kara Leonard, NIOC Maryland
CTT1 Christopher Lomont, NIOC Hawaii
IT1 Mark Long, NCTS Sicily
IT1 Thomas Loughridge, NIOC Whidbey Island
IT2 Dominic Lounsbery, NCTS Naples
CTR2 Charles Mainwaring, NIOC Georgia
IT2 Brian Marcello, NCTAMS LANT
ET2 Amber March, NCTAMS LANT
IT1 Mikel Marlin, NCTAMS PAC
CE1 Giovanni Marquez, NCTS San Diego
IT2 Mervin Martinez, NCTAMS PAC
IT2 Lakeisha Massenburg, NAVCYBERFOR Suffolk
CTI1 Elizabeth McCarty, NIOC Georgia
CTN2 Skyler McClelland, NIOC San Diego
IT2 Justin McDonald, NCTAMS LANT
ET3 Lauren McLelland, NCTAMS LANT
IT2 Michael McMillan, NCTS San Diego
CTN1 Sean McNerney, NIOC Pensacola
ET2 Charles Meeks, NCTS San Diego
CTN2 Aaron Melhus, NIOC Norfolk
IT2 Burton Melzer, NCTS Bahrain
ET1 Kevin Meyer, NCTS Bahrain
CTR1 Justin Miles, NIOC Yokosuka
CTTSN Keagan Miller, NIOC Georgia
CTI2 Brandon Millichamp, NIOC Hawaii
IT2 Sophia Mineor, NCTAMS LANT NMCI DET Norfolk
CTT1 Victoria Mobley, NIOC Yokosuka
CTIC Matthew Monroe-Jimenez, NIOD Australia
IT2 Joseph Montano, FLTCYBERCOM

LS2 Rena Moore, NIOC Georgia
CTR3 Richard Morris, NIOC Maryland
CTN2 David Myers, NIOC Norfolk
CTI2 Lauren O'Donoghue, NIOC Georgia
ET3 Michael Oddy, NCTS Bahrain
CTM2 Hector Olmeda, Jr., NIOC Yokosuka
CTN1 Benjamin Olney, NIOC Pensacola
CTI1 Heather Owens, NIOC Georgia
CTN1 Samwel Oyamo, NIOC Norfolk
ET2 Albert Palmer, NCTAMS LANT
CTR1 Ryan Passarino, NIOC Georgia
CTI2 Kevin Peck, NIOC Georgia
CTT1 Erika Pepler, NIOC Colorado
IT1 Reneika Perkins, NIOC Norfolk
CTR2 Scott Peterson, NCDOD
CTR2 Gary Phelps, NIOD Digby
CTT1 Roderic Phillips, NIOC Georgia
CTT1 Theodore Preztak, NIOC Whidbey Island
LSC Arthur Racela, NIOC San Diego
CTI1 Taro Radke, NIOC Hawaii
CTR2 Meggan Rahn, NIOC Texas
IT1 Jose Ramirex II, NCTAMS PAC
IT2 Lydia Rathbun, NCTS Naples
CTN2 Dennis Reber, Jr., NIOC Georgia
CTR2 Naonesha Reddick, NIOC Maryland
CTR2 Derik Reimers, NIOC Hawaii
IT1 Susie Rhem, NCTAMS PAC
CTI3 Terrel Richardson, NIOC Maryland
IT1 Keith Risner, NCTAMS LANT
IT1 Nina Ritchie, NCTAMS PAC
CTI1 Jorge Rivera, NIOC Georgia
IT2 Derek Roberson, NCTAMS PAC
LS2 Jason Rockney, NIOC San Diego
CTM2 Alexander Sanchez, NIOC Hawaii
CTM2 Jonathan Sanders, NIOD Groton
IT1 Kevin Scott, NNWC Suffolk
IT1 Vanessa Self, NCTAMS LANT
ITC John Sheehy, NCTAMS LANT
IT2 Benjamin Sigl, NCTS San Diego
IT1 Timothy Simms, Jr., NCTAMS LANT
CTN1 Jeremy Simpson, NIOC Maryland
LTJG Coey Sipes, NCTS Naples
CTR1 Kristopher Slocum, NIOC Yokosuka
IT1 Brandon Smith, NIOC Whidbey Island
CTI1 Sadee Smith, NIOC Georgia
IT2 Rosalind Songer, NCTS San Diego
CTN1 Roderick Sparks, NCDOD
CTN1 Kevin Sroka, NIOC Maryland
IS3 Joshua Stringfellow, NIOC Georgia
CTR2 Tyler Stull, NIOC Maryland
YN2 Jasmine Tabery, NIOC San Diego

ET2 Lance Taniguchi, NCTAMS PAC
CTN2 Wilma Thacker, NIOC Pensacola
CTT2 Andrew Thomas, NIOC Maryland
LS3 Cory Thompson, NCTAMS LANT
CTR3 Peter Thompson, NIOC Maryland
CTR2 Miari Thornhill, NIOC Maryland
CTR1 Courtney Tillery, NIOC San Diego
CTTSN John Tomlinson, NIOC Georgia
CTR2 Jeannette Torres, NIOC Norfolk
CTM2 Matthew Trump, NIOC Norfolk
LTJG Lawrence Trundle, NAVCYBERFOR FID Fallon
CTIC Traca Tuthill, NIOC Bahrain
CTR2 Brittney Unthank, NIOC Georgia
CTM2 Jose Vargas, NIOC Bahrain
CTM2 Jose Vargas, NIOC Bahrain
CTI1 Joshua Voyles, NIOC Bahrain
CTI1 Aslan Walker, NIOC Georgia
IT1 Hoza Wallace, NCTAMS LANT NMCI DET Norfolk
OSC George Waller, NCTAMS LANT
IT2 Antoinette Washington, NCTS San Diego
CTNC Kyle Watts, NIOC Georgia
CTN1 Tyson White, NIOC Norfolk
CTT2 Shelby Whitehead, NIOC Maryland
IT2 Kody Williams, NCTS Naples
IT2 Larry Williams, Jr., NCTAMS LANT
IT1 Mignone Wolf, NCTAMS LANT DET Hampton Roads
YN3 Jonathan Workman, NCTAMS PAC
YN2 Quinntina Wright, NIOC Georgia
IT3 Amber Yeomans, NCDOD
CTN1 Aisha Young, NIOC San Diego



