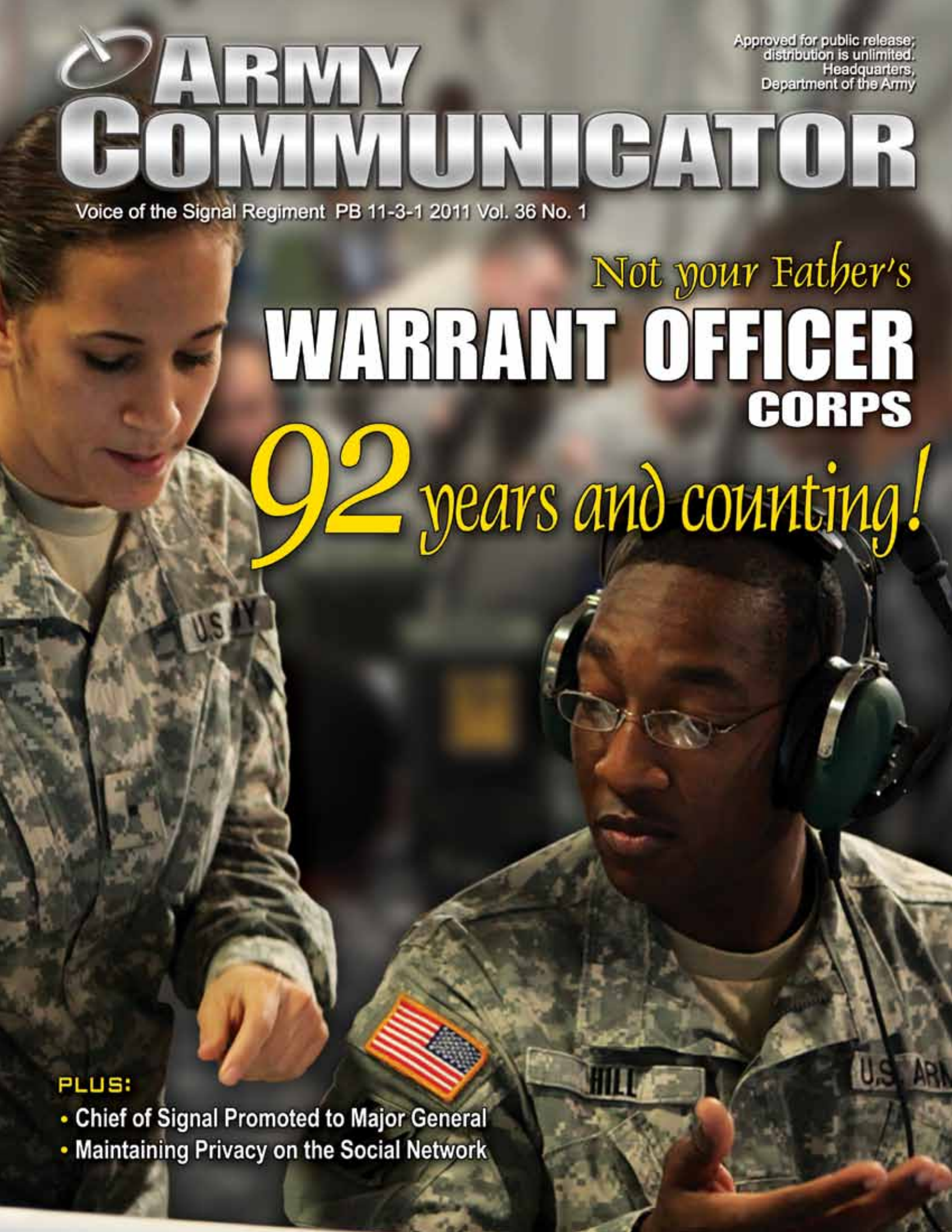
Approved for public release; distribution is unlimited.
Headquarters,
Department of the Army

# ARMY COMMUNICATOR

Voice of the Signal Regiment PB 11-3-1 2011 Vol. 36 No. 1

## Not your Father's WARRANT OFFICER CORPS

## 92 years and counting!



PLUS:

- Chief of Signal Promoted to Major General
- Maintaining Privacy on the Social Network

# Report Documentation Page

*Form Approved*
*OMB No. 0704-0188*



| 1. REPORT DATE | 2. REPORT TYPE | 3. DATES COVERED |
|---|---|---|
| **2011** | | **00-00-2011 to 00-00-2011** |

| 4. TITLE AND SUBTITLE | 5a. CONTRACT NUMBER |
|---|---|
| **Army Communicator. Volume 36 Number 1, Spring 2011** | 5b. GRANT NUMBER |
| | 5c. PROGRAM ELEMENT NUMBER |
| 6. AUTHOR(S) | 5d. PROJECT NUMBER |
| | 5e. TASK NUMBER |
| | 5f. WORK UNIT NUMBER |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)<br>**U.S. Army Signal Center of Excellence,Signal Towers (Building 29808), Room 713,Fort Gordon,GA,30905-5301** | 8. PERFORMING ORGANIZATION REPORT NUMBER |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) | 10. SPONSOR/MONITOR'S ACRONYM(S) |
| | 11. SPONSOR/MONITOR'S REPORT NUMBER(S) |

12. DISTRIBUTION/AVAILABILITY STATEMENT
**Approved for public release; distribution unlimited**

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT | b. ABSTRACT | c. THIS PAGE | | | |
| **unclassified** | **unclassified** | **unclassified** | **Same as Report (SAR)** | **84** | |

# CHIEF OF SIGNAL

Alan R. Lynn

## Warrant Officers

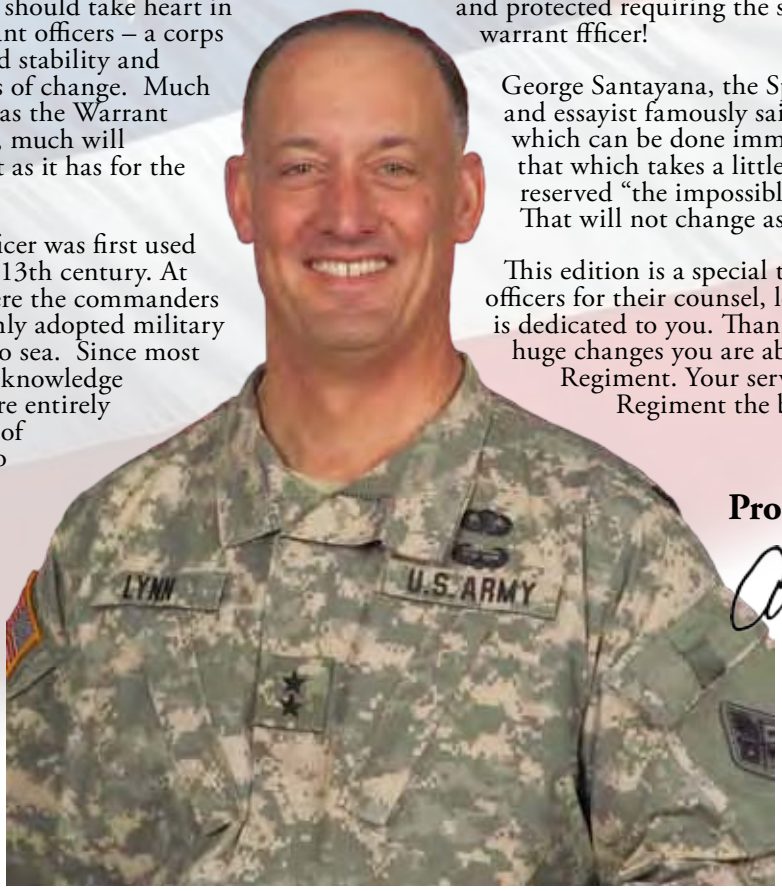
# *The past and the future of the Regiment*

Signaleers,

The Signal Functional Area Assessment that has been approved by our Undersecretary of the Army will have a tremendous impact on the Regiment. Beginning in 2013, much of what you know about the Regiment will change. I have served through the introduction of Mobile Subscriber Equipment, Modularity, and Increment 1 of the Warfighter Information Network Tactical. While each of these initiatives had a huge effect on the Signal Corps, the changes we are about to experience as we implement the FAA will be even greater. The FAA will profoundly re-shape our doctrine, organization, training, leader development, and personnel.

Given the dramatic changes we are facing, I decided to dedicate this issue of *Army Communicator* to our warrant officers. I did this for two reasons. First, because our Signal warrants will play a central role as we implement the FAA, it is absolutely essential for us to understand where we are, and where we are going, with our Warrant Officer Corps. Second, as we enter this period of immense change, we should take heart in the history of our warrant officers – a corps that has always provided stability and continuity during times of change. Much is about to change, but as the Warrant Officer Corps shows us, much will remain the same … just as it has for the past 800 years.

The rank of warrant officer was first used by English fleets in the 13th century. At that time, noblemen were the commanders of English ships, and only adopted military ranks when they went to sea. Since most of these officers had no knowledge of seamanship, they were entirely reliant on the expertise of the warrant officers who tended to the technical aspects of running the ship. Although our leaders are now very knowledgeable, the Signal Regiment continues to rely on warrant officers for their expertise on the technical aspects of our profession. The Warrant Officer Corps has never let us down.




Warrant officers are "systems-of-systems" experts. They have a firm grasp on joint and multinational operations, and know how to integrate Signal capabilities into complex operating environments. They are competent and confident warriors, innovative integrators of emerging technologies, dynamic teachers, and developers of specialized teams of Soldiers. Warrant officers are leaders with the extensive professional experience and the technical knowledge to serve as role models and mentors for junior officers and NCOs. That will not change as we implement the FAA.

I vividly remember the very first time a warrant officer coached me away from a bad decision. It helped me gain a new perspective and made me expect only the best from my warrant officers. The more senior I have become, the more heavily I have relied on the quality advice and technical expertise of our warrant officers. Every general officer, colonel, and sergeant major, to name a few, shares in that experience. That will not change as we implement the FAA. If anything, the future holds more advanced systems and technology that must be integrated, operated and protected requiring the skills of an expert—the warrant fficer!

George Santayana, the Spanish American philosopher and essayist famously said, "The difficult is that which can be done immediately; the impossible is that which takes a little longer." We have always reserved "the impossible" for our warrant officers. That will not change as we implement the FAA.

This edition is a special thanks to our warrant officers for their counsel, leadership, and service. It is dedicated to you. Thank you in advance for the huge changes you are about to make to the Signal Regiment. Your service has made our Army and Regiment the best in the world!

**Pro Patria Vigilans!**

U.S. Army Signal Center of Excellence
Fort Gordon

## Command



## Editorial Staff



By Order of the Secretary of the Army:
**GEORGE W. CASEY JR.**
*General, United States Army*
*Chief of Staff*

Official:
JOYCE E. MORROW
*Administrative Assistant to the Secretary of the Army*
0000000

*Army Communicator* (ISSN 0362-5745) (USPS 305-470) is published quarterly by the U.S. Army Signal Center, of Excellence at Signal Towers (Building 29808), Room 713 Fort Gordon, Ga. 30905-5301. Periodicals postage paid by Department of the Army (DOD 314) at Augusta, Ga. 30901 and additional mailing offices.

POSTMASTER: Send address changes to *Army Communicator*, U.S. Army Signal Center of Excellence, Signal Towers (Building 29808), Room 713, Fort Gordon, Ga. 30905-5301.

OFFICIAL DISTRIBUTION: *Army Communicator* is available to all Signal and Signal-related units, including staff agencies and service schools. Written requests for the magazine should be submitted to Editor, *Army Communicator,* U.S. Army Signal Center of Excellence, Signal Towers (Building 29808), Room 713, Fort Gordon, Ga. 30905-5301.

This publication presents professional information, but the views expressed herein are those of the authors, not the Department of Defense or its elements. The content does not necessarily reflect the official U.S. Army position and does not change or supersede any information in other official U.S. Army publications. Use of news items constitutes neither affirmation of their accuracy nor product endorsement.

*Army Communicator* reserves the right to edit material.

CORRESPONDENCE: Address all correspondence to *Army Communicator,* U.S. Army Signal Center of Excellence and Fort Gordon, Signal Towers (Building 29808), Room 713, Fort Gordon, Ga. 30905-5301. Telephone DSN 780-7204 or commercial (706) 791-7204. Fax number (706) 791-3917.

Unless otherwise stated, material does not represent official policy, thinking, or endorsement by an agency of the U.S. Army. This publication contains no advertising.U.S. Government Printing Office: 1984-746-045/1429-S.



*Worldwide web homepage address*
*http://www.signal.army.mil/ocos/AC/*
*E-mail: ACeditor@conus.army.mil*

**PB 11-3-1**
**Spring 2011**
**Vol. 36 No. 1**

# Army Communicator

*Voice of the Signal Regiment*

## Table of Contents

### *Features*




*Cover by Billy Cheney*

**Cover:** *Warrant officers come from diverse backgrounds to form an elite corps of leaders at higher levels with more responsibility than ever in the history of the Signal Corps.*

**Join the Discussion** *This is an evolving landscape where your opinion and experiences can have an impact. At the end of articles where you see this icon, you can weigh in and comment on-line.*

# *Signal Regiment needs warrant officers*

My name is Clark and I'm a Soldier.

I am proud to contribute my comments to this issue that is dedicated to our highly proficient warrant officers.

At this time, this field offers a solid opportunity. Opting for the warrant officer corps is a great career choice for any Signal noncommissioned officer who is motivated to accept the challenges of managing the top levels of our networks and information systems.

Signal warrant officers provide the Army and our joint commands an inventory of highly skilled technicians and leaders with the requisite aptitude, training and experience necessary to plan, install, administer, manage, maintain, operate, integrate and secure the strategic, operational and tactical communications infrastructure and voice and data information systems, services and resources in support of wartime and peacetime operations. Signal warrant officers are responsible for the seamless, secure, consistent and dynamic information systems at all levels of command from the fighting platform to the sustaining base in support of Army, Joint and multinational war fighting missions.


Information systems operation, information assurance, and information protection are integral to the command and control of Army and Joint forces in every operation, and thus, are the essential elements of information dominance on the modern battlefield.

Opportunities for qualified enlisted Soldiers from all three components seeking a career as a 250N Network Management Technician, 251A Information System Technician, or 254A Signal Systems Support Technician have never been greater. Requirements for staffing are dramatically increasing in both warrant officer MOSs. If you think you meet the minimum qualifications for either MOS, I encourage you to put together a packet and submit it now! Uncle Sam and the Signal Regiment Need You!

**"My name is Clark, and I'm an Army-proud professional Soldier!"**

Thomas J Clark

*To: CSM Thomas J. Clark*
*As you bring your military career to a close, we the members of the Signal Regiment take this opportunity to express our sincere thanks for your excellent leadership as the Signal Corps Regimental Command Sergeant Major. Every individual who knows you acknowledges that it has been a privilege serving with you* ***as you magnificently represented Signal Soldiers! Thank you for helping us stay focused on caring for our*** *most valuable asset--our Soldiers who perform the Signal mission every day. Thank you for your courage,* ***sacrifices and service to the nation. May God bless and keep you strong in your new endeavors. Trust that we will always remember, "Your name is Clark and you are a Soldier!"***

# REGIMENTAL CWO Todd M. Boudreau

# *Warrant officers positioned to lead revolutionary communications technology changes*

Signaleers,

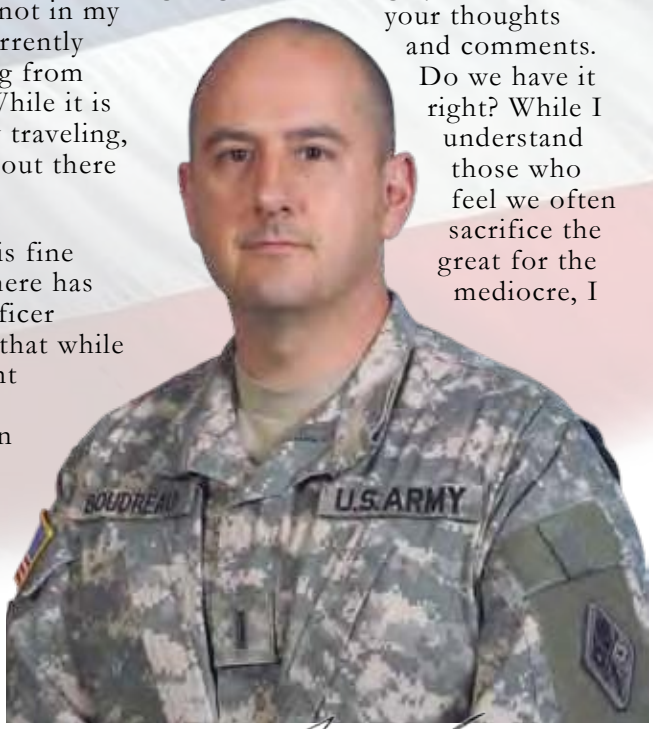
You hold in your hands the first ever warrant officer edition of the Army Communicator. I can personally think of nothing more fitting than to have the first ever warrant officer edition as the lead edition of the Army Communicator for the 151st year of the Signal Regiment. In the next chapter of our Regiment, warrant officers must be focused and positioned to lead the revolutionary charge into uncharted fields of communications technology.

As I write this note, I am once again on the road and not in my office. In fact, I am currently sitting in a C-130 flying from Iraq back to Kuwait. While it is taxing to be constantly traveling, I truthfully love being out there with you!

I asked the staff of this fine publication to see if there has ever been a warrant officer edition and I was told that while there have been warrant officer heavy editions, there has never been an edition that could be entitled with such a distinction. So this is definitely a first.

Within this historic edition you will read a number of articles purposed to educate the force on where we are going with the Signal warrant officer cohort. Numerous changes are taking place, but in truth, nothing too radical. I am merely taking a cohort that I have been raised in, and am extremely proud to serve as one among the visionary leaders guiding it to the next level. Many of these articles are meant to provide you a basis of understanding as well as to evoke response and correspondence.

If you are a mid to senior grade Signal warrant officer, please review your MOS and where it is going. I urge you to share your thoughts and comments. Do we have it right? While I understand those who feel we often sacrifice the great for the mediocre, I challenge anyone to come up with a better solution.



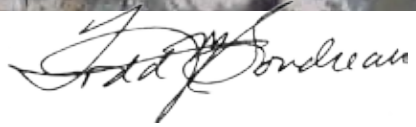

In our technology driven environments the landscape and scenarios are constantly changing. Even if a perfect solution were momentarily available, in a very short span of time, the questions will have changed.

I also solicit comments from senior NCOs and officer leadership. I am wise enough to know that I am not smart enough to know and understand everything. I learn so much from many of you on a daily basis. Please continue providing me with your valuable advice.

Also within this edition you will find articles written by other warrant officers about what they are doing and where we are going. Hopefully you will find this edition to be thought provoking, educational, and of use to you as you meet your mission demands in your varied and complex duties and responsibilities.

I close with a hearty and heart-felt appreciation for all that you do. I always stand a little straighter, a little taller, and a little prouder when I am around you. Thank you for your dedication and service in being ever Watchful for Our Country.

Pro Patria Vigilans!



# Chief of Signal earns second star

*By Wilson A. Rivera*

The 35th Chief of Signal pinned on a second star during a promotion ceremony 16 Feb., 2011 at Fort Gordon.

Following in the legacy of his father, MG (Ret) Robert G. Lynn, BG Alan R. Lynn was appointed to the rank of major general during a promotion ceremony held at Leitner Lake Conference Center.

Like his father, a Signal Corps officer during the Vietnam War, the Chief of Signal continues serving his nation and country as generations of Army officers have done in the past within his family.

"Although I walk in your footsteps, I could never measure up to my father," said Lynn. "As a young boy I saw my father as this great big man; huge shoulders, taking on huge responsibilities."

The newly promoted MG Lynn has made significant accomplishments and achievements during his career, said Director of the Army Staff LTG William J. Troy.

LTG Troy said, he [MG Lynn] changed how the Army does things fundamentally in the world of communications that were never done before--such as connecting channel networks as a captain with the 101st Airborne Division in the largest historic air assault during Operation Desert Storm. He linked NATO switchboards to U.S. switchboard standards, which was a huge achievement since it, again, was never done before.

LTG Troy, chief of staff of III Corps at the time, said he first recognized what type of leader MG Lynn was working as the G-6 Chief Information Officer assigned to the 3rd Signal Brigade in Operation Iraqi Freedom, 2004. He would ask a signal question and the reply was always, "Sir, we're professional, why don't you leave it to us. Don't try understanding it," LTG Troy said.

Photo by Wilson A. Rivera

**Newly promoted MG Alan R. Lynn honors his father MG (Ret) Robert G. Lynn after he donned his father's beret with two stars during a promotion ceremony held 16 Feb., 2001 at Leitner Lake Conference Center.**

As the Chief of Signal for the Regimental Signal Corps and the Signal Center of Excellence, MG Lynn continues his military career redesigning the signal force with the best equipment available. The Signal Corps is training the brightest people on how to get more commercial use out of communications, creating smaller packages with smaller team formations making them much more capable, using the best electronics at the lowest level possible.

"[MG Lynn] is fashioning the signal force to how we are going to do things in the future, how we are going to communicate, and what type of networks are we going to build," said LTG Troy. "How are we going to figure that out? ... We always send our best officers to command at our schools and centers of excellence," said LTG Troy. "They have so much influence on the future of the Army. These students, Soldiers, officers that come through here want to see the model of how it's supposed to be done."

"It was the people on Fort Gordon, the great Soldiers and families that brought me to this promotion, and I'm giving thanks to them for the place I am now," MG Lynn said.

***Wilson A. Rivera*** *is editor of the Signal Newspaper at Fort Gordon.*

# Warrant Officer Corps marks 92nd year

***By CW5 (Ret) David P. Welsh***

The 92nd anniversary of the Army Warrant Officer Corps was observed July 9, 2010.

An act of the U. S. Congress in 1918 established the Army Mine Planter Service as part of the Coast Artillery Corps. Implementation of the act by the Army was published in War Department Bulletin 43, dated 22 July 1918.

A total of 40 warrant officers were authorized to serve as masters, mates, chief engineers, and assistant engineers on each mine planting vessel. Although only one rank of warrant officer was authorized by Congress, in effect, three grades were created because of the varying levels of pay authorized for masters, first mates, second mates, and corresponding levels of marine engineer personnel.

This is also when brown was adopted as the official color of the Army Warrant Officer Corps. The color was a natural offshoot from the brown strands of the burlap bags that Mine Planter Service personnel wore as their insignia of rank. Also, in 1918 the Army opened a school to train mariners at Fort Monroe, Va., commanded by an officer who had graduated for the U.S. Naval Academy.

In World War I, the Coast Artillery Corps was responsible for mine defenses in major ports. Vessels ranging in size from small motor boats to 1,000-ton ocean-going ships were used to lay and maintain minefields. Conflict between Solders and civilian employees who manned these vessels revealed the need to ensure that the vessels were manned by military personnel.

Here are some highlights from the rich history of the Army Warrant Officer Corps:

The National Defense Act of 1920 provided for warrant officers to serve in clerical, administrative and bandleader positions. This act also authorized 1,120 warrant officers to be on active duty. During this time warrant officers were excluded from performing duties from which enlisted personnel were also excluded.

On 12 May 1921, a distinctive insignia was approved for warrant officers. It consisted of an eagle rising with wings displayed, adapted from the Great Seal of the United States. The eagle is standing on two arrows, which symbolize the military arts and sciences. The eagle rising is enclosed within a wreath. Warrant officers of the Tank Corps were the first to wear this new insignia.

In 1936, Army leaders were uncertain about what an Army warrant officer was and whether there was a place for warrant officers in the Army's personnel structure. Although warrant officer rank had been awarded to such specialties as band leaders, marine engineers, field clerks, and pay clerks, the rank had also been used as a reward. The rank was offered to former commissioned officers who no longer met the officer educational requirements and to outstanding enlisted personnel who were too old to be commissioned and who otherwise could look to no further advancement.

In 1940, warrant officers began serving as disbursing agents. Warrant officer appointments began to occur in larger numbers for the first time since 1922. However, overall strength declined due to a significant number transferred to active duty as regular commissioned officers. In 1941, Public Law 230 authorized appointments up to one percent of the total Regular Army enlisted strength. This law also established two pay rates for warrant officers, Warrant Officer Junior Grade (W-1) and Chief Warrant Officer (W-2). One other benefit of Public Law 230 was the authorization of flight pay for those involved in aerial duties.

In November of 1942, the position of warrant officer was defined by the War Department in the rank order as being above all enlisted personnel and immediately below all commissioned officers. January 1944 saw the authorization of appointment of women as warrant officers and by the end of WW II, 42 female warrant officers were serving on active duty. Warrant officers were filling 40 different occupational specialties by early 1946 and approximately 60 specialties by 1951.

In January 1944, the appointment of women as warrant officers was authorized. In 1949, the Career Compensation Act brought about two new pay rates for warrant officers. The designations of Warrant Officer Junior Grade and Chief Warrant Officer were retained; the grade of chief warrant officer was expanded with the addition of pay grades of W3 and W4.

In 1953, the inceptions of the Warrant Officer Flight Program lead to the training of thousands who later became helicopter pilots during the Vietnam War.

In 1954, The Warrant Officer Personnel Act of that year established Warrant Officer grades W1 through W4, and officially eliminated the Mine Planter Service.

On 21 January 1957, a new warrant officer concept, resulting from a Department of the Army study, was announced and provided the following guidelines:

1. The need for warrant officers
2. The warrant officer category would not be considered a reward or incentive.
3. The first published definition for warrant officers was established in AR 611-112 and defined the warrant officer as follows:

"The warrant officer is a highly skilled technician who is provided to fill those positions above the enlisted level which are too specialized in scope to permit effective development

**(Continued on page 6)**

**(Continued from page 5)**

and continued utilization of broadly trained, branch qualified commissioned officers."

In July 1972, Army warrant officers began wearing newly designed silver rank insignia with black squares, where one black square signified WO1 and two through four black squares signified CW2 through CW4. Also in 1972, a tri-level education system had been established and provided formal training at the basic or entry level for warrant officers in 59 occupational specialties. The educational system further provided intermediate level formal training in 53 specialties and formal training for 27 specialties at the advanced level.

In 1978, Army National Guard and Army Reserve warrant officers were integrated into the Army Professional Development System. This satisfied the need for qualified, highly trained warrant officers to access to the active Army rapidly in times of emergency.

In 1982, the Warrant Officer Training System was established by the U. S. Army Training and Doctrine Command. WOTS consisted of three levels "Entry," "Advanced" and "Senior."

On 1 October 1984, all direct appointments of Army warrant officers ceased by direction of the Army vice chief of staff. A Warrant Officer Entry Course was established at Fort Sill, Okla. In the mid-1980s a Warrant Officer Entry Course-Reserve Component was established in the Warrant Officer Training Branch at the Army Reserve Readiness Training Center at Fort McCoy, Wis. This course evolved into Warrant Officer Candidate School-Reserve Components and it was conducted until September 1994 when

all Warrant Officer Candidate School courses were consolidated and transferred to the Warrant Officer Career Center, Fort Rucker, Ala.

In 1985, Army leaders developed a new definition of the warrant officer that encompassed all warrant officer specialties.

"An officer appointed by warrant by the Secretary of the Army, based upon a sound level of technical and tactical competence. The warrant officer is the highly specialized expert and trainer, who, by gaining progressive levels of expertise and leadership, operates, maintains, administers, and manages the Army's equipment, support activities, or technical systems for an entire career."

The Defense Authorization Act for Fiscal Year 1986 amended Title 10 of the United States Code to provide that "Army chief warrant officers shall be appointed by commission." The primary purpose of the legislation was to equalize appointment procedures among the services. Chief warrant officers of the Navy, Marine Corps, and Coast Guard had been commissioned for many years. Contrary to popular belief, the commissioning legislation was not a TWOS recommendation but a separate Army proposal. Further clarification of the role of an Army warrant officer, including the commissioned aspect, was found in Army Field Manual 22-100.

"Warrant officers are highly specialized, single-track specialty officers who receive their authority from the Secretary of the Army upon their initial appointment. However, Title 10 U.S.C. authorizes the commissioning of warrant officers (WO1) upon promotion to chief warrant officer (CW2). These commissioned Warrant Officers are direct representatives of the president of the United States. They derive their authority from the same source as commissioned officers but remain specialists, in contrast to commissioned officers, who are generalists. Warrant officers can and do command detachments, units, activities, and vessels as well as lead, coach, train, and counsel subordinates. As leaders and technical experts, they provide valuable skills, guidance, and expertise to commanders and organizations in their particular field."

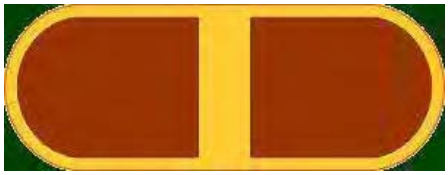
In a 1988 message, Army established that, pending submission and approval of the new rank of CW5 that Warrant Officers selected by a Department of the Army board and designated as master warrant officer (MW4) would be senior to all Warrant Officers in the grade of CW4. The MW4 continued to be paid at the W-4 pay grade. In December 1988 the first Master Warrant Officer Training Course graduated and the first thirty CW4s were designated as Master Warrant Officers.

In 1989, A Warrant Officer Management Act proposal was submitted by the U.S. Army Warrant Officers Association on behalf of the Army to the Congress. In 1991 the WOMA proposal was considered by the Congress and it was incorporated into the National Defense Authorization Act for FY 1992. Six key provisions were enacted based on the Warrant Officer Management Act as signed by the President in December of 1991, these were as follows:

- A single promotion system for Warrant Officers.
- Tenure requirements based on years of Warrant Officer Service.
- Establishment of the grade of chief warrant officer five with a 5 percent cap on the number of warrant officers on each service's active duty list at any one time.
- Selective mandatory retirement boards for retirement eligible warrant officers.

In February 1992, the Warrant Officer Management Act provisions went into effect.

On 1 October 1992, the appointment of Army warrant officer candidates to WO1 was established as the graduation date from Warrant



Officer Candidate School. Prior to that date, WOC were not appointed until completion of the then Warrant Officer Technical and Tactical Certification Course for their military occupation specialty. Since WOTTCC for various MOS were of various lengths, the length of time spent as a WOC varied greatly.

On 9 July 2004, new chief warrant officer five insignia and wear of Army officer branch insignia and branch colors were announced as uniform changes for Army warrant officers. The new chief warrant officer five insignia was a silver-colored bar, 3/8 inches in width and 1-1/8 inches in length, with a black line in the center of the bar. This aligned the Army CW5 Insignia with that of the Navy and the Marine Corps; particularly it makes the rank more readily recognizable in joint operations. Ceremonial Warrant Officer Insignia Change and Flag Ceremonies were held at various locations on 9 July and other dates. This change in effect relegated the brass Eagle Rising insignia into Warrant Officer Corps history.

On 14 October 2005, new Army Warrant Officer Definitions were published in Department of the Army Pamphlet 600-3. This pamphlet includes the career development of warrant officers, The new official definition of an Army warrant officer is:

"The Army warrant officer is a self–aware and adaptive technical expert, combat leader, trainer, and advisor. Through progressive levels of expertise in assignments, training, and education, the warrant officer administers, manages, maintains, operates, and integrates Army systems and equipment across the full spectrum of Army operations. Warrant officers are innovative integrators of emerging technologies, dynamic teachers, confident war fighters, and developers of specialized teams of Soldiers. They support a wide range of Army missions throughout their career. Warrant officers in the Army are accessed with specific levels of technical ability. They refine their technical expertise and develop their leadership and management skills through tiered progressive assignment and education.

The Department of the Army Pamphlet follows the above general definition with additional definitions for each warrant officer grade, WO1 through CW5.

On 11January, 2008 - The assistant Secretary of the Army (Manpower and Reserve Affairs) issued a memorandum authorizing 30 years of active service for all Regular Army warrant officers of any grade. Previously only Regular Army chief warrant officers five were allowed 30 years of active warrant officer service.

On 26 April, 2010, H.R. 5136, National Defense Authorization Act for Fiscal Year 2011, was introduced in the U.S. House of Representatives. Section 507 of the bill would amend Section 571(b) of Title 10, U. S. Code to provide that appointments in the grade of regular warrant officer, W-1, be made by the regulation issued by the Secretary of the Military Department and that these appointments shall be made by the President except that appointments in that grade in the Coast Guard shall be made by the Secretary concerned. The Bill was pending in Congress as of June 2010.

As of 30 September 2010, the Army warrant officer cohort is comprised of about 24,550 men and women.

- Active Army - 62%
- Army National Guard - 32%
- Army Reserve - 12% (not counting members of the Individual Ready Reserve also available for mobilization)
- Technical Branch warrant officers - 65.4%
- Aviation warrant officers - 34.6%
- Percentage of the Army - 2%
- Percent of the officer corps - 14%
- Branches with warrant officers assigned - 17
- Number of warrant officer military occupation specialties - some 70

The above information is extracted from the online Warrant Officer History maintained and frequently updated by the non-profit Warrant Officers Heritage Foundation. A more detailed history can be found on the Foundation's website at www.usawoa.org/WOHERITAGE/. Click on the warrant officer history link at the top. The online history contains many pictures, links to copies of original documents, and information about warrant officers with historical significance.

***CW5 (Ret) David P. Welsh*** *served in the Reserve and on active duty, culminating in his assignment as the Reserve Warrant Officer Policy Integrator in the Office of the Chief Army Reserve in the Pentagon. He retired from active duty in 1998 with some 42 years of combined Reserve and active duty service. He was national president of the U.S. Army Warrant Officers Association from 1988 to 1992 and a member of their full-time staff from 1998 to 2003. CW5 Welsh founded the Warrant Officers Heritage Foundation in the summer of 2003 and currently serves as president and a board of directors member.*

## Acronym QuickScan

**CWO –** Chief Warrant Officer
**MOS –** Military Occupation Specialty
**NDAA –** National Defense Authorization Act
**TRADOC –** U. S. Army Training and Doctrine Command
**WOC –** Warrant Officer Candidates
**WOCS –** Warrant Officer Candidate School
**WOJG –** Warrant Officer Junior Grade
**WOMA –** Warrant Officer Management Act
**WOTS –** Warrant Officer Training System
**WOTTCC –** Warrant Officer Technical and Tactical Certification Course

# Warrant officer accessions

*By CW5 Todd M. Boudreau and CW4 William Winkler*

The career of an Army warrant officer is a challenging and rewarding one with as many intangible as tangible benefits The U.S. Army warrant officer program provides a number of benefits to include world-class training and education, higher pay, faster promotion potential, extended career opportunities, and challenging assignments.

## USAREC Warrant Officer Branch Missions

The Warrant Officer Branch Missions, U.S. States Army Recruiting Command has the responsibility to recruit highly qualified applicants to serve as Army warrant officers. This team consists of several warrant officers and a small number of enlisted recruiters who actively conduct warrant officer recruitment briefings around the globe.

Additionally, they receive and process every warrant officer application before passing it to the warrant officer boards section. Application processing includes receipt, quality assurance, and waiver processing. Once the packet is presented to the boards branch, a copy is sent to the proponent.

The Warrant Officer Branch Missions also maintains the USAREC's Warrant Officer Recruiting Information Web Site (http://www.usarec.army.mil/hq/warrant/index.htm). This website offers a one-stop shop for information about Army warrant officer recruiting.


Photo by Larry Edmond

**CW5 Todd M. Boudreau, Regimental chief warrant officer, provides program information to potential warrant officers during a recruiting session February 2011 in the Signal Towers at Fort Gordon, Ga.**

## Branch Warrant Officer Personnel Developers (Proponent Managers)

Each Army branch that includes warrant officers has the added responsibility to establish the technical prerequisites for each warrant officer military occupational specialty. These prerequisites are submitted to USAREC and posted to the above website. They are also used as the basis of qualification for warrant officer accessions applicants. Personnel developers review every warrant officer accessions packet for their branch and provide an official memorandum rating the applicant either qualified to compete on a warrant officer accessions board for the specified warrant officer MOS or not qualified due to one

or more deficiencies. Every deficiency is identified on this memorandum and a copy is returned to the applicant so corrections may be made, if possible. Finally, if the packet contains a waiver request for a general prerequisite, the branch makes a recommendation for or against approval based on the needs of the Army and mitigating circumstances specific to the applicant and/or MOS.

## The Process

The warrant officer accessions process is very similar to that used to access branch officers. Candidates assemble an accessions packet which contains specific information used to assess the candidate's qualifications and provide accessions board members adequate information on which to conduct a best-qualified board. Board packets typically include a number of required documents along with supporting documentation. Required documents include:

1. USAREC Application Checklist
2. DA Form 61 (Application for Appointment)
3. Letters of Recommendation
4. Resume
5. ERB (Enlisted Record Brief)
6. OMPF (Last 10 years of NCOERS and/or AERs in order from newest to oldest)
7. College Transcripts (if applicable and required)
8. DA Form 6256 (AFAST Form from Test Center for MOS 153A only)
9. Official Photo

Typical supporting documentation includes:

10. Memorandum from security manager indicating security clearance
11. Physical
12. DA Form 160-R (Application for Active Duty)
13. Statement of Understanding
14. Waivers (e.g., Moral, Age, AFS, APFT, and Branch Prerequisite)
15. Conditional Release (Reserves & Other Services)

The approval authority for moral waivers is Human Resources Command, for age and AFS waivers is DA G1, for APFT waivers is DA G3, and for branch specific prerequisite waivers is the applicable proponent.

Letters of recommendation must not be older than 12 months. For most applicants, three LORs are required: (1) an LOR from the applicant's current Company Commander (or first UCMJ level), (2) an LOR from the applicant's current Battalion Commander (or second UCMJ level), and (3) an LOR from a branch senior warrant officer (CW3 to CW5); not all branched require this third LOR (Signal does not). Although a letter from a senior Signal warrant officer is not required, it will add weight to the overall strength of the packet. In its place, and of much greater value, is a letter from an IT professional (e.g., S6, communications GS-13, or even a senior Signal warrant officer), with personal knowledge of the applicant's technical skills and leadership potential.

Additionally, though not a requirement nor a prerequisite, awards and the following certification also provide great weight to the overall strength of the packet and should be cited in the resume and included in the packet: MCSA, CCNA, MCSE, CCNP, CCSP, CCIE, and the various Information Assurance and Computer Network Defense certifications (e.g., Net+, Sec+, CISSP, etc.).

## The Prerequisites

Prerequisites fall into two categories: (1) those every candidate must meet and (2) those the specific branch establishes. Branches may also list mandatory and preferred prerequisites.

In general, there are ten general prerequisites every warrant officer applicant must meet in order to compete on a warrant officer accessions board. Some prerequisites may be waived, and others may not. These prerequisites include:

1. U.S. Citizenship (No Waivers)
2. GT score of 110 or higher (No Waivers)
3. High school graduate or have a GED (No Waivers)
4. Secret security clearance (Interim acceptable for application)
5. Pass the standard 3-event APFT (Can apply for waiver)
6. Meet height/weight standards (No Waivers)
7. Pass appointment physical (Class 1A flight physical for 153A)
8. Have 12 months remaining on current enlistment contract
9. Have less than 12 years AFS at the time of submission (Can apply for waiver)
10. Be between the ages of 18 and 46 (33 for 153A)

Signal specific mandatory prerequisites include:

1. SGT (E5) or above (May be waived for USAR or ARNG Soldiers)
2. A minimum of 36 months of rated time documented in NCOERs (May be waived for USAR or ARNG Soldiers when Soldier's civilian employment includes verifiable leadership/managerial responsibilities)
3. Four years of documented practical experience in the tasks and skills specified for each MOS on the USAREC website noted above
4. A minimum of 6 SH of college level English (neither speech nor public speaking courses meet this requirement) from an accredited academic institution; successful completion of the CLEP general examination in English or an Associate degree or higher (when the preponderance of college credit

**(Continued on page 10)**

(Continued on page 9)

is from college instruction vice credited experience) are the only acceptable alternatives

Signal specific preferred prerequisites include:
1. Advanced Leader Course (BNCOC) graduate
2. Attain 12th grade equivalency on the Reading Grade Level portion (vocabulary and comprehension) of the Test of Adult Basic Education-A (TABE-A, or TABE-D)
3. Sec+ certified

Prerequisite waivers are mostly based on the needs of the Army; if a branch has difficulty meeting its accessions mission, a waiver is more likely to be approved than a branch that has more than adequate fully qualified applicants. Signal historically falls into the latter category.

Regarding APFT Waivers, the revised AR 350-1 (dated 18 Dec 09 with an effective date of 18 Jan 10) paragraph 3-12, i(3) states:

Candidates enrolling in WOCS or OCS must pass the standard three-event APFT as an enrollment requirement; the alternate APFT is only authorized with HQDA, DCS, G-3/5/7 approval. The walk event on the alternate APFT is the only authorized alternate event used as an enrollment requirement. The Soldier must also be able to walk the 6.2 mile ruck march for WOCS or the 12 plus miles for OCS with 48 lbs. or more in their rucksack within school time parameters. If a Soldier enrolling in WOCS or OCS fails the initial APFT, the Soldier will be denied enrollment but allowed one retest with a subsequent class. Soldiers failing the second APFT will be considered ineligible for enrollment and must reapply for OCS or WOCS selection.

Accordingly, the only APFT waiver requests that are eligible for consideration are those requesting a waiver for the walk event; the push up and sit up events cannot be waivered under these guidelines.

To date, mandatory Signal prerequisites have not been waived; applicants must meet each of these prerequisites to be qualified to compete on a selection board. These prerequisites have been established to ensure only the best qualified Noncommissioned Officer applicants compete for the limited number of warrant officer positions. Additionally, they ensure applicants have the requisite background and Signal experience required to successfully pass the applicable MOS producing Warrant Officer Basic Course. Our current Signal WOBC are extremely academically challenging. They are between 25 and 32 weeks long and are, for all but one training day, focus entirely on complex information technology solutions. Students require a broad and solid base of IT knowledge, skills, abilities, and experiences to be successful.

Non-Army personnel may also apply. The first hurdle is to ensure the 110 GT score has been meet. Air Force, Navy, and Coast Guard Service members who would like to get their scores converted need to first ensure that the individual qualifies with an Army GT of 110. If the Armed Services Vocational Aptitude Battery or Armed Forces Classification Test or in-service ASVAB was administered prior to 1 July 2004, Air Force members need a minimum General (G) score of 64 while Navy and Coast Guard Service members must combine their Arithmetic Reasoning (AR) and Verbal (VE) and have a minimum combined score of 109. If the ASVAB or AFCT was administered after 1 July 2004, Air Force members need a minimum General (G) score of 70 while Navy and Coast Guard service members must combine their Arithmetic Reasoning (AR) and Verbal (VE) and have a minimum combined score of 111. Marines needing ASVAB scores converted must contact: HQMC M&RA MPP-50 Testing.


**Soldiers selected into the Signal Warrant Officer Corps enjoy world-class training on par with advanced civilian industrial standards.**

The USAREC website contains all of the information required to include mailing addresses for verification of the above prerequisite as well as how to secure a memorandum granting approval of separation from the service member's current service contingent upon selection into the warrant officer program, taking the Army 3-event physical fitness test, etc.

Finally, it is significant to note that since Soldiers are formally separated from the Army and subsequently conditionally appointed as a WO1 upon graduation from the WOCS, students who fail to pass the WOBC are administratively separated from the Army. If they desire to continue to serve in the Army, they must find an Army recruiter and may enlist again back into the Army – under the needs of the Army; there is no guarantee nor should there be any expectation that an individual will be enlisted back into the Signal Regiment, into their past MOS, nor in their last enlisted grade.

## Board Procedures

Once an application packet has successfully made it through the review process and has been found qualified to appear before an accessions board, it is logged and maintained by the warrant officer boards section of USAREC. Not all MOS are boarded every month; larger MOS are boarded more often than MOS of smaller population. Signal accessions packets are boarded three times a year; January, May, and September.

Board members are senior warrant officers of the same branch from which packets are being boarded. Members receive several briefings and even conduct a practice board; this board is run as a secretariat Department of the Army promotion board and maintains the same standard of credibility as such. During the board, members are only able to view one packet at a time; the packet must be voted for the member to move on to the next packet. Voting is conducted similar to a promotion board in that members take a "whole Soldier" approach and vote 0-6 with the ability to add a plus (+) or minus (-) for further effect.