SUPERIOR CIVILIAN SERVICE MEDAL

Marlinda Hodges, FLTCYBERCOM



MERITORIOUS CIVILIAN SERVICE MEDAL

Pat Faver, NAVCYBERFOR
Brian Whyte, FLTCYBERCOM



MILITARY OUTSTANDING VOLUNTEER SERVICE MEDAL

ITC Gene Detweiler, NCTAMS PAC
YN2 Jonathan Edwards, NCTS San Diego
YNC Priscilla Muguy, NCDOD
IT2 Josiah Sawyer, NCTS Guam
LT Christopher Tighe, NIOC San Diego
YN2 Jonathan Edwards, NCTS San Diego
YNC Priscilla Muguy, NCDOD
IT2 Josiah Sawyer, NCTS Guam
LT Christopher Tighe, NIOC San Diego

CIVILIAN LENGTH OF SERVICE AWARDS

Nancy Rantanen, FLTCYBERCOM - 35 Years
Vernetta Schroder, FLTCYBERCOM - 30 Years
Joseph Brown, FLTCYBERCOM - 25 Years
Sean Cunningham, FLTCYBERCOM - 25 Years
Elizabeth Varner, FLTCYBERCOM - 25 Years
Stephen Fehr, FLTCYBERCOM - 15 Years
Tammy Johnson, FLTCYBERCOM - 15 Years
Stephen Launse, FLTCYBERCOM - 15 Years
John Neidig, FLTCYBERCOM - 15 Years
Charles Cyrus, FLTCYBERCOM - 10 Years
Jorge Castro, FLTCYBERCOM - 10 Years
Walter Goodall, FLTCYBERCOM - 10 Years
Scott Raye, FLTCYBERCOM - 10 Years
Dale Taylor, Sr., FLTCYBERCOM - 10 Years
Gregory Thompson, FLTCYBERCOM - 10 Years
Mary Torres, FLTCYBERCOM - 10 Years
Deborah Alvarado, FLTCYBERCOM - 5 Years
Peggy Burke, FLTCYBERCOM - 5 Years
Adam Clevenger, FLTCYBERCOM - 5 Years
Alvin Gogue, FLTCYBERCOM - 5 Years
James McCarty, Jr., FLTCYBERCOM - 5 Years
Christopher McClintock, FLTCYBERCOM - 5 Years
Vickie Mimsharris, FLTCYBERCOM - 5 Years
Jeffrey Montgomery, FLTCYBERCOM - 5 Years
Katharine Orłowski, FLTCYBERCOM - 5 Years



Securing Major Leadership Roles - Women Lead from the Front

Taken from NavAdmin 043/14

March is National Observance of Women's History month. The national and Department of Defense theme for 2014 is, "Celebrating Women of Character, Courage and Commitment."

Women began serving in our Navy years before the passage of the 19th Amendment in 1920, which granted women the right to vote.

Women continue to influence, impact and make history in our Navy today. In 2013, many Navy leadership positions were filled for the first time by women to include: VADM Nanette Derenzi, the 42nd Judge Advocate General of the Navy; CAPT Sara A. Joyner, commander, Carrier Air Wing THREE; and CMDCM Susan Whitman, Force Command Master Chief for Commander, Navy Surface Atlantic. VADM Michelle Howard was nominated for appointment to the rank of Admiral and assignment as Vice Chief of Naval Operations. Upon confirmation, she will make history

as the Navy's first female four-star Admiral and the first woman to hold this position. And in April 2014, VADM Jan E. Tighe, Commander FCC/C10F, became the first woman to command a numbered Fleet.

Today, women in our Navy make up 18 percent of the active and reserve forces with more than 59,000 women serving on active-duty and more than 9,000 serving in the Navy Reserve. Additionally, over 54,000 women serve in a wide range of specialties as Navy civilians. Currently there are 32 active and Reserve flag officers, 69 Senior Executive Service (SES) members, 48 Command Master Chiefs and three Command Senior Chiefs leading from the front.

On Jan. 24, 2013, the Secretary of Defense and the Chairman of the Joint Chiefs of Staff announced the rescission of the 1994 Direct Ground Combat definition and Assignment rule. The rescission states the DoD's commitment to remove gender-based barriers to

service. Women are now routinely assigned to ships, afloat staffs, Naval construction Battalions, medical units, aviation squadrons and submarines. The Navy will continue to expand opportunities in the future as new ships and ship classes are commissioned.

Information on the contributions of women to our nation's legacy can be found at <http://womenshistorymonth.gov/> and <http://nwhp.org/>.



VADM Michelle Howard, Deputy CNO Ops, Plans and Strategy (N3/N5)