Once an entire MOS has been boarded, the warrant officer boards section establishes a numerical Order-of-Merit List (OML). This OML is used to feed one of three categories: (1) Fully Qualified – Selected (FQ-S) individuals are those who made the selection quota and will be processed into the Warrant Officer Program, (2) Fully Qualified – Not Selected (FQ-NS) individuals are those who were not selected on their first look by a selection board, and (3) Not Competitive – Not Selected (NC-NS) individuals are those who were not selected on their second look by a selection board.

FQ-S individuals usually receive orders to attend the Warrant Officer Candidate School approximately four to six months after their selection; these individuals must have a current qualified appointment physical (with no disqualifying medical condition IAW AR 40-501) and security clearance verification when they report to Fort Rucker for WOCS. FQ-NS individuals are automatically boarded by the next warrant officer candidate selection board which considers their requested warrant officer MOS; such individuals are encouraged to update their application as appropriate. NC-NS individuals have their application returned to the current address listed in block #19 on the DA Form 61 and may not reapply for one year from the date on their DA Form 61 (Application for Appointment), page 3, block 42.

## After Selection

Once a Soldier is selected on an Army warrant officer selection board, one more significant decision must be made before accepting this great honor. It is expected that all WO1s be assigned to a deploying unit, even if a Soldier has a number of deployments as an enlisted Soldier. Muddy boots assignments and boots-on-ground time as a warrant officer is important to solidify the training received at the Warrant Officer Basic Course as well as to establish credibility. I recommend that every selected Soldier think this through and discuss it with their family. If this is going to be a problem it is better identified up-front.

Many candidates spend over $1,000 purchasing clothing items that they already own. If your uniform items are still serviceable do not feel that you have to replace them. However, if they are serviceable but do not fit properly, you must have clothing that is sized appropriately. There are two packing lists. One that has mandatory clothing items and another that has optional items. You must have everything on the mandatory items list. This should be your entire initial issue. Do not bring extra unless authorized on the list. If it specifies a color, it must be that color (i.e. white underwear).

On the optional items list you should only bring those things that will make you more comfortable. Many candidates suggest bringing a Camel Back that will be used for the six-day field exercise, long underwear for winter months, and females should bring pumps for the reception. There is also a list of mandatory items that includes toiletries and office supplies. Keep toiletries to a minimum to avoid cluttering your personal security area. You may want to wait on office supplies until you arrive at Fort Rucker, Ala. Previous students may have left behind many of the items that you will need such as index cards, one-inch rings, medical tape, two-sided tape, etc. You can always purchase them here at Clothing Sales or the Shoppette if there are no extras in the class admin room.

The next challenge is to prepare for and successfully complete the Warrant Officer Candidate School. This course provides a very important part of our

**(Continued on page 12)**

(Continued from page 11)

warrant officers' training that ensures each has the basic understanding of what is expected of an Army officer.

A great link with information that prepares a potential warrant officer is http://usacac.army.mil/cac2/WOCC/wocs.asp. Note that some Distributive Learning is required prior to WOCS attendance. Once a Soldier has enrolled in ATRRS for Course 911-09W, the Soldier must access the training at https://www.bb.wood.army.mil by logging in with their AKO short name and password. Ensure you plan accordingly. Failure to complete the dL portion of WOCS will result in a delay in start date or dismissal from the course. Note also that there is an electronic copy of the WOC SOP on the dL site. There are many procedures that must be followed at WOCS that are covered in the SOP. The more one knows, the easier the transition. Many mistakes candidates make while in WOCS are covered in the WOC SOP.

After successful completion of WOCS, the newly (though conditionally) appointed WO1 will be welcomed to Fort Gordon, Ga., the home of the Signal Regiment, for technical training in the appropriate WOBC. Students are challenged to learn many things that will prepare them for their first assignment. The recommended link for use in preparation for WOBC is: https://www.us.army.mil/suite/page/133249.

We ask that Soldiers be patient for 60 to 90 days to allow us to get schedules for WOCS and WOBC completed. If a Soldier has not heard from the Signal Regiment at the end of 90 days, the Soldier should contact the Regimental chief warrant officer.

## Conclusion

This provides a brief synopsis of the Army Warrant Officer Accessions Program with special emphasis on Signal. The Army Warrant Officer Program not only provides the Army with premier technical officers who are "self aware and adaptive technical experts, combat leaders, trainers, and advisors," but it also provides enlisted Soldiers who are more inclined to follow such a path the opportunity to perform their core technical duties longer, join a small elite corps of professionals who want to make a difference, who want to advance their careers, who want to stay in their career fields, who want better retirement pay for family, and who have the technical capabilities to do more.

## Acronym QuickScan

**AER** – Academic Evaluation Report
**AFCT** – Armed Forces Classification Test
**AFS** – Active Federal Service
**ALC** – Advanced Leaders Course
**APFT** – Army Physical Fitness Test
**ARNG** – Army National Guard
**ASVAB** – Armed Services Vocational Aptitude Battery
**BNCOC** – Basic Noncommissioned Officer Course
**CCIE** – Cisco Certified Internetwork Expert
**CCNA** – Cisco Certified Network Associate
**CCNP** – Cisco Certified Network Professional
**CCSP** – Cisco Certified Security Professional
**CISSP** – Certified Information Systems Security Professional
**CLEP** – College Level Examination Program
**DL** – Distributive Learning
**ERB** – Enlisted Record Brief
**FQ-NS** – Fully Qualified – Not Selected
**FQ-S** – Fully Qualified – Selected
**GED** – General Educational Development
**GT** – General Technical
**HQDA, DCS** – Headquarters Department of the Army, Deputy Chief of Staff
**IAW** – In Accordance With
**IT** – Information Technology
**LOR** – Letters of Recommendation
**MCSA** – Microsoft Certified Administrator
**MCSE** – Microsoft Certified Systems Engineer
MOS – Military Occupational Specialty
**NC-NS** – Not Competitive – Not Selected
**NCOER** – Noncommissioned Officer Evaluation Report
**Net+** – CompTIA Network+ Certification
**OCS** – Officer Candidate School
**OML** – Order-of-Merit List
**OMPF** – Official Military Personnel File
**PSA** – Personal Security Area
**Sec+** – CompTIA Security+ Certification
**SOP** –Standard Operating Procedures
**TABE** – Test of Adult Basic Education
**WOCS** – Warrant Officer Candidate School
**UCMJ** – Uniform Code of military Justice
**USAR** – United States Army Reserve
**USAREC** – United States Army Recruiting Command
**WO1** – Warrant Officer 1
**WOBC** – Warrant Officer Basic Course
**WOC** – Warrant Officer Candidate
**WOCS** – Warrant Officer Candidate School

# Young Signal warrant officer living lifelong dream to be a Soldier

**WO1 Elizabeth Tysall at Fort Gordon, Ga. in 2011.**

*By CW5 Todd M. Boudreau*

If you want to see an example of the Signal warrant officer today take a look at WO1 Elizabeth Tysall to get a picture of who they are, whence they come and to what they aspire.

WO1 Tysall says, "Since I was a little girl, I have always wanted to serve my country."

She says, provocative and entertaining narratives stories from her father, grandfather, and uncles about their military exploits dumped fuel onto the smoldering fire that burned within her from the earliest point she can remember. Studying the military seemed a natural adjunct to life all around her. She read voraciously of epic battles and various military campaigns. Even the Bible provided vivid descriptions of battles and the warriors who waged victorious campaigns.

As a child WO1 Tysall said she and her siblings would play cavalry. There was always a huge land dispute, reservation problem or other such conflict or battle to resolve. They constantly manufactured a war.

It surprised no one that as soon as she was old enough she set out to be a Soldier. The week after graduation from high school, she went directly to basic training. That is when she marks the start of her true relationship with the Army. From that very moment she says knew that this was the job for her.

WO1 Tysall resolutely states, "Our country needs a strong and successful military. And that military needs leaders who enjoy their jobs…who are dedicated to doing the right thing, regardless of the impact on their personal circumstances."

## Military Background

Her diligence earned her rapid promotions. She quickly moved into the ranks of the noncommissioned corps. From September 2003 until February 2005, she served as a watch NCO and emergency action cell controller in the U.S. Army Europe G-3, Heidelberg, Germany. She was responsible for the decoding of classified mission-relevant traffic in support of Operations Iraqi Freedom and Enduring Freedom. SGT Tysall revamped the Read Book for the USAREUR G-3, which became widely used by other Directorate Staff Officers. She also monitored Army and Joint level sites for mission relevant traffic. SGT Tysall was selected as the USAREUR NCO of the month for January 2005.

In February 2005, she assumed the position of operations NCO, Headquarters and Headquarters Company USAREUR, Heidelberg. During her tenure at HHC she was responsible for all training functions that were executed by HHC USAREUR. Additionally, she developed and maintained tracking systems for MEDPROS, and Family Care Plans. As the USAREUR Schools NCO, SSG Tysall was responsible for the ATRRS functions of more than 700 USAREUR Soldiers.

SSG Tysall moved to the U.S. Central Command in September 2006 and was subsequently trained as a Global Command and Control Systems administrator. As a GCCS administrator, she built and maintained the GCCS Server Enclave at CENTCOM, and was selected to serve as the CENTCOM Forward Headquarters GCCS NCOIC. While at CFH, she implemented a physical fitness program for the Joint service members within the CENTCOM J-6. In August 2008, she was selected to serve on the commander's communications team.

From September 2008 until she reported for training at the Warrant Officer Candidate School, she was employed on numerous missions throughout the CENTCOM Area of Responsibility including Europe, North America, Africa, and Asia. During this time, she led advance communications missions, served as the personal communicator, field tested innovative communications equipment and techniques, and was involved in the development and refinement of classified on-the-move communications mediums; all in pursuit of constant global connectivity for the commander, USCENTCOM.

WO1 Tysall's military education as an enlisted Soldier includes the Warrior Leaders Course, the Advanced Leaders Course, and the Battle Staff NCO Course. She was the Distinguished Honor Graduate for Warrant Officer Candidate Course, class 10-018. She is currently in training at the Signal Warrant Officer Basic Course. She also attended the Air Force's Global Command and Control Systems Administrators Course, is Department of the Army Level II certified in Information Assurance, and has completed the

**(Continued on page 14)**

(Continued from page 13)

National Security Agency's COMSEC Custodian and DIAS Courses. She is currently pursuing a Bachelor of Science degree in Information Technology Management from American Military University.

WO1 Tysall's military awards and decorations include the Defense Meritorious Service Medal, Meritorious Service Medal, the Army Commendation Medal, the Army Achievement Medal with Silver Oak Leaf Cluster, the Global War on Terrorism Expeditionary Medal, the Global War on Terrorism Service Medal, the Driver's Badge, and the German Schutzenschnur Bronze Badge. She was named the USCENTCOM Army NCO of the Year for 2006.

WO1 Tysall has two sons, Trevor, born 2001 and Thomas, born 2005.

## What They Aspire to Accomplish

Following is an excerpt from a WOCS writing assignment entitled 'My Role as a Military Officer,' in which W01 Tysall succinctly ascribes her aspirations: "The people in our great nation look to the officers in our military for confidence, strength, and courage. They expect and deserve individuals with good character, those who can set and enforce standards, and those who are willing to lead the young Americans who enlist in our Armed Services to success.

As everyone knows, we are a nation at war. It is not a quiet conflict, not one fought only on the battlefield, not one only fought in Washington, D.C.

This current set of wars is being debated in living rooms throughout the country by families fueled by what the media feeds our countrymen. It is being contested in our nation's capital by our elected officials. It is being challenged by our global neighbors. Soldiers, Airmen, Sailors, and Marines who comprise our fighting forces are fighting those engagements in such arena as well as on the ground, in the air, and on the sea. Depending on the current mood of the media, our countrymen might look at our fighting forces as monsters, part of a terrible death and destruction device; or they could be lauded as heroes, leading the impressionable field of American volunteers who choose to serve this great nation.

"Keeping the members of our fighting forces safe and secure is the most important task of any military leader. It is a leader's responsibility to train and protect America's volunteer force. The leader must inspire confidence in those who are in their charge. Setting, then enforcing standards is an important way to do this.

A leader must analyze the mission and base their direction on that mission. Junior leaders have an even more pronounced supporting role as they will use this knowledge to advise and inform their commander. All activities and functions of a unit are the ultimate responsibility of the most senior leader or commander.

This individual must guide subordinates and lead them to success. The intermediary leaders will support this endeavor by seeking the tactical and technical attributes of the entire group and situation. Then they will mitigate the holes that manifest. These people will also produce a trustworthy environment for all personnel.

It is imperative that all subordinates trust and have confidence in their leadership. This fosters a

**Warrant officer candidates stand in formation at 1st Warrant Officer Company, Warrant Officer Candidate School.**

positive foundation for open communication and streamlines the entire process of getting things done. Those subordinate to the leaders will have a much easier time completing tasks when they are doing so for concerned and informed leaders. The leader needs to be someone that the group can count on for direction and strength. Becoming that leader is essential to mission success.

There are many different reasons to become an Officer in the United States Army. For me, it will be the best vessel to take care of our nation and the young men and women who volunteer to help defend it. It will also bring me closer to the realization of a personal desire formed in my childhood. I have always given my best. I am a driven human being. This behavior will not stop.

My ambition will not wane. Mission accomplishment is what I have to offer. My troops will be well-conditioned and confident, because I will set the example. I will listen to them and be the leader on which they can depend. I do not only want to be an officer. I need to be an officer. This is what I have been called to do for the American warriors who keep our great nation free."

## The Making of a 255A

WO1 Tysall is currently enrolled in her Warrant Officer Basic Course and is scheduled to graduate with MOS 254A. You can read more in the issue about the evolution of the MOS 254A to include its inception, past history, current status, and future repurposing to MOS 255A. In brief, MOS 251A and MOS 254A are in the process of merging. As such, both WOBC programs of instruction were modified and as of 1 October 2009, they were both extended to 32 weeks of training and have the exact same course content.

MOS 255A will be the Army's premier cyberspace content technician. They will be charged with establishing and maintaining the ability to collect, process, store, secure, search for and discover, retrieve, and disseminate information utilizing the application layer environment of the Army's portion of the cyberspace domain; they enable information dissemination management/content staging (IDM/CS) in order to perform the required information management/knowledge management (IM/KM) functions supporting combat information superiority and decision dominance. In short, the 255A will own cyberspace content management (CyCM). See the article entitled "The Army's expert cyberspace content technician – MOS 255A" for a more in-depth understanding of this new MOS.

## Conclusion

Although WO1 Tsyall stands above many of her peers, she is indicative of the level of professionalism, leadership, and technical expertise our newest WO1s bring to the fight. While we have always had some candidates assessed earlier in their career as well as some a little later, the average Signal warrant officer accessions candidate is a staff sergeant with 10 years Active federal service.

When it comes to leadership, commanders should look at newly appointed warrant officers similarly to newly appointed lieutenants. However, in areas of general military leadership, knowledge, and technical abilities, commanders should remember that these new WO1s are prior enlisted NCOs. As such, commanders should mentor them in their new officer roles as they would a second lieutenant, but expect great things from them in technical and tactical relevance.

## Acronym QuickScan

**ATRRS** – Army Training Requirements and Resources System
**CFH** – CENTCOM Forward Headquarters
**COMSEC** – Communications Security
**CyCM** – Cyberspace Content Management
**DIAS** – Distributed INFOSEC Accounting System
**GCCS** – Global Command and Control Systems
**IDM/CS** – Information Dissemination Management/ Content Staging
**IM/KM** – Information Management/ Knowledge Management
**MEDPROS** – Medical Protection System
**MOS** – Military Occupational Specialty
**NCO** – Noncommissioned Officer
**NCOIC** – Noncommissioned Officer in Charge
**HHC** – Headquarters Company
**USAREUR** – U.S. Army Europe
**USCENTCOM** – U.S. Army Central Command
**WOCS** – Warrant Officer Candidate School

# Today's cohort is definitely not your father's Warrant Officer Corps

*By CW5 (Ret) Andrew Barr*

I witnessed some dramatic changes in the overall management and use of warrant officers during the three decades I was allowed the honor of wearing the warrant officer rank in the U.S. Army.

Today's Signal warrant officers are the best educated, extensively trained, and most relevant group of officers to ever wear a warrant officer bar. They are placed in more crucial and challenging positions that impact unit function and mission than ever before. Today's warrant officer is better educated and trained because the Army and the branch leadership understand they must invest in the Signal warrant officers' lifecycle because of their relevancy in today's Army formations. The investment has been tremendous and the payoff is reflected in a warrant officer corps that is providing superlative performance.

## There I Was

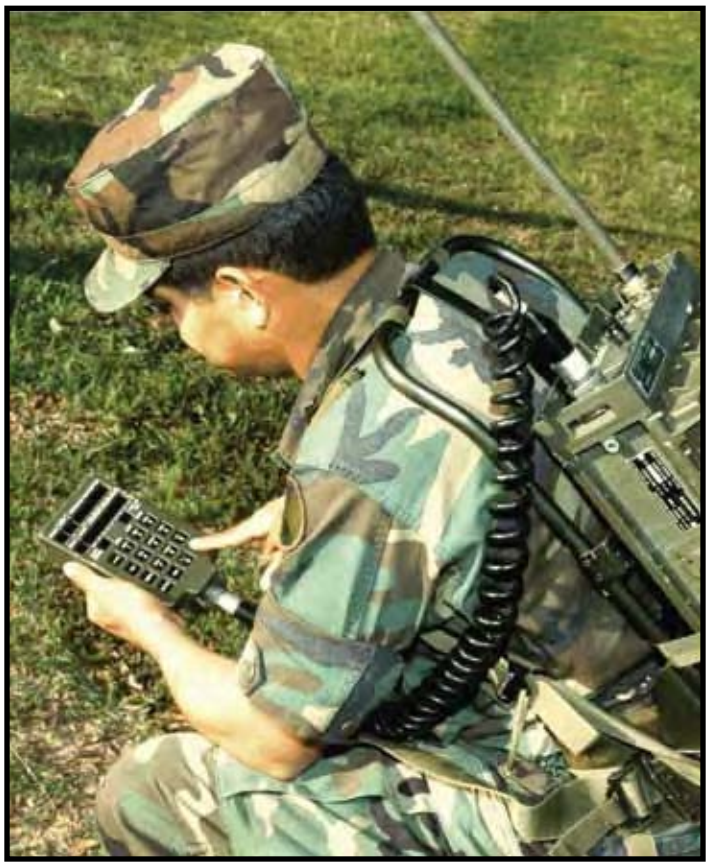
A recount of my experiences as a warrant officer serves to illustrate the dramatic changes in warrant officer management. In 1979, I had a small ceremony where my senior rater removed my stripes and placed a warrant officer bar on my shoulders. I was then sent to my first assignment as the technical expert. I received no additional technical or officer training and was expected to be a subject matter expert; when in reality I was a Soldier wearing a W1 bar with noncommissioned officer skills, expected to act like an officer.

My first assignment was as the operations officer supporting the U.S. Military Training Mission in Saudi Arabia. I was the only Signal warrant officer in the organization which was the norm for the time. I was tasked with managing over 30 Soldiers who were responsible for the operation of two fixed telecommunications centers separated by over 200 miles, seven high frequency radio sites located throughout the kingdom, and a handful of secure telephones.

Lucky for me my rater, MAJ Kevin Upton, believed in mentoring and counseling. He taught me how to be an officer and spent time teaching me how to brief, write, read, dress, and the esoteric nuances expected of an officer. He explained my specific roles and responsibilities. I discovered later that MAJ Upton set me up for success. Most of my peers did not have a similar experience and would later encounter tremendous career difficulties.

My first operations officer assignment required a seasoned warrant officer but when I was assessed, management of positions was not being accomplished well. There was a saying that 'a warrant is a warrant is a warrant' indicating leaders did not recognize the progressive experience and training (which was lacking) of the warrant officer was as important as that for commissioned officers or NCOs of the period. There was no difference in the position coding. So a unit could receive a new W1 or the most seasoned W4 to fill a vacant position.

Today, warrant officers are placed in positions of increased responsibility based on their progressive training and experience. Manning documents identify specific pay grade requirements and, when possible, the correct grade is sent to fill the positions. Based on inventories of each grade, it may not



**Signal warrant officers and Soldiers used the Enhanced Position Location Reporting System that was first fielded in 1987.**

always be perfect, but we seldom see a W1 filling a senior position or a senior warrant officer filling an entry level position as was normal in the 80s.

My second assignment was the 414th Signal Company at Fort Meade, Md in 1981 to a tactical Signal battalion that contained three area Signal centers providing echelon above corps support.

This was my first assignment to a tactical Signal unit because my enlisted time was in Armor and Infantry units as a tactical communications chief and radio teletype operator. There would be other Signal warrants in the unit and this is where I discovered that my expectations as taught by MAJ Upton and the expectations by the other warrants would not be the same. I would go to my first physical training formation only to find that all enlisted Soldiers and other officers were there, but I could not find the other warrants. I would go to officer professional development only to discover I was the lone warrant officer in attendance. I attended unit social functions and felt obligated to support the commander as requested, while the other warrants did not feel the same obligation.

Attending off duty functions allowed me to have discussions with the decision makers, build personal relationships with the other officers in the organization, and ultimately allowed me to better influence decisions. Part of the confusion on behalf of the other warrants was that our roles and responsibilities were not well documented and that each commander or rater would determine the expectations of their warrant officers. The warrants expressed the feeling that they did not feel they were part of the officer corps and were only a part of a small group of warrant officers. This shortfall has changed dramatically during the past 10 years.

Our roles and responsibilities are well documented in Army publications and are readily accessible by the commanders and O-grade officers in the field who rate warrant officers.

Interacting in all settings with fellow officers provided additional opportunities; such as the opportunity for selection over several warrant officers who were senior to me to be the platoon leader of an 80 Soldier ASC when the organization was short of commissioned officers. This experience was another learning experience that allowed me greater options in future assignments where I would be responsible for many Soldiers.

I attended the Warrant Officer Advance Course in 1983. Signal was one of the branches that had a WOAC at that time. This was my first formal professional military education course as an officer. I signed into the unit at Fort Gordon and went to the assigned building and room on the following day. It was located in the old training area located between Academic Drive and 7th Street. They are probably among the oldest buildings still standing on Fort Gordon. All other students, officer and enlisted, were being taught in the new buildings on post.

We received a couple weeks of formal training on logistics, administration, and a few other common core topics that were beneficial. We were then told to visit the classrooms located on

**(Continued on page 18)**

**Today Signal warrant officers are managing technology that includes smartphone technology with an extraordinary array of applications that multiply daily.**

(Continued from page 17)

post that were of interest to us and ask if we could sit in on the instruction. We never touched any equipment or discussed any specifics about what we would be required to do in our future positions. My racquetball game was never better than when I left Fort Gordon three months later.

Today, the WOAC is a challenging experience where the warrant officer leaves with the knowledge and skills to better support their units at the W3 level. Fort Gordon has invested greatly in the training opportunity. It is not a review of what the officer learned in their basic course but an upper level, if not graduate level, educational experience for the student.

## There We Were

A Department of the Army study, The Warrant Officer Study, was completed in 1985 and a number of changes occurred as a result of the study. This was the first DA-level comprehensive study of warrant officer management from pre-appointment to retirement. It spanned the total Army, both active and reserve.

The study determined that warrant officers' technical expertise alone was not enough to meet the requirements of the Army's current and future doctrine. They identified that warrant officers needed to be proficient in basic tactical and leadership skills. This finding led the Army to stop direct appointments and to establish a warrant officer candidate school for all newly appointed warrant officers similar to the officer candidate school that the other officers attended.

Technical warrant officers started attending a course that the Aviation branch established for training their warrant officers at Fort Rucker, Ala. Two satellite locations for the training were established; one at Aberdeen Proving Grounds in Maryland and the other at Fort Sill, Okla. These satellite locations remained as training sites for a couple of years until all training was centrally located at Fort Rucker in 1990. The curriculum was the same at all three. The primary problem with the curriculum was that most Aviation warrant officers were junior enlisted Soldiers or Soldiers who enlisted to become pilots and only experienced basic training in their Army career. The Signal warrant officer was already an NCO with several years' experience. The training did not consider the skills and experiences the NCO brought to the course. It was 20 years before the WOCS would recognize the NCO skills and provide two separate courses; one for the candidate who was neither a graduate of the Warrior Leader Course or a NCO, and one for those who were both. It has become a relevant part of the leadership training received by the newly accessed warrant officer. This was a great step in providing a better, more relevant training experience.

In 1987, I was commissioned an officer in the U.S. Army, as were all chief warrant officers. Congress changed the law to standardize the procedures used by the military services that had warrant officers in their inventory. A key provision was that all chief warrant officers received commissions, while warrant officer ones continued to be appointed, not commissioned. The primary goals of the decision to commission warrant officers included the authority to administer oaths of reenlistment, designate selected warrant officers as commanding officers with greater authority to impose non-judicial punishment under Article 15, UCMJ and to characterize service of commissioned WO as "commissioned service." The opportunity to administer oaths is something I have cherished over the years. I am extremely proud of the many warriors to whom I was allowed to administer the oath. Although the opportunity to command is not one that Signal required, we have had a few positions where it was used. Other branches use their warrants to fill that position concurrent with their technical expertise. Prime examples are the bandmasters and transportation warrant officers. There have been many attempts to have a newly appointed W1 be commissioned and not appointed.

Many of the recommendations from TWOS were implemented in law or policy in 1992. Passage of the Warrant Officer Management Act of 1992 mirrored the Defense Officer Personnel Management Act that was passed in1980. DOPMA established a common officer management system built around a uniform notion of how military officers should be trained, appointed, promoted, separated, and retired. Similarly, WOMA changes included a single promotion system for warrant officers, tenure requirements based upon years of warrant officer service and authorization for the Secretary of the Army to convene boards to recommend warrant officers for selective mandatory retirement. This was a direct attempt to integrate warrant officers into the officer corps.

The W5 pay grade was also part of WOMA. This had been a desire of the Army for many years and was finally approved in law. The new pay grade was established to fill the most senior levels of the Army. This was an indication of the increase in the relevance and overall understanding of the warrant officer by Army leadership.

The TWOS study group, as many previous study groups, had determined that a requirement existed for highly experienced senior warrant officers to serve as branch technical integrators and advisors to commanders and their staffs. This finding served as primary justification for establishment of the new grade.

During this same period, a number of policy changes occurred. They included coding of posi-

tions in authorization documents by rank grouping and automatic Regular Army integration at the CW3 level.

The Warrant Officer Leader Development Action Plan, the plan developed based on the results from TWOS was approved in 1992. WOLDAP was a total Army plan designed to ensure both active and reserve warrant officers were appointed, trained and utilized to a single standard.

Before moving on however, it is prudent to note another DA study named The Army Training and Leader Development Panel was completed in 2002. It picked up where TWOS left off. The study concluded the Army must make fundamental changes in the warrant officer cohort to support full spectrum operations.

At the heart of the change was a complete integration of warrant officers into the larger officer corps; a process begun in the 1980s but never completed. Specifically, the study concluded that the Army needs to clarify the roles of warrant officers, then make changes to their professional development, training and education, and manning.

Many initiatives were identified following the final report that had a dramatic impact on today's warrant officers' ability to support the force.

I will skip some assignments and go to 1999 when I was promoted to CW5 and assigned to serve in a branch immaterial position in the G1 of the Army located in the Pentagon. I had no idea what I got myself into, but it was obvious that I would have to learn quickly to be relevant in this position. Again, a number of O-grade officers assisted me to learn how to be a staff officer since none of my PME courses had prepared me to work in that type of environment.

I was involved in two major studies of the warrant officer and was part of the implementation process when, in 2004, I was selected to be the second Regimental chief warrant officer of the Signal Regiment.

The biggest changes to the warrant officer during my three decades occurred during the past eight years. I will highlight a few of them and attempt to provide a short analysis of each.

## Here We Are

A new definition for the warrant officer was developed in 2005 to encompass all warrant officer specialties and grades and to include the leadership responsibility. It currently reads:

"The Army Warrant Officer is a self–aware and adaptive technical expert, combat leader, trainer, and advisor. Through progressive levels of expertise in assignments, training, and education, the WO administers, manages, maintains, operates, and integrates Army systems and equipment across the full spectrum of Army operations. Warrant officers are competent and confident warriors, innovative integrators of emerging technologies, dynamic teachers, and developers of specialized teams of Soldiers. They support a wide range of Army missions throughout their career. Warrant officers in the Army are accessed with specific levels of technical ability. They refine their technical expertise and develop their leadership and management skills through tiered progressive assignments and education."

The Warrant Officer Division, first established in 1974 at PERSCOM to centrally manage warrant officer assignments and professional development, was deactivated and the responsibility for professional development and management, assignments, training, and education of all officers was assigned to the branch proponents in the Officer Personnel Management Division at PERSCOM. This change was required to better support the organizations in the field and identified that warrant officers are full members of the Signal officer corps. This was another part of the integration into the officer corps.

Another initiative that was part of the integration process was a change to AR 670-1 that directed warrant officers to wear the insignia of their branch and not the insignia of the warrant officer called the Eagle Rising. This was met with many emotional challenges. With over 80% of today's Signal warrants having never worn anything but the branch insignia, the emotion has subsided and it has been moved to its place in history. The purpose behind wearing the branch insignia is part of integrating warrant officers into the officer corps which brings synergy and better understanding that warrants are officers. Wearing branch specific insignia and colors in lieu of the warrant officer insignia and colors changed in 2004. Additionally, the increasingly joint nature of operations with the Department of Defense and the expanded use of the most senior warrant officers in joint operations validated the need to standardize CW5 rank insignia among all the services that employ them. The CW5 insignia that was approved in 1972 is worn instead of the master warrant insignia that had been worn since 1992. The master warrant officer was an interim rank used by the Army from 1989 until 1992 when the W5 grade was approved. A formal DA selection board was used to identify the MWO who would be placed in the senior positions that the CW5 eventually filled. The decision was made by DA leaders when CW5 was formally approved to continue to use the MWO insignia so those MWO who were not selected for promotion would not be identified.

Other changes that support the integration included placing warrant officer information in publications that contain officer

**(Continued on page 20)**

(Continued from page 19)

information instead of maintaining two separate publications.

In 2004, DA mandated that each proponent establish a chief warrant officer of the branch position to serve as the principal advisor to the commanding general/branch chief on all matters pertaining to warrant officers. Specific roles and responsibilities were identified for these positions that would allow better involvement and management for each branch warrant officer. The Signal Regiment established its RCWO position in 1999.

In 2005, the promotion zones of consideration were reduced allowing CW2s and CW3s to get promoted faster. It eliminated the Below Zone opportunity for promotion to CW3 and CW4. The reduction allowed a CW2 or CW3 to be considered for promotion to the next grade with 3 years time in grade and promoted in their fourth year. It allowed a newly accessed warrant officer to be promoted to CW4 in ten years of warrant officer service. CW4 TIG remained at 5 years. This was the second time in less than 8 years the zones had been reduced. A similar change occurred in 1997 reducing the TIG from 6 years to 5 years. A number of reasons contributed to this decision, but it ultimately increased the number of senior warrant officers in the inventory. A problem may be realized soon that too many senior warrants are in the inventory and steps may be taken in the future to increase the TIG zones for promotion.

Delinking professional military education from promotion was effected a few years ago. Prior to this change, a Signal warrant officer had to be a W3 or on an approved promotion list to attend their WOAC. This meant that a warrant officer could go eight years without attending formal technical training at a branch school. If the purpose of the WOAC was to prepare a warrant officer to fill the CW3 positions and they were not allowed to go to school until they were filling the position, it was obvious the process was flawed.

Technical changes in the Signal community added to the challenge. Delinking the PME from the promotion process allows a warrant to attend WOAC, WOSC and WOSSC at an earlier time to better prepare them for the next promotion. Many discussions of requiring completion of PME attendance have been around for years and may be mandated if warrant officers do not voluntarily attend. The Reserve Components currently require attendance prior to promotion.

The accession process has been dramatically refined and now must be accomplished online. The chain of command is part of the staffing process and applicants can easily apply. A formal process was established in the 1980s and much better information is now provided for the applicant. The process has matured to an extremely easy, valid applicant friendly online procedure that can be completed in a very short amount of time. A board of officers review and vote on each application. The board uses the time tested selection process that the Army uses for promotions and command and schools selection. It is now a legitimate process that allows the Army to access the best applicants.

One of the greatest things accomplished at Fort Gordon was to require all Reserve Components to complete the same training as the Active Component.

Prior to 2005, RC warrant officers could take a series of tests and get credit for attendance at the technical training. The RC students were being disadvantaged and were not being set up for success because the tests were not a valid indication of the student's knowledge. The dramatic increase in theory education and hands-on training and testing eliminated that option and the knowledge that the RC warrant would be deployed and expected to provide the same support mandated that all complete the same training.

A significant targeted pay increase for warrant officers was provided in 2007. This pay raise assisted with the accession process because, for the first time, an E7 did not lose money in base pay when pinning on a W1 bar.

It also showed that the Army is very serious in supporting the performance of the warrant officer. It was a very difficult action to gain added pay for the warrant officers because it is a Department of Defense pay scale. The Air Force does not have warrant officers and the other branches maintain a much smaller inventory of warrants. This action took over five years to accomplish.

I believe the biggest cultural change for warrant officers occurred when the Army changed the basic structure for the Army and went to the brigade centered structure.

This action placed Signal warrant officers in a combat arms brigade for the first time. It doubled the necessary Signal warrant officers required to support the force. The increase also applied to the RC. Prior to 2004, Signal warrants supported the brigade from the Signal battalion. The brigade commander did not know who the warrants were or what they did. Teams were sent from the Signal battalion to support the brigades, but they did not contain the Signal warrant. Therefore, the brigade commander's exposure to any warrant officer was usually limited to only one technical warrant, the motor maintenance technician, who was in every battalion motor pool.

This is important because the combat arms brigade commander may later become a general officer in a decision-making position to support the lifecycle management of warrant officers. I briefed

many senior general officers while assigned to the Pentagon and learned quickly that I needed to provide a short introduction brief on what technical warrant officers did to support the Army prior to any formal briefing of any warrant officer topic. The general officers understood the purpose of Aviation warrant officer but had little or no knowledge of the technical warrant based on their limited exposure. That is now changing. Every brigade now has about 50 warrants of a variety of branches in their unit. The Signal warrant officer in the brigade is being recognized by the commander and the impact provided by the warrant officer is being identified. The brigade commander is not basing all opinions of warrant officers on his experience with only one technical warrant officer. Exposure to only one of anything limits your view.

Another recent significant change is in the number of warrant officers being assigned to the senior Army organizations. More senior warrant officers are being placed at senior level headquarters as staff officers providing their influence as the proven experienced technical leaders in the decision making processes that affect the Army. The more advice they provide the more advice the senior leadership desires from them.

## There You Must Go

We must assertively dispel the notion that warrant officers are a separate segment of the officer corps and move with diligent actions to completely integrate into one officer corps bonded with common goals and an understanding of one another's roles. Warrant officers must discontinue any thoughts of inflexibility to perform outside their specialties in order to operate effectively in the full spectrum of Army operations.

I saw many other changes in the management and education of the warrant officer during the last three decades that I will not address based on the space allocated for this article. Let me state again that the Signal warrant officer of today is the best trained, educated, and relevant Signal warrant officer to stand in our formations.

It is not your daddy's Warrant Officer Corps anymore. Technology, the changes in training, and fighting a war for more than 10 years have changed things significantly.

Anyone who has not been associated with the Army during the last 10 years would not recognize the warrant officer of today. The changes have legitimized the warrant officer and what they do to earn their pay. The previous changes are just a beginning of what the warrant officer of the future will see. It was awesome to see firsthand the relevancy of the warrant officer change as it did and to have a vision of what is expected of the future warrant.

***CW5(Ret) Andrew Barr*** *retired in March of 2010 after serving almost 40 years in the Army, over 30 of those years as a warrant officer. He served in a myriad of assignments and was the second Regimental chief warrant officer for the Signal Regiment.*

## Acronym QuickScan

**ATLDP** – Army Training and Leader Development Panel
**ASC** – Area Signal Centers
**CW2** – Chief Warrant Officer Two
**CW3** – Chief Warrant Officer Three
**CW4** – Chief Warrant Officer Four
**CW5** – Chief Warrant Officer Five
**CWOB** – Chief Warrant Officer of the Branch
**DA** – Department of the Army
**DOPMA** – Defense Officer Personnel Management Act
**EAC** – Echelon Above Corps
**JIIM** – Joint, Interagency, Intergovernmental, and Multinational
**MDMP** – Military Decision Making Process
**MWO** – Master Warrant Officer
**NCO** – Noncommissioned Officer
**OIL** – Observation, Insights and Lessons
**OPD** – Officer Professional Development
**OPMD** – Officer Personnel Management Division
**PERSCOM** – (Army) Personnel Command
**PME** – Professional Military Education
**PT** – Physical Training
**RC** – Reserve Component
**RCWO** – Regimental Chief Warrant Officer
**SSC** – Senior Service College
**SMA** – Sergeants Major Academy
**TIG** – Time in Grade
**TWOS** – The Warrant Officer Study
**W1** – Warrant Officer One
**WLC** – Warrior Leader Course
**WO1** – Warrant Officer One
**WOAC** – Warrant Officer Advance Course
**WOBC** – Warrant Officer Basic Course
**WOCS** – Warrant Officer Candidate School
**WOLDAP** – Warrant Officer Leader Development Action Plan
**WOMA** – Warrant Officer Management Act
**WOSC** – Warrant Officer Staff Course
**WOSSC** – Warrant Officer Senior Staff Course

# Historical view of the Signal Warrant Officer Corps occupational specialties

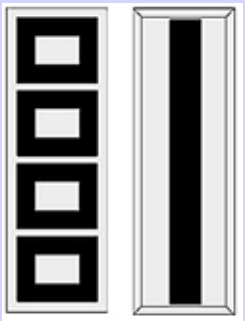
*By CW5 Todd M. Boudreau*

Here is an historical look at our Signal warrant officer military occupational specialties.

While we might not be able to trace our Signal warrant officer MOS back to 1918, there are distinct warrant officer MOS functions associated with the Signal Corps that go back as far as October 1943 (i.e., MOS 4400, Signal Supply Officer and MOS 0145 Radar maintenance and repair officer).

## The Earliest Years

The best point of entry is 1961 to chronicle the history of contiguous MOS adjustments which lead to the current Signal warrant officer MOS. For example, MOS 286A, communications-electronics repair technician, which had previously been MOS 4415, Signal equipment maintenance and repair officer (established in July of 1948) was created in June 1961. A number of related MOSs were also created in this action in 1961 to include MOS 281A, radio repair technician; MOS 282A, radar repair rechnician; and MOS 284A, television repair technician. Most of these MOSs were eventually subsumed into MOS 286A in the 1970s which remained a stalwart Signal warrant officer MOS for many years.



**Shown here on the left is the master warrant officer four (MW4) insignia authorized 1988-1991, which then became chief warrant officer five (CW5) insignia from 1991-2004. On the right is the CW5 insignia authorized 2004 to the present.**

## MOS 250B

In October 1987, MOS 286A was converted to MOS 256A, communications-electronics repair technician, which also eventually subsumed MOS 257A, data processing systems repair technician two years later. MOS 257A had been converted from MOS 287A, data processing systems repair technician, (created 19 Sep 77) which had previously subsumed both MOS 301A, data processing equipment repair technician, (created 3 Jun 61) and MOS 361A, fire distribution systems repair technician, (created 11 Sep 62).

Some of our more senior Signaleers may remember MOS 256A, since it remained on our authorization documents for almost 10 years. However, MOS 256A succumbed to the push to move all repair MOSs to the Ordnance Corps. Thus, in June 1995, all but a few select 256A positions were re-coded 918B.

The small handful of positions that remained Signal was coded with the Additional Skill Identifier 3E, satellite communications. These positions and a few individuals holding them were re-coded/reclassified to MOS 250B ASI 3E. MOS 250B, Tactical automated network technician, was created in October 1988, initially subsuming personnel and positions of MOS 250A, telecommunications technician with ASI 3T. MOS 250B are best known for their depth and breadth of experience in Mobile Subscriber Equipment and the TRI-TAC switching suite of equipment. This is a great place to divert momentarily.

## MOS 250A

MOS 250A was added in October 1987 as it subsumed MOS 290A, Telecommunications Technician, created September 1977 from MOS 341A, cryptographic equipment repair technician, (created 3 Jun 61) which was previously MOS 4418, cryptographic repair officer, (created 18 Nov 57) and MOS 721A, cryptographic technician, (created 3 Jun 61) which was previously MOS 0224, message center officer, cryptographic, (created 30 Oct 43). MOS 250A, best known for their depth and breadth in communications security and telecommunications message systems, is another of our more recent MOS which existed for over 10 years when it was ultimately subsumed, along with MOS 250B, into MOS 250N, network management technician in April 1999.

## MOS 250N

MOS 250N remained relatively stable until September 2000 when all COMSEC functions were transferred to MOS 254A, (created in 2000 though not an effected MOS until April 2003) and all CW5 positions were transferred to MOS 255Z (also created in 2000 though not an effected MOS until April 2003). MOS 250N are best known for their depth and breadth of experience in transport and circuit switch equipment to include Internet Protocol routing. See the article entitled, "The Army's expert cyberspace network management technician – MOS 255N" for more information regarding the current 250N and its repurposing actions.

## MOS 255N

This brings us to the current state and fate of MOS 250N. As of November 2009, MOS 250N has been in

**Robert H. Lee was an early Signal warrant officer.**

transition to MOS 255N which will be effective October 2012. The training currently offered under the 250N Warrant Officer Basic and Advance Courses (WOBC and WOAC respectively) was refined on 1 October 2009 to meet most of the training requirements of MOS 255N. Position recoding from 250N to 255N will be effective 1 October 2012. Those graduating from either the 250N WOBC or WOAC as of fiscal year 2010 may be awarded MOS 255N at the discretion of HRC. All others holding MOS 250N will be reclassified to MOS 255N during the 6 June – 30 September 2012 reclassification window. Note that there is an entire article dedicated to MOS 255N within this edition of the Army Communicator.

## MOS 251A

Going back to 1961, MOS 741C, Data Processing Technician, ADPS, was created from combining MOS 2403, ADPS operations technician, (created 6 Nov 58) and MOS 2404, ADPS Programmer, (created 6 Nov 58). In December 1970 it split into MOS 741B, 741C, 741D, & 741E and was eventually deleted in April 1976 when it and its family of MOS consolidated into 741A.

MOS 741A, data processing technician, continued to exist for over 10 years until it was converted to MOS 251A, Data Processing Technician, in October 1987. Like MOS 250N, MOS 251A too transferred all COMSEC functions to MOS 254A and all CW5 positions to MOS 255Z in September 2000. MOS 251A are best known for their depth and breadth of experience in server operations and information systems and assurance programs. See the article entitled, "The Army's expert cyberspace content technician – MOS 255A" for more information regarding the current 251A and its repurposing actions.

## MOS 255A

This leads up to the current state and prospects of MOS 251A. As of November 2009, MOS 251A has been in transition with MOS 254A to MOS 255A which will be effective October 2012. The training currently offered under the 251A (and 254A as noted below) WOBC and WOAC was refined on 1 October 2009 to meet most of the training requirements of MOS 255A. Position recoding from 251A to 255A will be effective 1 October 2012. Those graduating from either the 251A/254A WOBC or WOAC as of FY10 may be awarded MOS 255A at the discretion of HRC. All others holding MOS 251A will be reclassified to MOS 255A during the 6 June – 30 September 2012 reclassification window. Note that there is an entire article dedicated to MOS 255A within this edition of the Army Communicator.

What remains to close out is MOS 254A, Signal Systems Support Technician and MOS 255Z, Senior Signal Systems Technician; both created in 2000 though not effected MOS until April 2003.

## MOS 254A and 255Z

In concert with the recent changes to MOS 250N and MOS 251A, as of November 2009, MOS 254A has been in transition with MOS 251A to MOS 255A which will be effective October 2012. MOS 254A was created to provide a Signal technical expert in non-Signal, maneuver formations. MOS 254A are best known for their depth and breadth of experience in maneuver Signal operations, Combat Net Radios, COMSEC, and Signal support to tactical operation centers. Since their inception, however, several significant shifts have incurred. First, the bandwidth and computing power of today's Digital TOC has increased to equal (and in some cases surpass) that of the nominal center in which MOS 251A is found. Second, Army transformation and modularity has negated the terminology "non-Signal maneuver formation." The brigade combat team today has organic Signal support unlike ever before. Therefore, MOS 254A has shifted to overlap MOS 251A in more than 80 percent of all critical tasks. See the article entitled, "The Army's expert cyberspace content technician – MOS 255A" for more information regarding the current 254A and its repurposing actions.

Finally, MOS 255Z will only see a slight shift to include renaming to senior network operations technician. Note also that there is an entire article dedicated to MOS 255Z within this edition of the Army Communicator.

This provides a brief synopsis of our Signal warrant officer MOS from the 1940s through today. For additional information on either the implementation of changes to MOS 255A, N, S, and Z please refer to the article posted by CW4 William Winkler entitled, "Warrant officer 255 series implementation" on page 53. Also included in this edition are in-depth articles on each of these new MOSs.

## Acronym QuickScan

**COMSEC** – Communications Security
**FY** – Fiscal Year
**IP** – Internet Protocol
**MOS** – Military Occupational Specialty
**MSE** – Mobile Subscriber Equipment
**TOC** – Tactical Operation Center
**WO** – Warrant Officer

# Cyberspace content management technician (MOS 255A)

*By CW5 Todd M. Boudreau*

To fully grasp the evolution and current role of the Army's cyberspace content management technicians you have to embrace one significant fact that is often misconstrued. Signal warrant officers are not Subject Matter Experts. Instead they are Systems Matter Experts.

Perhaps we should use SysME instead of SME to alleviate confusion.

To clarify this point, consider the current definition of a warrant officer from DA Pamphlet 600-3 (February 2010): "The Army warrant officer is a self aware and adaptive technical expert, combat leader, trainer, and advisor. Through progressive levels of expertise in assignments, training, and education, the WO administers, manages, maintains, operates, and integrates Army systems [underline added for emphasis] and equipment across the full spectrum of Army operations. Warrant officers are innovative integrators of emerging technologies, dynamic teachers, confident warfighters, and developers of specialized teams of Soldiers. They support a wide range of Army missions throughout their career."

This point is significant. With the complexity of today's communications systems, our Signal warrant officers cannot afford to limit themselves as SMEs. That is the role of the junior NCO. One look at a requirements document that lists a Signal warrant officer will reveal a number of enlisted positions that function as SMEs. The warrant officer position is then required to be a SysME--one who brings each related component (subject) and integrates it into the total--the system. Indeed some Signal warrant officers are SMEs, but SysME more accurately describes their increased sphere of responsibility.

Another important point to consider before we move to the objective 225A is that we are like a formation in motion. By this I mean that there are still legacy issues that our Signal warrant officers face in their individual MOS. Due to doctrine, organizational designs, current equipment, systems, and legacy leadership ideology, the description of a 255A indicated in the following narrative will not immediately materialize.

We can't make an immediate right flank, march. Instead, we are in the beginning of a column right in which you will have some units immediately receiving newly trained 255A, N, and S and employing them as envisioned. These units have already made


**Diagram 1**

the turn. Other units, however, will find themselves further back in the formation and as such, the designated 255A Soldier will still be performing duties that are shifting to 255N (e.g., Local Area Network installation, operation, and maintenance).

Finally, for the sake of clarity, I will categorize three separate but related systems, one per element of network operations. Above is the NetOps construct that shows its three elements which I will simply state as cyberspace content management, cyberspace network management, and cyberspace defense. See diagram 1 above.

Two more notations are necessary to frame this discussion. First, because these three are 'elements' and not 'enablers,' NetOps does not exist unless all three are in play. Second, the purposed overlap indicates higher level NetOps functions within an element that is either supported by or supports another element. These concepts will be further defined in later articles on MOS 255N, 255S, and 255Z.

The MOS 255A technician, one of two future enlisted-level accessions MOS (255S is a warrant officer-level, i.e., W3 accession MOS), is responsible for cyberspace content management. This is the Army's premier information systems and services technician MOS. The 255A technician is charged with establishing and maintaining the ability to collect, process, store, secure, search for and discover, retrieve, and disseminate information utilizing the application layer environment of the Army's portion of the cyberspace domain. They administer and manage systems which perform Information Dissemination Manage-

ment/Content Staging in order to enable Information Management/ Knowledge Management functions supporting combat information superiority and decision dominance.

## Where We Were

In more than two decades, MOS 251A, Information Systems Technician, created in October 1987 which was previously coded MOS 741A, Data Processing Technician, had only seen two significant revisions during its lifetime. Both occurred in September 2000 when all COMSEC functions were transferred to MOS 254A and all CW5 positions were transferred to MOS 255Z.

However, we are in the midst of its close out and most significant revision. MOS 251A is combining with MOS 254A and subsequently will be converted to MOS 255A, Information Services Technician. While MOS 254A, Signal Systems Support Technician, saw its inception in September 2000, it has only been effective since April 2003. Less than a decade later, it too will be deleted as it is combined with MOS 251A and converted to MOS 255A as well.

Two years ago, it was decided that these two MOS (251A and 254A), due to the forces of transformation and technological advances which caused MOS 254A to shift into a role it had not planned to fill in its inception, had come to mirror each other in most of the critical skill-sets.

There were also a number of other issues that required immediate attention to include the grade pyramid which ensures an adequate base of junior positions to support a smaller number of senior positions as well as adequate numbers of senior positions to support future advancement and promotion potential. In 2007, the base of this pyramid for MOS 254A was grossly over the Army standard resulting in little promotion potential for this MOS; concurrently, it was upside down for MOS 251A resulting in numerous junior 251As filling more senior 251A positions."

## Where We Are Heading

### *Apprentice Cyberspace Content Managers*

Junior 255A (i.e., W1 and W2) focus on acquiring and refining technical and administrative skills as they directly plan, install, administer, manage, maintain, operate, integrate, service, secure, and troubleshoot information systems and services and supervise and train personnel at the brigade level. Their focus is mainly on the applications and systems and how to leverage them to assist their commander to prosecute the collective unit mission. They are concerned with the systems that provide the capability to manage, manipulate, and disseminate information.

The term 'apprentice' must not be misunderstood. Newly appointed CyCMs, while apprentices as warrant officers, are not new to information technology. They average 10 years active Federal service with a minimum of four years documented practical experience in IT administration, Army battle command system administration, local area network administration, and/or information assurance/ computer network defense. Nor are they apprentice leaders since the average grade at time of accessions as a Signal warrant officer is staff sergeant. As a minimum, they must have at least 36 months of documented rated time as a leader as evidenced by official NCO evaluation reports.

However, in their new realm, they are apprentices. As such, the junior CyCM begins to learn each and every 'subject' within their 'system.' Being an SysME does not allow them to abdicate their responsibility to be an expert in each one of the subjects under their purview.

The goal is that they fully realize their role as a "self aware and adaptive technical expert, combat leader, trainer, and advisor" which will only occur if they are the consummate experts over each subject assigned to them. In that, as a WO1/CW2, their "primary focus is becoming proficient and working on those systems linked directly to their AOC/MOS" (DA Pam 600-3), this is the time for them to lay their foundational understanding of the devices and applications used in their system.

**(Continued on page 26)**

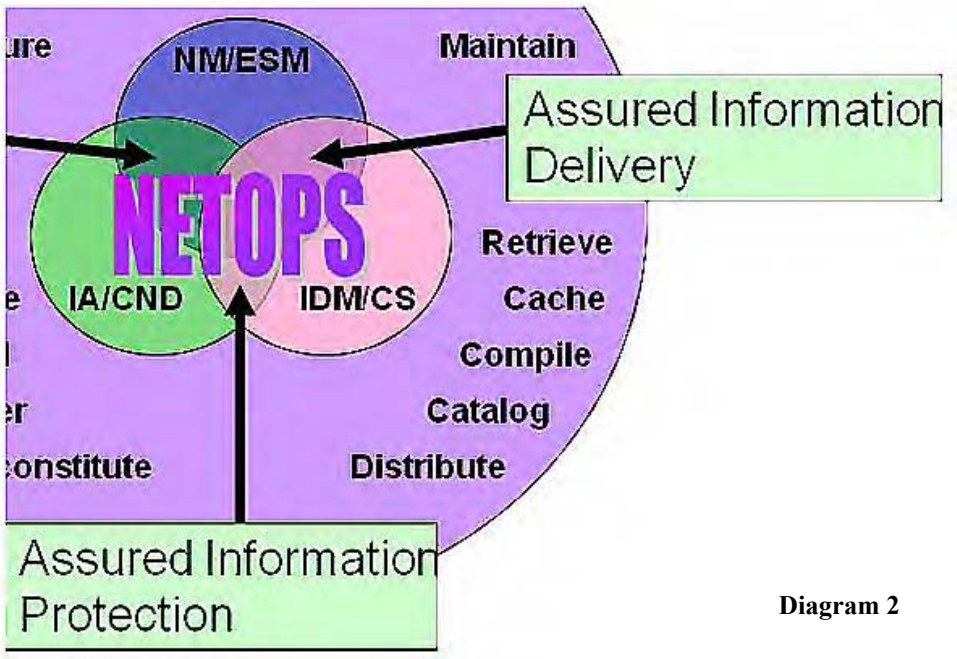



**Diagram 2**

**(Continued from page 25)**

The WO1/CW2 255A focuses on the install, maintain, and operate aspects of the system in which they are responsible. They are to focus on the individual pieces of their system, many of which they were trained on in their WOBC. Examples of such devices and applications in today's Army inventory includes (but are not limited to) servers, storage area networks, battle command common services, exchange, active directory, SQL, SharePoint, Adobe Connect, virtualization, video teleconference systems, information systems and services level Information assurance management, standard Army management information systems, etc. See diagram 3. It is noteworthy that this repurposing of MOSs along with changes in technology has shifted various responsibilities to other MOSs. For example, the repurposing of our various MOSs has shifted COMSEC from MOS 254A to enlisted Soldiers working in sections under the 255S.

MOS 255S will not fill COMSEC custodial positions, but instead will be placed in positions of leadership over COMSEC sections. Additionally, tactical radio communications systems are networkable IP-enabled, node/PoP-self creating devices that inherently create cyberspace transport as they are operated. Thus they shift under the responsibility of MOS 255N. However, IA activities have not, nor will they ever, shift to MOS 255S. MOS 255A Soldiers are fully responsible to posture their systems and ensure those systems remain compliant to all IA policies, practices, and governance.

The apprentice CyCM is nominally assigned to a brigade combat team where he/she has the greatest ability to encounter the widest array of devices and applications found within the breadth of assigned systems. Having spent approximately eight months in WOBC, the BCT is not only the level where junior warrant officer positions are most prevalent, but also provides the best opportunity to see the system put to use by its intended user – the combat commander. The astute apprentice CyCM uses this opportunity not only to provide the foundational training and experience in IT systems that he/she will build upon throughout his/her career, but he/she also is ever cognizant of the tactical purpose of these systems. He/she begins learning how to converse in IT communities and the tactics, techniques, procedures and vernacular of the combat arms community.

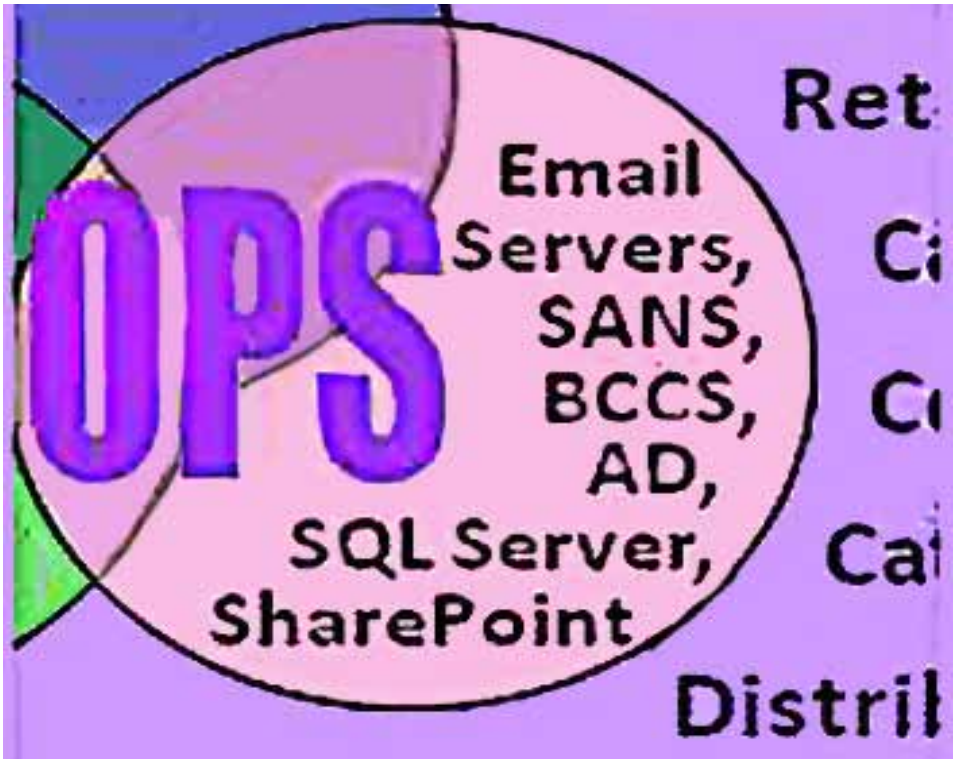



**Diagram 3**

It is important to note that the 255A MOS are not knowledge managers. Our 255A are technical officers who operate in the art, skill, and physical realm. They use practical aspects of physics [the physical technological devices that manipulate data elements] under the purview of their skills within the art of IDM/CS. KMs operate in the physiological and physics realm. They seek to understand the cognitive reasoning patterns of their principle and then leverage the practical aspects of physics [the physical technological devices that manipulate elements of information] in order to present the right actionable information to the primary decision maker at the right time.

For the KM, it is all about the actionable information becoming the correct knowledge. For the 255A, it is all about the systems controlling such information for manipulation by the KM. The 255A enables the KM.

KMs mainly operate in the cognitive domain while the 255A operates in the cyberspace domain. KMs decide what needs to be presented while 255As decide how (and sometimes if) something is presented. Most often success hinges on expectation management.

The best KM is attached to the principle decision maker to ensure they understand the decision maker's thought processing and get the right information presented at the right time in order to ensure the decision maker is knowledgeable on what the full scope of the

decision entails; to include second and third order effects. However, if the KM presents a plan to introduce either information that is not readily accessible or in a manner that is not practical, it is the 255A who will feel the pressure. Accordingly, the best 255A supports the principle decision maker's KM and thus must understand the KM's plans in order to help shape what will be presented to the principle decision maker; again, expectation management – and ensuring the mission is accomplished.

There is much, much more to this, but this provides a basic understanding. *(The next edition of the Army Communicator will address the KM subject in depth.)*

## Journeymen Cyberspace Content Managers

Mid-grade 255A (W3) focus past the individual applications and devices to acquire skills in the individual attributes of CyCM (i.e., the science of IDM/CS) as well as the intricacies of the interrelationships with the other NetOps elements. This development prepares them to be true experts in their craft and advisors to senior leadership on complex and complicated NetOps issues. In accordance with DA Pam 600-3, as a 255A becomes "more senior, their focus becomes integrating branch systems into larger Army systems."

Journeymen CyCM, as advanced-level technical and tactical experts, now step slightly away from the devices, applications, and even the system they oversee and begin to seek an in-depth understanding of the principles and science behind their systems. See diagram 4. Having gained expert experience in how these devices operate, they learn the deeper answer to why they are developed and how they are leveraged to enable knowledge management. Virtualization, meta-tagging, etc. become the realm in which the journeyman 255A begins to operate. It is the intellectual capital of the master 255A that will help the Army move forward in optimizing and securing its data elements in the future.

The saying that 'information is power,' is an incomplete truth. It is more accurate to say 'information enables power.' And subsequently, if not properly managed, it may disable power as well. A commander's inability to quickly locate specific actionable data has the effect of disabling the power that can be brought into the fight. Journeymen CyCM seek to sharpen their skills in the art and science of Information Dissemination Management and Content Staging to ensure their warfighting commander is fully enabled through their KM. They find and leverage the newest technologies and techniques and thus enable their KM to empower their commander. They seek out professional forums to ensure they remain informed on technology advancements and trends as well as opportunities to further their educational training through university courses and civilian certification programs.

The journeymen CyCM is nominally assigned to a division or corps where he/she has the greatest ability to focus on the bigger picture. Still remaining close to the devices and applications within their systems of responsibility, they find themselves moving past the install, maintain, and operate mission and becoming involved with the planning and engineering of IDM/CS for large organizations. In preparation for the demands of such assignments, these CyCM will attend the 255A Warrant Officer Advance Course.

Prior to WOAC attendance, enrollment into the Action Officer Development Course (131 P00) must occur after promotion to CW2 in order to qualify for WOAC Prerequisite Studies credit. The AODC was adopted as the resource for this distance learning WOAC Prerequisite Studies course. It is completed on-line via the Internet, and provides warrant officers serving in CW2 or higher duty positions relevant training in organization and management techniques, communication skills, preparing and staffing documents, conducting meetings and interviews, problem solving, time management, writing, coordinating activities, and ethics. CW2s have the flexibility to enroll at any convenient time between 24 and 48 months of total warrant officer service. Once enrolled, the course must be completed within one year. Journeymen 255As attending their resident WOAC will find project management and enterprise level systems integration two key technical components taught to prepare them to fulfill their duties.

The journeymen CyCM's credibility is very high in assigned organizations and the influence they have cannot be underestimated. Mentorship of apprentice CyCM becomes an inherent part of their duty description. They also begin to gain more uniformity in the supporting and supported roles of their peer Signal warrant officers, the 255N Cyberspace Network Management Technicians and the 255S Cyberspace Defense Technicians. No longer do they focus their duties and responsibilities on their systems solely. Now they begin to fully understand that the data and information they are entrusted to manage is meaningless if it fails to reach its intended destination and/or becomes exploited or manipulated by a cyberspace adversary.

Finally, some journeymen CyCM may feel a pull toward the cyberspace defense arena. It is at the beginning stages of his journeymenship (senior CW2 or junior CW3) where he may make the decision to move from the CyCM realm to the CyD realm. The decision point will normally be just prior to WOAC attendance. The expect-

**(Continued on page 28)**

(Continued from page 27)

ed prerequisites for such a transition along with the planned board process are addressed in list article on page whatever.

## Master Cyberspace Content Managers

Senior 255A (W4), having mastered applications, systems, and CyCM attributes move from the outer edges of the CyCM circle in the NetOps venn diagram, toward the center (See diagrams 1 and 2 on pages 24 and 25). They are now moving from mastery of one element toward the goal of W5 – mastery of NetOps in total. In accordance with DA Pam 600-3, the senior level 255A now adds such functions as "technical leader, sustainer, and advisor" to their list of duties and responsibilities.

Master CyCMs, as senior-level technical and tactical experts in their chosen field, have also gained familiarity with the other two elements of NetOps (i.e., CyNM and CyD). As they continue to develop as CW4 255A, they go beyond understanding the basic concepts of assured information delivery and assured information protection ensuring that these attributes of NetOps are obtained. While there is never an expectation of finger-pointing between the three associated skill-sets, the master CyCM takes ownership of these concepts and relationships (as do each of our Signal warrant officer MOSs) and in the absence of each sister MOS, takes charge. When all three MOSs are present, the conscious shared desire for synergy is the goal.

The master CyCMs are nominally assigned to a corps, ASCC, or higher level organization where their training and experience has its greatest impact. To prepare the CW4 255A for the duties and responsibilities encountered at these levels of organization, attendance at the Warrant Officer Staff Course is crucial.

The current WOSC includes a 41-hour self-paced course taught in the Blackboard learning content management system (web-based) designed to be completed over a 90-day period. It is designed to prepare future resident students for the core curriculum of the WOSC. The WOSC resident course provides instruction on tactical and operational scenarios in a joint, interagency, intergovernmental, and multinational environment with a strategic overview.

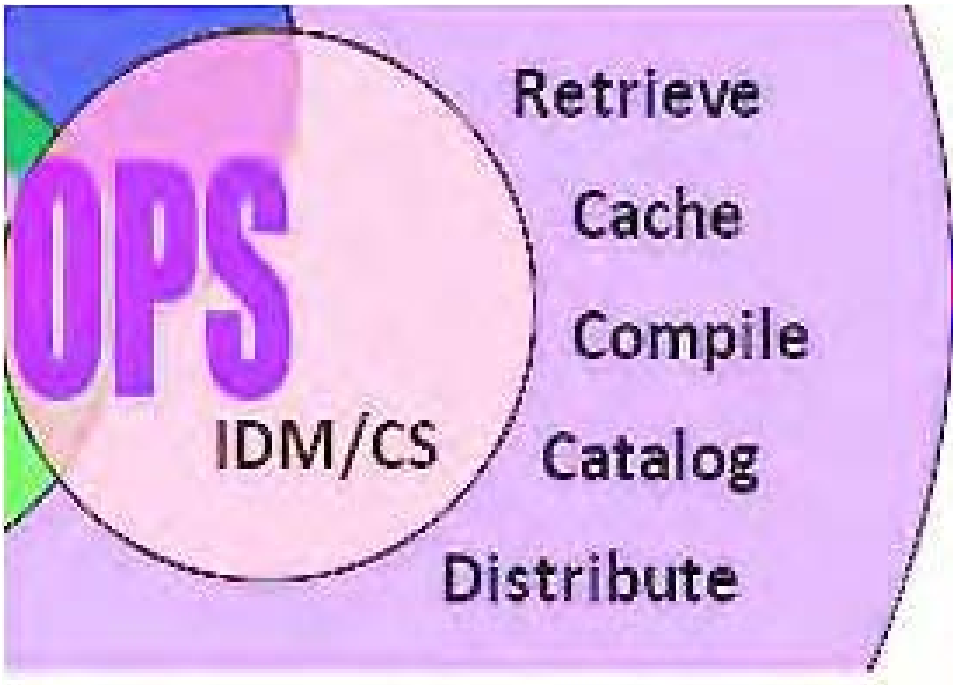



**Diagram 4**

History and battle analysis provides in-depth understanding of both the military decision making process and staff systems integrator-manager skills training and education. Knowledge management and project management with associated PEs are also introduced to reinforce the learning objectives. Assigned readings, an observation, insights and lessons learned paper as well as an MOS briefing must be completed to round out the course requirements. A recent decision to add functional branch training during this point in a warrant officer's career ensures maintenance of a solid tether to the advancements in the warrant officer's area of expertise.

A needed continuing education gap is being closed in the warrant officer corps. Because a warrant officer is authorized 30 years of service as a warrant officer, and should attend their Professional Military Education as early as possible, it was noted that with nominal WOAC attendance somewhere around the 5-6 year mark as a warrant officer, no further institutional branch/technical training would be provided for the remaining 24-25 years of WOS. Not willing to accept this, branches have been given approval to add such a functional branch training course subsequent to the WOSC. We are also investigating the necessity of a similar course following the Warrant Officer Senior Staff Course.

The currently planned WOSC follow-on course will be conducted similar to the Pre-Command Course. This five-week course will include as its foundation the Information Technology Infrastructure Library which is a set of concepts and practices for information technology services management, information technology development and IT operations. ITIL gives detailed descriptions of a number of important IT prac-

tices and provides comprehensive checklists, tasks and procedures that any IT organization can tailor to its needs. ITIL is published in a series of books, each of which covers an IT management topic. Also addressed are topics such as Army transformation, future Signal systems, LandWarNet architecture, enlisted MOS training, branch 25A and Functional Area 24A and 53A training. Since many of these officers will either arrive from or transfer to joint organizations, an up-to-date understanding of where the Army and the Signal Regiment is heading is absolutely necessary for the master CyCM to be fully successful.

The master CyCM continues to learn and grow in an area that never reaches a plateau. They, through their six-to-ten years of warrant officer service, continue to provide the Army and Department of Defense expert support to the ever critical IT systems which house and/or enable our nation's most lethal weapon systems. Just prior to promotion to CW5, the master CyCM is scheduled to attend the WOSSC. The current WOSSC includes a 47-hour course taught asynchronously in the Blackboard learning content management system (web-based) over a 60-day period. This course is not self-paced. Phase 1 (DL) asynchronous training consists of assigned professional readings, submission of two written papers, and participation in student to student, and student to instructor discussions. It is designed to prepare future resident students for the core curriculum of the WOSSC. Phase 1 (DL) must be completed prior to attending the Phase 2 resident course. The four-week Phase 2 (resident) course attended by the Army's most senior warrant officers provides senior CW4s or new CW5s with the master-level education, knowledge, and influential leadership skills necessary to apply their technical expertise in support of leaders on strategic level JIIM staffs during full spectrum operations. The curriculum focuses on topics relevant to today's Army such as staff skills, training doctrine, force integration, leader development, contemporary operational environment, insurgency, counterinsurgency, creative thinking, and critical thinking techniques.

Subsequent to promotion to CW5, the master CyCM becomes part of an ever smaller, elite group of Signal warrant officers, the Cyberspace Network Operations Technician, MOS 255Z. For further information on MOS 255Z, see the article on page 48 in this issue of the *Army Communicator* summarizing their career paths and describing their skills, attributes, duties, and responsibilities.

Join the Discussion
https://signallink.army.mil

## Acronym QuickScan

**ABCS** – Army Battle Command System
**AGDM** – Average Grade Distribution Matrix
**AOC** – Area of Concentration
**AODC** – Action Officer Development Course
**ASCC** – Army Service Component Command
**BCCS** – Battle Command Common Services
**BCT** – Brigade Combat Team
**CNA** – Computer Network Attack
**CND** – Computer Network Defense
**CNE** – Computer Network Exploitation
**CNO** – Computer Network Operations
**COMSEC** – Communications Security
**CyCM** – Cyberspace Content Management
**CyD** – Cyberspace Defense
**CyNM** – Cyberspace Network Management
**CyNOT** – Cyberspace Network Operations Technician
**DL** – Distributive Learning
**IA/CND** – Information Assurance/Computer Network Defense
**IDM/CS** – Information Dissemination Management/Content Staging
**IM/KM** – Information Management/Knowledge Management
**IP** – Internet Protocol
**IT** – Information Technology
**ITIL** – Information Technology Infrastructure Library
**ITSM** – Information Technology Services Management
**JIIM** – Joint interagency intergovernmental and multinational
**KM** – Knowledge Management
**LAN** – Local Area Network
**MOS** – Military Occupational Specialty
**NCO** – Noncommissioned Officer
**NCOER** – Noncommissioned Officer Evaluation Report
**NetOps** – Network operations
**OIL** – Observation, Insights and Lessons Learned
**PE** – Practical Exercise
**PME** – Professional Military Education
**PoP** – Point of Presence
**SME** – Subject Matter Expert
**SQL** – Structured Query Language
**STAMIS** – Standard Army Management Information System
**SysSME** – Systems Matter Expert
**TTP** – Tactics, Techniques, Procedures
**TWOS** – Total Warrant Officer System
**WOAC** – Warrant Officer Advance Course
**WOBC** – Warrant Officer Basic Course
**WOS** – Warrant Officer Service
**WOSC** – Warrant Officer Staff Course
**WOSSC** – Warrant Officer Senior Staff Course

# Cyberspace network management technician (MOS 255N)

***By CW5 Todd M. Boudreau***

*(For a more complete understanding of the development of MOS 255N, read the article on MOS 255A in this edition of the Army Communicator on page 24.)*

## Where We Were

We had to address the question "What is a warrant officer MOS?" in the process of repurposing our current MOS. Branch officers have areas of concentration and enlisted Soldiers have MOSs. Warrant officers have both. A warrant officer MOS is comprised of a two-digit branch identifier (e.g., 25 for Signal), a third digit to define an AOC (e.g., 255 for Network Operations), and a fourth alpha character to finally comprise a warrant officer MOS (e.g., 255N for Cyberspace Network Management Technician).

The MOS 250N was created in 1998 and subsumed MOS 250A and 250B in April 1999. It then remained relatively stable until September 2000 when all COMSEC functions were transferred to newly created MOS 254A and all CW5 positions were transferred to newly created MOS 255Z. Since then, no major changes have taken place other than the inclusion of newer transport and routing technologies.

Looking back at our legacy Signal warrant officer MOS, we in fact had four AOCs: (1) 250, Network Management; (2) 251, Automated Information Systems Operations; (3) 254, Signal Systems Support Operations; and (4) 255, Signal Systems Operations. Each AOC had only one MOS. The decision was made to repurpose AOC 255 to Network Operations and then place all four MOS under this one AOC. This becomes more significant as we recognize the correlation between the interdependencies of the three elements of the NetOps construct and the interdependencies of the three base Signal warrant officer MOS as indicated below.

## Where We Are Heading

Below is the NetOps construct on the 255A that shows its three elements and how the repurposed MOS matches each. MOS 255Z remains our capstone Signal warrant officer MOS and thus the senior MOS that acts to ensure, shape, and enable NetOps on the battlefield. MOS 255A is responsible for cyberspace content management while MOS 255N (Network Management Technician) is responsible for Cyberspace Network Management. Later articles will detail how MOS 255S is responsible for Cyberspace Defense and MOS 255Z is responsible for Cyberspace NetOps (CyNetOps) in its entirety. Because these three are 'elements' and not 'enablers,' NetOps does not exist unless all three are in play. The purposed overlap indicates higher-level NetOps functions within an element that is either supported by or supports another element. Further elaborating on the former, I use Computer Network Operations as a comparison. CNO has three enablers, Computer Network Attack, Exploitation, and Defense (CNA, CNE, and CND respectively). As enablers, CNO will continue to exist without CND, however, it is not fully enabled. Conversely, CyNetOps does not exist is one of its elements is missing; similar to the removal of an element of hydrogen from H2O, you no longer have water, you now have chemical compound HO. Just as water exists in the bonded mixture of H2O, CyNetOps exists in the bonded mixture of CyCM, CyNM, and CyD. It is the interrelationship of these three that births CyNetOps. Finally, these interrelationships form shifting supported and supporting responsibilities that must be understood and fostered by full spectrum CyNetOps.

MOS 255N, the second of two enlisted-level accessions MOS, is the Army's premier network transport technician responsible for voice, video, and data networks, establishing and maintaining the transport layer environment of Army's portion of the cyberspace domain through Network Management/Enterprise Systems Management (NM/ESM) functions to include fault management, configuration management, auditing and accountability measures, maintaining performance standards, and implementing security measures at all levels in support of combat information superiority and command and control. In short, the 255N owns CyNM.

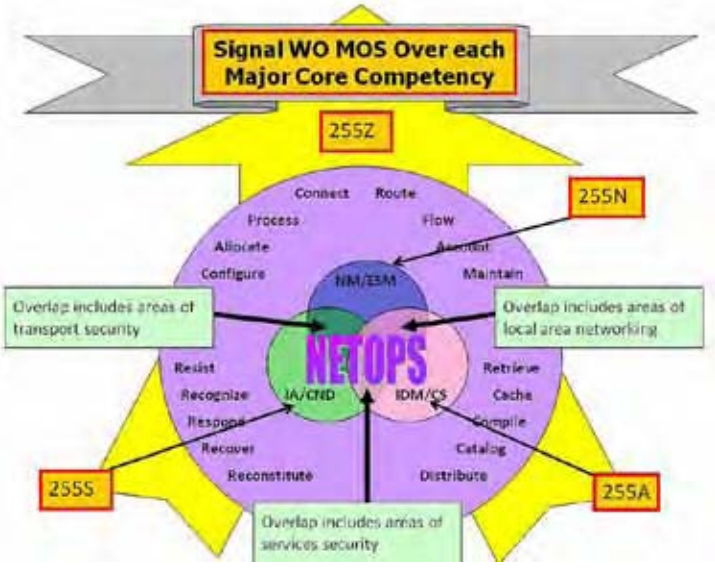



**Diagram 1**

I make the same caveat that I offered to the objective 225A; we are a formation still in motion. Doctrine, organizational designs, current systems and equipment, and legacy leadership ideology may still lag behind the below ideal and objective description of MOS 255N. As in MOS 255A, we are not able to make an immediate right flank, march.

Here too we are in the beginning of a column right, meaning you will wind some units who are able to immediately able to receive newly trained 255A, N, and S and employ them as detailed within this publication; they have already made the turn. Other units, however, will find themselves further back in the formation.

## Apprentice Cyberspace Network Management Technicians

To understand the apprentice level warrant officer, an understanding of the transition from Noncommissioned Officer to warrant officer fostered by attendance at the Warrant Officer Candidate School is helpful. WOCS continues to evolve to better align its philosophy and activities to meet the needs of an Army at war. The driving force is the desire to produce warrant officers better qualified to operate effectively in the demanding operational environment.

Following is a synopsis of the changes made in 2006 and the resultant WOCS in operation today.

While WOCS has adjusted and evolved through the years, 2006 marked another such notable year in its development. WOCS has always been associated with its physical rigor. Prior to 2006 physical training heavily focused on the Army Physical Fitness Test. An increase from entry level APFT scores to graduation APFT scores was a significant metric used to gauge its success. Goals included a desire to improve physical fitness, to improve candidates' understanding of the elements of fitness, and to prepare them to assist with their commander's fitness programs. Subsequent to the 2006 changes, PT became more warrior tasks and battle drills centered. The current goals of the WOCS APFT are to maintain and/or improve a candidate's state of combat readiness and to develop both foundational fitness and fundamental skills to prepare the officer leader for operational deployment.

The focus of the WOCS has gone through significant changes. Prior to 2006, many have said the course had a barracks centered focus. AC-RC differences along with the limited resident only training rendered its purpose and effectiveness questionable. Subsequent to changes made in 2006, most now say WOCS is developing officers. The inclusion of a distance learning phase to build experience and its field leadership exercise has added a credible amount of increased rigor.

As outlined on the Warrant Officer Career College website, the current WOCS focus emphasizes officer roles and responsibilities more, and individual activities less. Candidates are required to meet high standards for maintaining their personal living areas. However, the standards

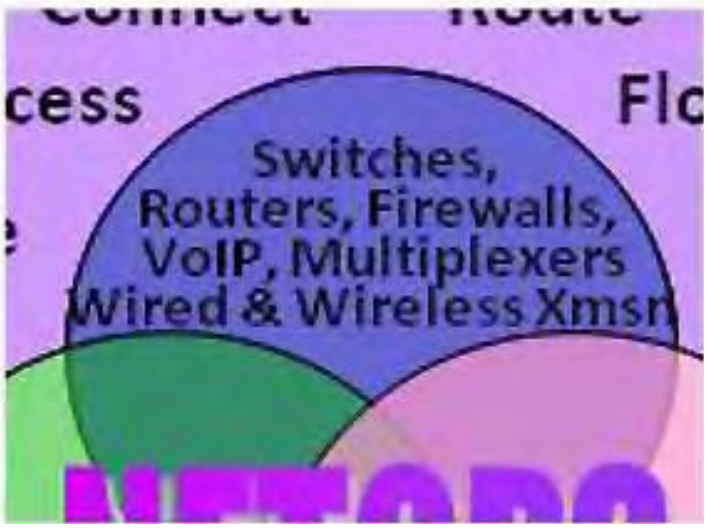



**Diagram 2**

are based on the need to maintain a clean and orderly living environment rather than what many in the past perceived as arbitrary specifications designed to heighten stress levels.

There are experiential learning events throughout the program, particularly warrior tasks and battle drill related activities that provide leadership opportunities while emphasizing lessons relevant to the OE. These activities culminate in a FLX that draws heavily on recent lessons learned. This capstone event provides candidates expanded opportunities to apply flexible, adaptive leadership principles in stressful, sometimes ambiguous, situations to reinforce and build upon previous classroom theory studies and discussion.

Training, advising, and counseling officers and academic instructors concentrate primarily on training and secondarily on assessing candidates' performance. This becomes apparent in the time and effort TACs and instructors devote to serving as role models, mentors, and coaches. Throughout all the changes, rigor is maintained—even increased—and the goal continues to be to provide candidates the foundation they need to succeed as warrant officers in a changing Army, and to be adaptable to the ever increasing challenges of the OE.

Having successfully completed WOCS and being appointed to WO1 in the U.S. Army, the junior 255N (i.e., W1 and W2) focus on acquiring and refining technical and administrative skills as they supervise and manage the operation and internetworking of telecommunications networks, networked information systems and equipment, networked transmission and transport systems, network management platforms, and associated personnel at both the local and wide area network level. Their focus is also mainly on the equipment and systems and how to leverage them to assist their commander to prosecute the wartime mission.

The apprentice CyNM averages 10 years active Federal

**(Continued on page 32)**

(Continued from page 31)

service with a minimum of four years documented practical experience in voice and data internetworking, local and wide area networks, and/or network planning. Additionally, he/she is most likely a prior staff sergeant and must minimally have at least 36 months of documented rated time as a leader as evidenced by official NCO evaluation reports.

The junior CyNM begins learning each and every 'subject' within the 'system.' As in the 255A, a WO1/CW2 255N, the "primary focus is becoming proficient and working on those systems linked directly to AOC/MOS" (DA Pam 600-3). During the initial assignment is the time for the junior CyNM to develop a foundational understanding of the devices and applications used in his/her system. Where they are assigned and how they are utilized will greatly impact their future careers. Accordingly, similar to the CyCM, the apprentice CyNM is nominally assigned to a brigade combat team where he/she has the greatest ability to encounter the widest array of devices and applications found within the breadth of his/her assigned systems. After five months in WOBC, the BCT provides the best opportunity to see his/her system put to use by its intended user – the combat commander. The astute apprentice CyNM uses this opportunity not only to provide the foundational training and experience in communications transport and networking systems that he/she will build upon throughout his/her career, but also becomes aware of the systems tactical purposes. He/she learns how to converse not only in IT communities, but also the tactics, techniques, procedures and vernacular of the combat arms community he/she enables.

The WO1/CW2 255N focuses on the install, maintain, and operate aspects of the system in which they are responsible. They are to focus on the individual pieces of their system, many of which they were trained on in their WOBC. Examples of such devices and applications in today's Army inventory includes (but is not limited to) VoIP call managers, firewalls, routers, switches, multiplexers, voice switches, various RF transmission systems, network management software, etc. Shifts in technology have begun to cause a shift in responsibilities that are covered under the MOS repurposing strategy of the Signal warrant officer. For example, tactical tadio communications systems have begun to become networkable devices meaning they are IP-enabled, node/PoP-self creating devices that inherently create cyberspace transport as they are operated. As such, they shift under the responsibility of MOS 255N. This shift causes the 255N to focus on transport, regardless of WAN or LAN architecture. However, information assurance activities have not, nor will they ever, shift to MOS 255S. MOS 255A Soldiers are fully responsible to posture their systems and ensure they remain compliant to all IA policies, practices, and governance.

Another example of a shift in capabilities that has second and third order effects to include influencing Signal warrant officers is that of frequency and spectrum management. In the past, select Soldiers were trained in frequency and spectrum manage-

**Senior warrant officers are immersed in the latest technology and most advanced systems when they attend their Professional Military Education course at the Warrant Officer Career College.**

ment, awarded additional skill identifier D9, and placed in our formations where these skills could be best leveraged. Today, the electromagnetic spectrum has become such a critical component of our portion of cyberspace that the level of training at an ASI producing course, along with the inability to track and ensure full utilization of personnel trained in such skills, does not meet the criticality and full spectrum of the requirement. EMS operations includes not only EMS management, but also incorporates electronic warfare and electronic protect. As such, an MOS is required to ensure EMSO as a whole is fully synchronized; MOS 25E, Electromagnetic Spectrum Manager has been created to synchronize EMS management to include cyberspace operations in and through EMS as well as EW operations and EP actions. However, MOS 25E will be an asset to the 255S as that is where the bigger view of the network is taken. This leaves a gap in frequency and spectrum management which must be filled by our 255N.

## Journeymen Cyberspace Network Management Technicians

The Mid-grade MOS 255N (W3) focus beyond the individual assemblages and systems to acquire skills in the individual attributes of CyNM (i.e., the science of NM/ESM) as well as the intricacies of the interrelationships with the other NetOps elements. This development prepares them to be true experts in their craft and advisors to senior leadership on complex and complicated NetOps issues.

Journeymen CyNM, similar to their CyCM counterparts, as advanced-level technical and tactical experts, now step slightly away from the devices, applications, and even the system they oversee and begin to seek an in-depth understanding of the principles and science behind their systems. Having gained expert experience in how these devices operate, they learn the deeper answer to why they were developed and how they are leveraged to transport data and information, or better yet, command and control.

The journeymen CyNM is also nominally assigned to a division or corps where he has the greatest ability to focus on the bigger picture. Still remaining close to the devices and applications within their systems of responsibility, they find themselves moving past the install, maintain, and operate mission and become involved with the planning and engineering of transport services and enterprise level network management for larger organizations. In preparation for the demands of such assignments, these CyNM will attend the 255N Warrant Officer Advance Course.

Prior to WOAC attendance, enrollment into the Action Officer Development Course (131 P00) must occur after promotion to CW2 in order to qualify for WOAC Prerequisite Studies credit. Journeymen 255Ns attending their resident WOAC will find project management and enterprise level transport systems and integration, along with advanced routing, VoIP, security, QOS techniques, and transport systems as key technical components taught to prepare him to fulfill their ever expanding duties. The Army senior leadership has taken a renewed interest in warrant officer Professional Military Education. ALARACT 362-2010, Officer and Non Commissioned Officer PME Backlog Definitions, specifically calls out warrant officers stating, "All AC and RC warrant officers will complete WOAC prior to promotion to CW3." This ALARACT also states the requirement to attend WOSC prior to promotion to CW4 and the WOSSC prior to promotion to CW5. More on this subject is covered in the article on the Army's senior cyberspace network operations technician – MOS 255Z on page 48.

The journeymen CyNM's credibility is very high in such organizations and the influence they have cannot be underestimated. Mentorship of apprentice CyNM becomes an inherent part of their duty description. They also begin to gain more uniformity in the supporting and supported roles of their peer Signal warrant officers, the 255A Cyberspace Content Management Technicians and the 255S Cyberspace Defense Technicians. No longer do they focus their duties and responsibilities on their systems solely. Now they begin to fully understand that the transport networks they are entrusted to establish, maintain, and manage are meaningless if they fail to move data and information to the intended destination and/or become exploited or manipulated by a cyberspace adversary. Journeymen CyNM seek out professional forums to ensure they remain informed on technology advancements and trends as well as opportunities to further their educational training through university courses and civilian certification programs.

Finally, some journeymen CyNM may, similar to their peer 255As, feel a pull toward the Cyberspace Defense arena. It is at the beginning stages of his journeyman phase (senior CW2 or junior CW3) where one may make the decision to move from the CyCM to the CyD realm. The future decision point will normally be just prior to WOAC attendance. The expected prerequisites for such a transition along with the planned board process will be discussed in a later article.

## Master Cyberspace Network Management Technicians

**(Continued on page 34)**

(Continued from page 33)

Senior 255N (W4), having mastered assemblages, systems, and CyNM attributes, move from the outer edges of the CyNM circle in the NetOps venn diagram toward the center. They are now moving from mastery of one element toward the goal of W5--mastery of NetOps. While definitively a master CyNM, CW4 255N also serve as "technical leaders, sustainers, and advisors" to the commands to which they are assigned.

Master CyNM, as senior-level technical and tactical experts in their chosen field, have also gained familiarity with the other two elements of NetOps (i.e., CyCM and CyD). As they continue to develop as CW4 255N, they go beyond understanding the basic concepts of assured information delivery and assured system and network availability and ensure that these attributes of NetOps are obtained. As in master level CyCM, while there is never an expectation of finger-pointing between the three associated skill-sets and/or MOS, master CyCM takes ownership of these concepts and relationships (as do each of our Signal warrant officer MOS) and in the absence of each sister MOS, takes charge. When all three MOSs are present, the conscious shared desire for synergy is the goal.

The master CyNM is nominally assigned to a Corps, ASCC, or higher level organization where his/her training and experience has its greatest impact. To prepare the CW4 255N for the duties and responsibilities encountered at these levels of organization, attendance at the Warrant Officer Staff Course is crucial.

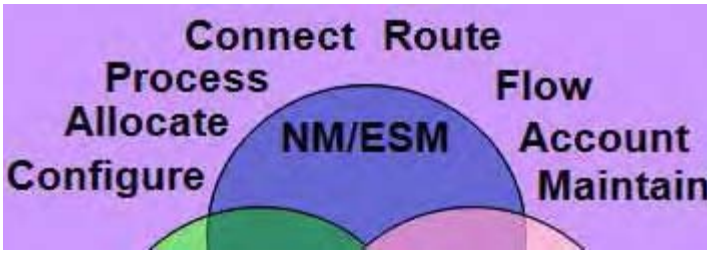



**Diagram 3**

The master CyNM is the Army's premiere resource of intellectual capital ensuring the Army meets its future demands throughout cyberspace. We are facing a crisis. Commercial technology has easily outpaced the technology used by the Department of Defense. Our war fighting commanders have expressed their recognition of the value of leveraging new technologies on the battlefield. Within the DOD, cyberspace security and defense are a matter of life and death in some cases. Therefore, we must make wise decisions when adapting and leveraging new technologies. Furthermore, we cannot shirk from the responsibility to ensure our Armed Forces have the best capabilities when they enter into engagements.

Subsequent to promotion to CW5, the master CyNM become part of an ever smaller, elite group of Signal warrant officer, the Cyberspace Network Operations Technician, MOS 255Z. For further information on MOS 255Z, an article summarizing the career paths and describing the skills, attributes, duties, and responsibilities is included on page 48 of this edition of the *Army Communicator*.

Join the Discussion
https://signallink.army.mil

## Acronym QuickScan

**AC** – Active Component
**ALARACT** – All Army Activities
**AOC** – Area of Concentration
**APFT** – Army Physical Fitness Test
**ASI** – Additional Skill Identifier
**BCT** – Brigade Combat Team
**CyCM** – Cyberspace Content Management
**CyD** – Cyberspace Defense
**CyNetOps** – Cyberspace Network Operations
**CyNM** – Cyberspace Network Management
**CyNOT** – Cyberspace Network Operations Technician
**DoD** – Department of Defense
**EMS** – Electromagnetic Spectrum
**EMSO** – Electromagnetic Spectrum Operations
**FLX** – Field leadership exercise
**IA** – Information Assurance
**IP** – Internet Protocol
**IT** – Information Technology
**LAN** – Local Area Network
**MOS** – Military Occupational Specialty
**NCO** – Noncommissioned Officer
**NCOER** – Noncommissioned Officer Evaluation Report
**NetOps** – Network operations
**NM/ESM** – Network Management/ Enterprise Systems Management
**OE** – Operational Environment
**PME** – Professional Military Education
**PoP** – Point of Presence
**PT** – Physical Training
**QOS** – Quality of Service
**RC** – Reserve Component
**RF** – Radio Frequency
**TTP** – Tactics, Techniques, Procedures
**TAC** – Training, Advising, and Counseling
**VoIP** – Voice Over Internet Protocol
**WOAC** – Warrant Officer Advance Course
**WOBC** – Warrant Officer Basic Course
**WOCS** – Warrant Officer Candidate School
**WOS** – Warrant Officer Service
**WOSC** – Warrant Officer Staff Course
**WOSSC** – Warrant Officer Senior Staff Course
**WT&BD** – Warrior Tasks and Battle Drills

# Cyberspace defense technician (MOS 255S)

*By CW5 Todd M. Boudreau*

## Where We Were

The analogy in this article is like a parable that will help you understand the multidimensional arena into which the Army is deploying expert cyberspace defense technicians.

To fully grasp the analogy you have to understand that our current cyberspace defensive measures are almost entirely reactive in nature.

Most often, adversarial activity is identified by the loss of critical data and/or the malicious manipulation of data elements and devices. After the fact, forensics often discover that such adversarial activity had been going on for quite a significant amount of time before it was discovered. At this point a "signature" is created and placed in devices that are used to look for such adversarial activity. These devices look at current activity and if any matches this "signature" they then alert and activate devices that detect or in some cases prevent further adversarial activity. If placed on a scale in its simplest of forms, it would look something like figure 1 below.

Having established a protected posture, we scan our networks for evidence of adversarial activity by comparing cyberspace activity against our current signatures and various indications and warnings established and in place at the time. Once an adversary has established intent to attack our networks, an operational preparation of the environment sets the way for an attack which then may present a viable avenue to exploit our networks and extract critical information. Once an attack and/or exploit are defeated, we begin the process of remediation to correct any faults, deficiencies, and/or vulnerabilities that created the threat. The defeated adversary then slightly changes the toolset in order to launch a new attack. More sophisticated adversaries create toolsets that automatically morph on their own in order to prevent detection or the capability of the remediation from being successful.

Finally, as the effects of Army transformation and technological advances have caused MOS 254A to shift into a role that mirrors MOS 251A, when both MOS were present in the same organization, the 251A has historically gravitated toward the NetOps elemental gap of Information Assurance and Computer Network Defense (IA and CND respectively). However, few 251A were properly trained and none received any institutional training. Furthermore, few 251A were able to ensure consecutive assignments in such positions making it difficult to impossible to build upon skills and experience.

## Where We Are Heading

The current methods are completely inadequate for a variety of reasons. First, we cannot afford to allow adversarial activity to occur unnoticed for any amount of time before we detect and take action. Second, more and more we find our adversaries are using polymorphic malware which means that the adversarial activity continues changing to make it almost impossible to stop with signature-based defensive measures. Instead, we need to begin focusing on

**(Continued on page 36)**

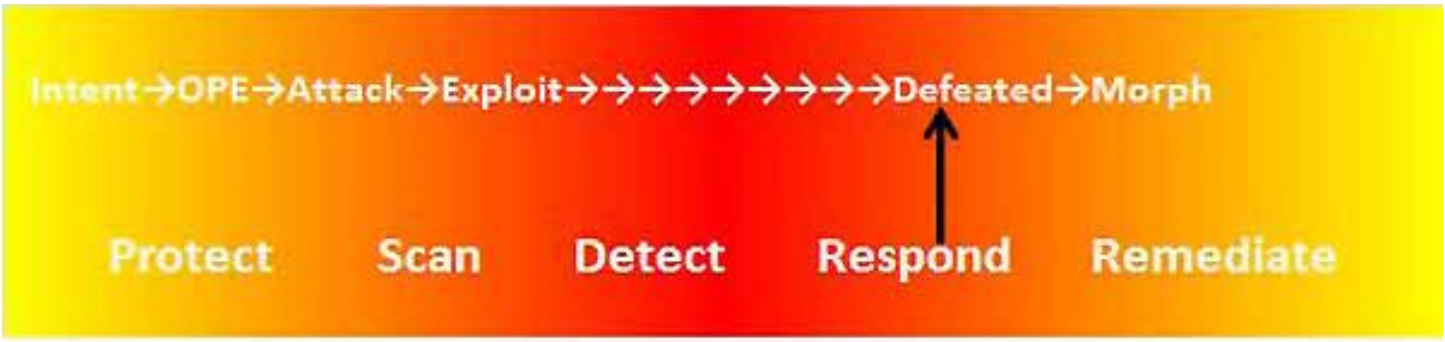



Figure 1 Current Scale Comparing Attack and Defense Cycles

(Continued from page 35)

anomalous activity.

This is not an entirely new concept. Credit and banking systems have been doing this for years. Recently when my credit card had been refused, I immediately contacted my financial institution. They asked me two questions: had I recently charged $1 to a common on-line DVD and Blu-ray disc rental-by-mail and video streaming company and had I recently charged $1 to a not-so-common on-line clothing store. I had done neither. This activity was uncommon to my nominal purchasing history and was viewed as an anomaly. This caused my credit card to be flagged. With a credit card, no funds are immediately transferred. Therefore, they were able to put a hold on my account and eventually disapprove the transactions with no money lost.

I advocate an anomaly based cyberspace defensive posture that moves the "detect and respond" further to the left of the attack cycle as illustrated below in figure 2. However, this calls for some changes in operations. Instead of the adversarial attack or exploit tipping our defensive measures, we must respond to the adversarial OPE. Let me make this clear with the analogy.

## Defending a Field

Some have described the nature of cyberspace defense as trying to find a needle in a pile of needles. The point of this illustrative presentation is that there are so many alerts to possible malicious activity on our networks, we are consumed wading through the plethora of false positives (i.e., alerts, indications, and warnings that turn out to be nothing) and/or inconsequential positives (i.e., those that are of little to no concern) that we miss the truly important indications and warnings allowing adversarial activity to continue unchecked for an unacceptable amount of time.

We miss the truly important alarm in the midst of the overwhelming noise of alarms. This needle in a pile of needles illustration accurately presents the issue at hand. Finding the important alert amongst the blaring myriad of alerts is truly like trying to find a special needle in a pile of needles, which also continues to grow in number by the minute. While this illustration has a lot of merit under these circumstances, much more needs to be understood beyond this one critical issue – especially in order to best present the need and capability of the Army's expert cyberspace defense technician.

Imagine a field of grass where each blade is part of an integrated and monitored root system. Any pressure on the field has the ability to trip a sensor and send a warning of a presence upon the field. An adversary wants to step on our field and disrupt, exploit, or destroy those operations which we conduct on and through this field.

However, to step on even a single blade may tip off his presence. So he introduces malicious grass seed into our supply of grass seed. The sheer amount of grass seed sowed into the field makes it impossible to verify every single seed. As the malicious seed begins to grow and take root, it soon provides a patch of grass that allows the adversary a foothold on our field.

Before we get to advancing the "detect and respond" to the left, we must add two exasperating situations. First, the field has also become overgrown with weeds and saplings providing our adversaries cover as they step onto the patch of malicious grass. Secondly, the current field includes friendly plots of sod which are not centrally managed by the larger defender of the field itself.

For unveiling the analogy, let me reveal here that these patches of sod represent the disparate networks that are currently kluged together within the confines of Army cyberspace. And finally the weeds and saplings are the result of poor IA practices. IA practiced upon cyberspace has been likened to preventative maintenance checks and services. Taking a higher view of IA, I include not only patching and IA vulnerability alert response compliance, but also total asset visibility and network transparency.

At the most recent Signal conference at Fort Gordon, MG Rhett Hernandez, Army Cyberspace Command commanding general, mentioned three interrelated aspects of one significant effort that is necessary as part of mak-


Figure 2 Future Scale Comparing Attack and Defense Cycles

ing cyberspace securely operational. The first two are to know ourselves and to know our enemy. The third is know the terrain one intends to defend. We must first see our cyberspace terrain if we are to effectively defend our cyberspace terrain.

Setting these two immense problems aside (i.e., disparate networks and poor IA), let's revisit that analogy to ensure we are tracking. The seeds represent normal network traffic that is nearly impossible to detect in advance of an attack even if it is malicious. For example, I am not talking about spam or low-tech phishing attacks. I am instead alluding to highly sophisticated attempts to attack our networks through e-mail traffic (for example) that have been crafted by a high-tech peer adversary. Most experts today admit this cannot be stopped. But the e-mail is only carrying a malicious seed that by itself is yet inert. However, as it begins to grow and root, before it has time to become a patch that allows even a toehold, it must be detected and defeated.

In the physical domain of the field of grass in my analogy, the first step is to establish a field-of-fire. Basic warrior tasks and battle drills teach a couple of basic principles in establishing a field-of-fire. First, one must determine how big the field can be and still be scanned effectively against the adversary. Second, one ensures overlapping fields-of-fire to prevent against a seam (at best) or a gap (at worst) which could allow the adversary an avenue of approach through our defenses. If the magnitude of adversarial activity that is to be detected is as small as a blade of grass, the field-of-fire must be small enough to remain manageable.

In the cyberspace domain, we must also default to these basic level cyberspace WT&BD and establish fields-of-fire that are manageable and include overlapping and interlocking fields-of-fire. These malicious e-mails don't plant grass. They plant hooks that provide a point of presence in our networks and data devices. Our cyberspace defenders must be able to scan their sector and detect such malicious PoPs in order to defeat them while the adversary is still in the OPE phase of the attack. Cyberspace defenders must see these hooks as anomalous to their cyberspace fields-of-fire.

One last thought is appropriate before moving on to the practical aspects of discussing MOS 255S. To quickly identify an anomaly, one must be able to quickly discount what is normal. Begging your patience to use another analogy, if someone is going to quickly, efficiently, and effectively defend your office building against a physical attack, such as an explosive device, they best know what normal looks like. Each desk, each box, each copy machine, each piece of furniture or physical structure that could be a fake planted by an enemy and secretly housing an explosive device should be readily identifiable by the defender if one plans to be successful. Similarly, if our cyberspace defenders are not familiar with the network and networked data devices, they are ill prepared to notice an anomaly during the OPE phase of the adversarial attack.

For the best defense posture, cyberspace defenders must live in the space they are assigned to defend. They must sense the anomaly within the normal as early as possible – before the adversary even gets a toehold. Know that we must move forward in this direction immediately. We have no time to wait. We are unquestionably beyond phase zero in cyberspace operations conducted in and through the cyberspace domain today.

## Enter the Cyberspace Defense Technicians

The below NetOps construct in figure 3 continues to show its three elements which are also the Regiment's three major core competencies. Previous articles have already addressed MOS 255A (responsible for Cyber Content Management) and MOS 255N (responsible for

**(Continued on page 38)**

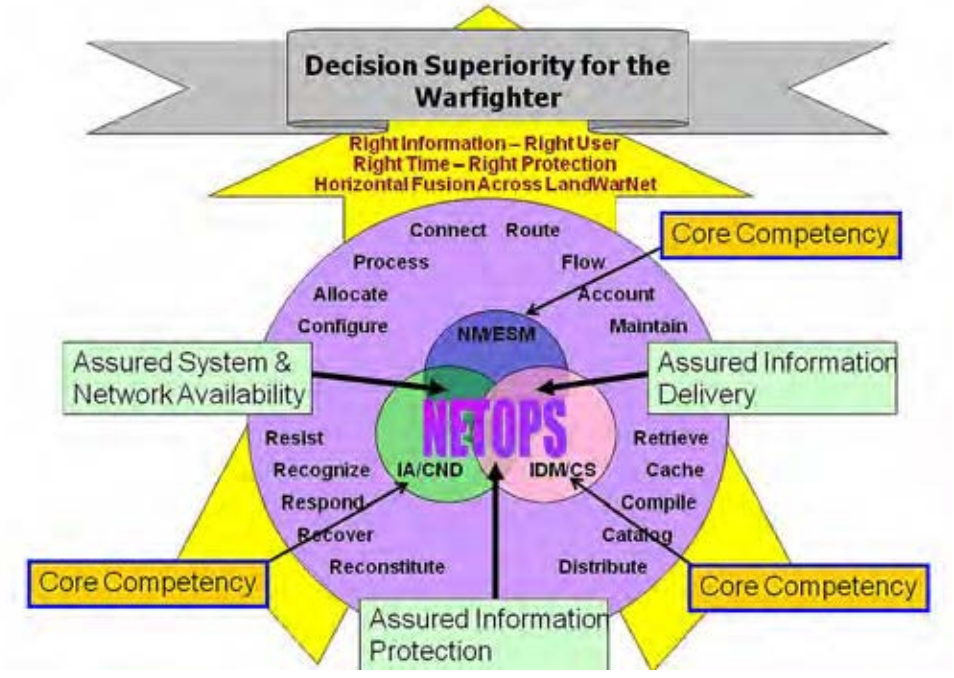



Figure 3 Network Operation Construct

(Continued from page 37)

Cyber Network Management); the last article in this particular series will address MOS 255Z (responsible for Cyber NetOps (CyNetOps) in its entirety).

This article now moves to describe MOS 255S (responsible for Cyber Defense) as the newest personnel capability added to the Signal warrant officer cohort.

As we began to look at the capability gap at hand (IA/CND), we made a couple of decisions up front. First, we realized the need to move from a perimeter-positioned and reactionary defensive model to an internally proactive, anomaly based, true defense-in-depth model. Second, knowing the interdependencies of CyD, CyCM and CyD, CyNM, we concluded the need for a more senior and experienced personnel base. Third, we acknowledged the current standard of CyD training to be in the hands of our commercial IT partners. Finally, we recognized the necessity of partnering with our Intelligence Community partners who can provide actionable intelligence relative to our adversaries' intent--their tactics, techniques, and procedures; and any real time feedback on both their current activities as well as their knowledge of ours.

A properly trained and deployed MOS 255S force will be key in meeting the first issue above. In order to move to an internally proactive, anomaly based, true defense-in-depth model, we need an intelligent personnel capability to be a part of the solution set.

To ensure that CyCM and CyNM efforts are not negatively affected, but supported and reinforced, it was decided that MOS 255S would not be an enlisted-level accession MOS. Instead, accessions into MOS 255S will be at the senior W2 grade. This is in line with preferred attendance at the Warrant Officer Advance Course. This ensures newly reclassified 255S have a greater understanding of their actions and the suggestions they make in the CyCM and CyNM areas to better posture for defense. Training will be discussed below. However, the requirement for all 255S to hold a top secret clearance with the ability to be read on to special compartmentalized information is of utmost importance. This allows the IC to feed actionable intelligence into the CyD cell.

Since there are no apprentice cyberspace defense technicians, it is imperative that we get our training right. The transition course from MOS 255S will also serve to give advance course credit (i.e., it will also function as a WOAC).

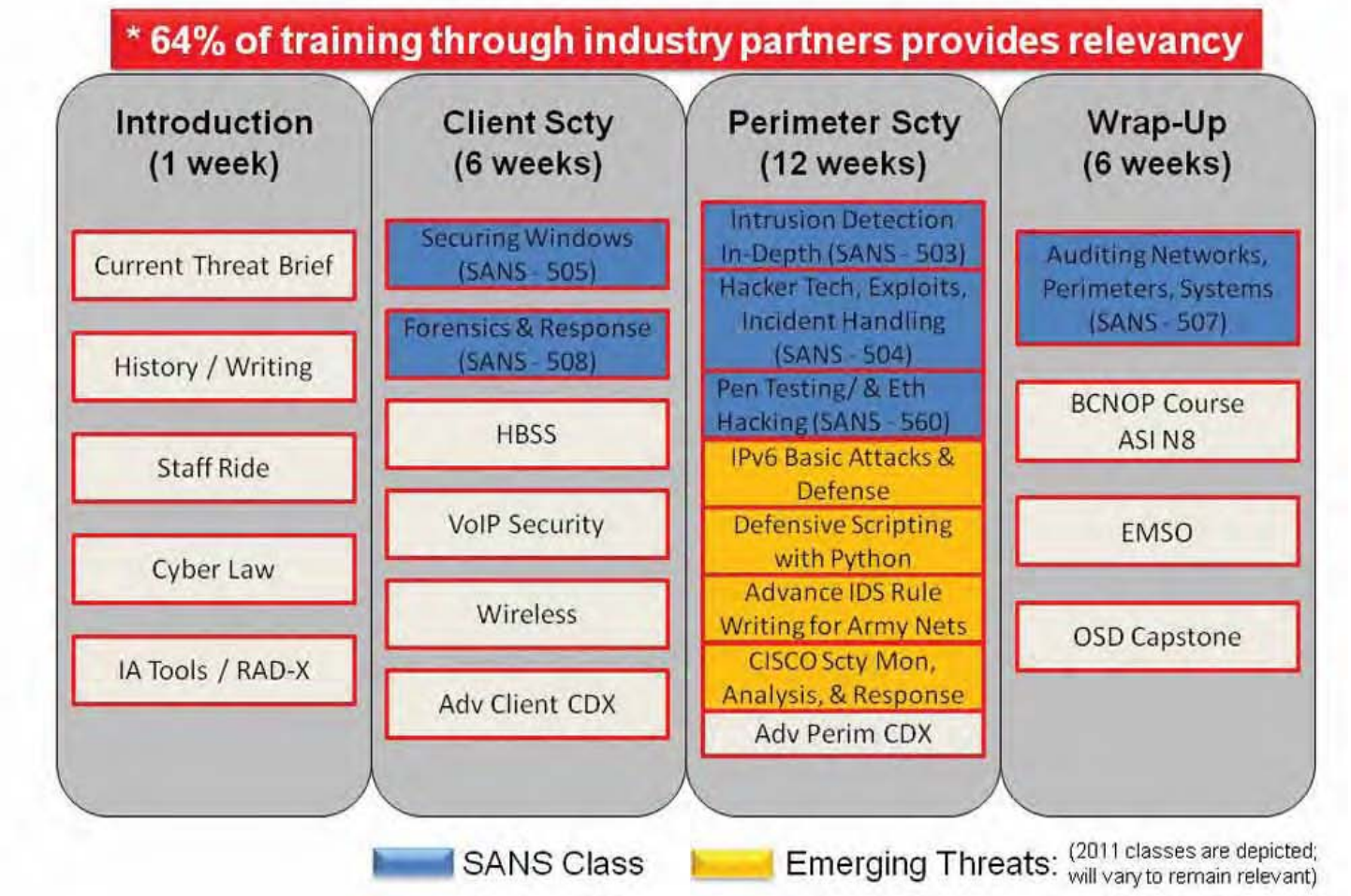



Figure 4. Current 255S Pilot Course Training Course Map

The most credible and holistic CyD training currently resides in the hands of our commercial IT partners. CISCO has a robust perimeter security track of training and the SANS Institute has a number of courses that meet both our client and perimeter training needs as well as a number of other very specific areas to be addressed. Figure 4 below is our current 255S course map.

## Journeyman Cyberspace Defense Technicians

MOS 255S are the Army's premier defenders of the Army's portion of the cyberspace domain. They perform computer network defense measures and advise information assurance measures and actions to include the protection, detection, and reaction functions at all levels in support of combat information superiority. Junior 255S (i.e., W1 and W2) do not exist. Instead, junior WOs who may look to access into 255S should focus on acquiring and refining technical and administrative skills within their respective MOS (i.e., 255A or 255N). As they develop these skills and achieve mid-grade CW2 status, should they desire to pursue MOS 255S, they should begin self-study in the cyber defense field, seek to find a senior 255S as a mentor, and look to fill information assurance management positions that will lead them to meeting the 255S prerequisites. IAM positions may be either focused on IA compliance in CyCM or CyNM.

Mid-grade 255S (W3) advise information assurance efforts while focusing on their associated sub-element (i.e., cyber defense) as well as non-lethal electronic protection efforts. They supervise associated personnel and oversee functions within the standards, transport, services, and applications layers of the network in order to achieve confidentiality, integrity, and availability of information, as well as the authentication and non-repudiation of users. They also supervise and/or oversee subordinate sections required to support information protection and network defense such as communications security sections, cryptographic network planning, and electromagnetic spectrum operations to achieve electronic protect, and the implementation and use of electronic keys required supporting communications networks and networked-systems. See figure 5.

It is imperative that commanders and senior leaders understand that MOS 255S will not oversee IA compliancy. MOS 255S are required to know normal and hunt in our portion of cyberspace to identify and defeat adversarial activity. Not all adversarial activity will be defeated. The 255S provides the Signal Regiment a basis to enter into full-spectrum cyberspace operations with our IC partners. The use of deception, cyberspace counter-fire, and adversarial cordoning are just a few of the TTPs a full-spectrum cyberspace operation may use. Therefore, to limit MOS 255S to IA is a colossal waste of talent and completely misses the point of the MOS. Journeymen 255S may advise IA and analyze IA deficiencies to give the "so what" to their respective commanders. They are able to determine the difference between vulnerability and an actual threat and can provide mitigation courses of action.

These journeymen 255S perfect the art of knowing normal by a continued and in-depth analysis of the various feeds received from sensors, data devices, and actionable intelligence received from various IC sources. Unlike the CyCM and the CyNM, it is the journeymen CyD who is nominally assigned to a brigade combat team where he/she has the greatest ability to encounter the widest array of devices and applications found within the breadth of his/her assigned systems. This also makes the 255S the senior Signal warrant officer in most formations. Journeymen 255S also find themselves in theater network operations security centers, regional computer emergency response teams, and a number of similar hands-on organizations to include as high as combat divisions.

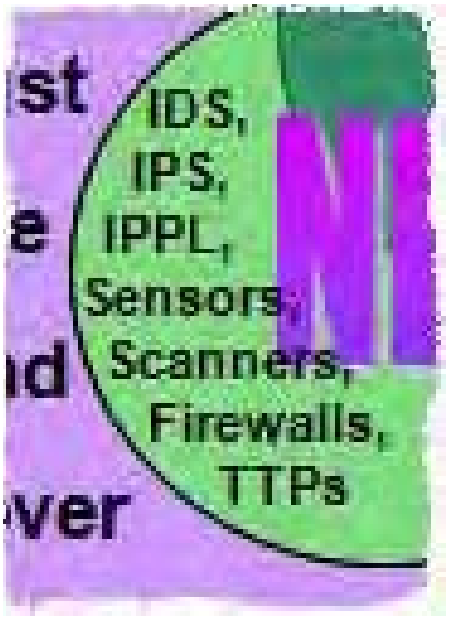


Figure 5

## Master Cyberspace Defense Technicians

Senior 255s (i.e., newly promoted W4), quickly master applications, techniques, systems, and CyD attributes which include actions to resist, recognize, respond, recover, and reconstitute. Highly specialized and highly motivated, they quickly inculcate these and move from the outer edges of the CyD circle in this Venn diagram toward the center. They too are now moving from mastery of one element toward the goal of W5--mastery of NetOps.

Master CyDs, as senior-level technical and tactical experts in their chosen field, have also gained familiarity with the other two elements of NetOps (i.e., CyCM and CyNM). As they continue to develop as CW4 255S, they go beyond understanding the basic con-

**(Continued on page 40)**

(Continued from page 39)

cepts of information protection and assured system and network availability and ensure that these attributes of NetOps are obtained. See figure 6. Their prior experience as either 255As or 255Ns is key to their rapid expansion of knowledge.

The master CyD is nominally assigned to a corps, ASCC, and higher level organization where their training and experience has its greatest impact. To prepare the CW4 255S for the duties and responsibilities encountered at these levels of organization, attendance at the Warrant Officer Staff Course is crucial. The master CyD will be, without argument, today's intellectual capital to ensure the Army not only meets its future demands within and through cyberspace, but that it is secured and defended. While this may not be a new problem-set, its scope has grown significantly. Past generations of Signal equipment were mainly proprietary and circuit-switched. As such, the obstacle between our adversary and our critical systems was quite large and almost insurmountable. Mobile subscriber equipment and TRI-TAC systems were proprietary and not easily reproducible by others. A significant amount of intellectual capital and funding were required to acquire, reverse engineer, fabricate, and reproduce such equipment by our adversaries. Additionally, the circuit-switched nature of MSE and TRI-TAC networks made it very difficult to introduce rogue equipment into our networks with the intent to exploit or disrupt.

Today, these barriers have all but disappeared with our reliance on commercial off-the-shelf equipment. Almost anyone with inclination can find a virtual potpourri of attack toolsets from which to choose. A malicious personality merely chooses from a variety of desired cyberspace effects much like one picks from an assortment of foods at al buffet restaurant. Attribution is made difficult with the virtual, non-contiguous, yet ubiquitous nature in which cyberspace presents itself. One merely needs to walk into a busy hotel and use the hotel's business center as a platform to launch a cheap, unsophisticated, yet often effective attack against our networks.

Presently, even a low-tech attack often overwhelms our primarily reactive defenses inundated with a myriad of false-positives. This creates another source of noise that helps to mask more complicated, high-tech, peer adversarial activity. IA compliance may lower the noise-floor making the former easier to spot, identify, categorize, and remediate. However, more complicated, high-tech, peer adversarial activity requires an expert cyberspace defense technician who is fully equipped, informed and actively hunting anomalies within our complex networks and systems.

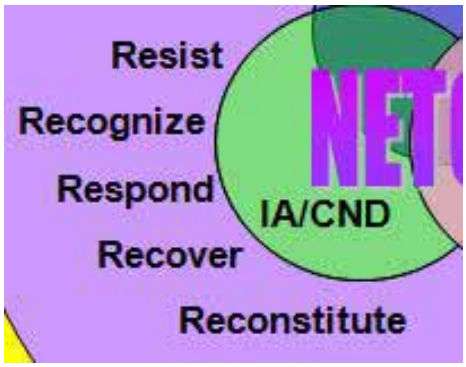



Figure 6

Subsequent to promotion to CW5, the master CyD also becomes part of an ever smaller, elite group of Signal warrant officers, the cyberspace network operations technician, MOS 255Z.

As will be done for all 255Z, senior leadership will be cognizant of their past MOS and as such leverage their knowledge, skills, attributes, and experience for future assignments. For further information on MOS 255Z, an article summarizing their career paths and describing their skills, attributes, duties, and responsibilities is included on page 48 in this edition of the *Army Communicator*.


## Acronym QuickScan

**ARCYBER** – Army Cyberspace Command
**ASCC** – Army Service Component Command
**CND** – Computer Network Defense
**COMSEC** – Communications Security
**CyCM** – Cyberspace Content Management
**CyD** – Cyberspace Defense
**CyNetOps** – Cyberspace Network Operations
**CyNM** – Cyberspace Network Management
**CyNOT** – Cyberspace Network Operations Technician
**DVD** – Digital Versatile Disc
**EMSO** – Electromagnetic Spectrum Operations
**IA** – Information Assurance
**IAM** – Information Assurance Management
**IAVA** – Information Assurance Vulnerability Alert
**IC** – Intelligence Community
**MOS** – Military Occupational Specialty
**MSE** – Mobile Subscriber Equipment
**NetOps** – Network operations
**OPE** – Operational Preparation of the Environment
**PMCS** – Preventative Maintenance Checks and Services
**PoP** – Point of Presence
**R-CERT** – Regional Computer Emergency Response Team
**SCI** – Special Compartmentalized Information
**T-NOSC** – Theater Network Operations Security Center
**TS** – Top Secret
**TTP** – Tactics, Techniques, Procedures
**WOAC** – Warrant Officer Advance Course
**WOSC** – Warrant Officer Staff Course
**WOSSC** – Warrant Officer Senior Staff Course
**WT&BD** – Warrior Tasks and Battle Drills

# Social Network Privacy

Overcoming Facebook policies that put users at risk

*By CW3 Elbert Peak*

## Facing the Facebook Privacy Dilemma

On-line social networking has benefits but also risks to be considered when using such sites as Facebook.

Internet privacy threats are a challenge that is impossible to completely mitigate on every social network, but there are steps one can take to significantly reduce the risks.

## The Rise of Facebook

Facebook is one of the largest web sites in the world. The site was started in 2004 by Mark Zuckerberg when he was an undergraduate student at Harvard. The site grew rapidly to include hundreds of millions of users.

Since September 2006, anyone over the age of 13 with a valid e-mail address can join Facebook as a user. Users can add friends and send messages and announcements, and update their personal profiles to notify friends about themselves. Social networking giant Facebook registered its 500 millionth member, the firm announced in July 2009.

Its millions of users around the world have reason to limit visibility of their personal information from the total World Wide Web but still want to be able to share that information with trusted contacts. Facebook became a huge success on that premise and ought to be able to continue thriving without doing an about face on privacy.

Humans are social beings and most seek some engagement with others. Facebook uses a social graph, which is the global mapping of people and how they're connected. Sociologists have been studying these graphs for decades. Famously, the social networks have a Small World Property--more widely known as the Six Degrees of Separation. This is both an anecdotal and scientific observation that we all are connected to each other--no more than six people away. What is the secret? It's because this is how human networks form. Dense clusters are interconnected by shortcuts.

There is a social networking privacy premise that people have the right to control their "private space."

The argument is generally upheld that "private space" is presumptuous and a user's right to control. You have privacy to the extent you control who is allowed into your "zone of inaccessibility." Discussions about privacy revolve around the notion of access, where access means either physical proximity to a person or knowledge about that person. The lack of privacy often makes individuals vulnerable to having their behavior controlled by others. Social networking is built on the ideology of sharing information and personal data. Users share a variety of information about themselves on their Facebook profiles, including photos, contact information, and tastes in movies and books. It's meant to be social.

**(Continued on page 42)**

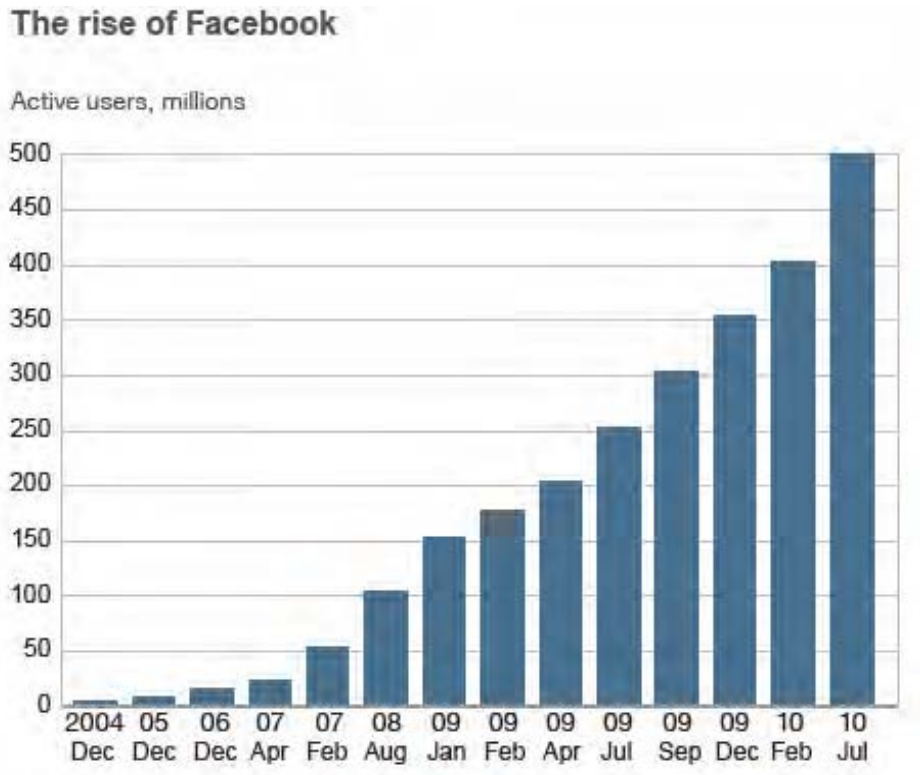



Diagram 1

(Continued from page 41)

# Facebook: Threats to Privacy

End-users share a wide variety of information on Facebook, but a discussion of the privacy implications of doing so has yet to emerge widely. I examined how Facebook affects privacy, and found serious flaws in the system.

Privacy on Facebook is undermined by three principal factors: users disclose too much, Facebook does not take adequate steps to protect user privacy, and third parties are actively seeking out end-user information using Facebook. With this much detailed information arranged uniformly and aggregated into one place, there are bound to be risks to privacy. Users may submit their data without being aware that it may be shared with advertisers. Third parties may build a database of Facebook data to sell. Intruders may steal passwords, or entire databases, from Facebook. Although many Facebook features empower users to control their private information, there are still significant shortcomings.


Facebook's privacy features give users a good deal of flexibility in who is allowed to see their information. The privacy settings page allows a user to specify who can see them in searches, which can see their profile, which can see their contact info, and which fields other users can see. In addition, the privacy settings page allows users to block specific people from seeing their profile. In the usage agreement, a user can request Facebook to not share information with third parties, though the method of specifying this is not located on the privacy settings page.

There are a number of systems changes that can be made, to give the user a reasonable perception of the level of privacy protection available, and to protect against disclosure to intruders.

### Brief Technical Description of Facebook

Facebook uses server-side hypertext preprocessor scripts and applications to host and format the content available on the service. Content is stored centrally on Facebook servers. Scripts and applications at Facebook acquire, process, and filter information on-demand, and deliver it to users in real time, to a Web browser over the Internet. Users begin their Facebook session at the service's top level site, http://www.facebook.com/.

At the main Facebook page, a user can log in to the service, or browse the small amount of information available to the general public. The main page of the service is simple, and does not provide any personally identifiable information or technical insight. During the login process, the service provides the user's web browser with some information, which is stored in the form of a cookie. Some of this information, such as the user's e-mail address, is written to a file so the user does not have to enter his or her e-mail at the next login.

Facebook's service creates and gives a user a unique checksum at every login, which the browser stores as a session cookie and generally does not write to a file. This checksum varies from login to login, but other parameters do not. Once logged in to the service, a user is free to interact with Facebook. The user may edit their profile, look at others' profiles, add or change their friends lost or personally identifiable information, and explore the service.

The core of the Facebook platform is the open graph application programming interface, which enables read and write data to Facebook. The open graph API allows applications, pages, Websites, and other software services to add Facebook features, like the "Like" button, to their own sites. Taking actions on other sites results in those actions being shared with your friends on Facebook, and may allow friends on those sites to see what you're doing also.

Every object in the social graph has a unique ID. You can fetch data associated with an object by fetching https://graph.facebook.com/ID . Alternatively, people and pages with usernames can be fetched using their username as an ID. All responses are JavaScript Object Notation objects. JSON is a lightweight text-based standard designed for human readable data interchange.

It's derived from the JavaScript programming language for representing simple data structures and associative arrays, called objects.

## Metadata in Facebook

Society spawns one gigantic social graph. In this graph, each one of us is a node. There is an explicit connection, if we know each other. For example, two people can be connected because they work together or because they went to school together or because they are married. Everything has an array of likes, friends, and recommendations stored within a social graph. User-contributed (or generated) metadata is the high value, structured matter that allows ads, and the overall user experience, to be more personalized. As the social Web evolves, privacy and metadata ownership issues will continue to produce friction in the system.

In effect, Facebook is building an identity graph, not just a social graph out of an individual's metadata. A key issue going forward is whether and how users become the control point for their online identities, including all the metadata that sites collect.


## Aggregation of Facebook Data

Could a more sophisticated aggregation of Facebook data allow privacy to be exposed? Facebook CEO Mark Zuckerberg says he is providing "the power to share in order to make the world more open…"

Facebook's advanced search allows one to query the database of users via any of the fields in a profile. The problem is compounded by a security hole that multiple people have discovered. The likebutton.me (http://likebutton.me) site created by Zachary Allia and itstrending.com (http://itstrending.com) site created by Matt Schlicht aggregates shared objects from Facebook's recommendation plug-ins (plug-in to make website content socially relevant) across online media websites. Both show the same data just in similar interfaces, displaying what your friends are "liking" and otherwise sharing on different sites. These sites aggregate data and displays in real time feed of most shared content on Facebook (vid-

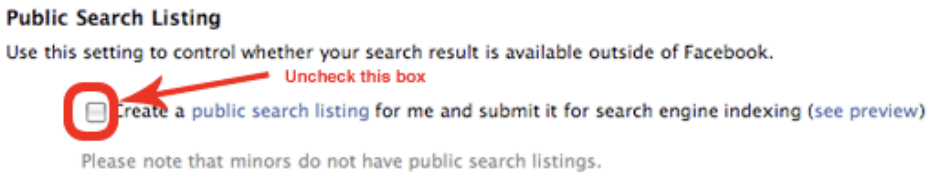
**(Continued on page 44)**


realized that this is a scary privacy issue," Bowes wrote. "I can find the name of pretty much every person on Facebook."

Bowes said Facebook users can change their settings so they do not appear in the public directory going forward, but even people who do that now will have their information available via Bowes' torrent file available on the file-sharing site Pirate Bay. There have been more than 10,000 downloads of the file.

"Once I have the name and URL of a user, I can view, by default, their picture, friends, information about them, an

(Continued from page 43)




eos, news, images, entertainment, gaming, etc). This is all possible by using publicly-shared data by users and their friends, based on each user's social graph. You must be logged into Facebook to see personalized results on these widgets.

Apparently two developers, Will Moffat and Peter Burns, (and possibly a third, James Home used for designing) built the site Youropenbook (http://youropenbook.org) to demonstrate how public our Facebook information really is.

One person stated online that "I'm willing to put myself out there on Facebook and other social networks and online sites, so to me, social media privacy can be a bit of an oxymoron no matter how many privacy settings I activate on Facebook."
The website Youropenbook is a demonstration of lack of privacy in Facebook.

With this site you can search public Facebook updates using Facebook's own search service. By using the Open Graph API, developers can make searches of public timeline information without logging into Facebook. Developer Timo Paloheimo did just that by creating the Open Facebook Search at http://openfacebooksearch.com. This website opens up new possibilities for developers to create totally new services on top of Facebook's data. Now you can embed Facebook searches to any website.

Another tool for searching public data on Facebook can be accessed at http://zesty.ca/facebook. This site was created by another developer, Ka-Ping Yee, using the Open Graph API. Try entering your name or e-mail address, your friends' names or e-mail addresses, or any keywords. Use the button to search for users, posts, events, groups, or pages. You might be surprised at what is publically available. Many users allow their status updates, likes, and other activity to be public without knowing.
Developers are using the available documentation from Facebook to make this happen. See http://developers.facebook.com/docs/api.

## Facebook Data Found on Pirate Bay

Last summer Ron Bowes, a Canadian security consultant and Nmap developer, used a piece of code to scan Facebook profiles, collecting data not hidden by user's privacy settings.

To figure out if your name is on the list released by Bowes you can either download the file or check your settings on Facebook. To do that, click on the "Account" pull down menu on the upper right of your Facebook page and click on "Privacy Settings." Then select "Basic Directory Information" and "View Settings." If "Search for me on Facebook" is marked for "Everyone," your information might be on the list.

## Avoid Facebook Account Hacks

Hackers are enticing Facebook users to install an application pitched as a "Dislike" button that jokingly notifies contacts at the social networking service "now I can dislike all of your dumb posts." Once granted permission to access a Facebook user's profile, the application pumps out spam from the account and spreads itself by inviting the person's friends to get the button, according to Sophos. Beyond tricking a user into completing a survey, and hence gaining access to your profile and the ability to spam your friends, there doesn't appear to be much about the scam that's dangerous.

Eventually, after the user completes the survey, it does redirect to FaceMod, the maker of a Facebook-based "dislike" button that takes the form of a Firefox browser plug-in. Sophos points out that the scam does not appear to have any direct connection to FaceMod.

Many of the malware applications reported spam by Facebook users have been taken down by Facebook. But still the thing to worry about is that the Facebook profile spying spam is not spreading through apps only, in fact it is spreading with the help of Facebook Events, Pages and groups too. So Facebook needs to filter out those spam pages, groups and events too.

Most of the profile spying groups, pages and app take you to a page that's completely filled with advertisements and affiliate links. Quite often they ask users to complete certain offers or surveys (see screenshot above) after which users end up passing their important information to the spammers or downloading infected files to their PC.

You will find a large number of Facebook pages, groups and apps that claim to tell users about who checked/viewed their profile. Actually they all are spam. Their sole purpose is to get a large user following by tricking people and then directing them all to pages heavily loaded with advertisements which in turn generates revenue for them. Facebook itself says that there is no way at all with which you can see/check who is visiting your Facebook profile. This is

what Facebook's recent status updates state about this rapidly growing spam.

Another attack that is trending is the clickjacking attack. This Facebook attack uses iFrames, which essentially places an invisible button over an entire web page, so that wherever the user clicks, they end up hitting the button - in this case a hidden Facebook "like" button. Many types of operations can take place from this type of attack hidden from the user, sometimes resulting in a cross-site scripting attack. Usually this type of XSS attack will bypass client-side security and malicious scripts on web pages can be executed on the end-user's computer.

### Tag…You're It!

This is the classic Facebook problem. You let loose for a few hours one night and photos or videos of the moment are suddenly posted for all to view, not just your close friends who shared the moment with you. The result can be devastating. Some have been fired from work after incriminating photos/videos were posted for the boss to see. For others, randomly tagged photos/videos have ended relationships. You should have to approve a tagged picture before it goes up rather than having to check periodically to see if any pictures are something you do not want posted. In which case you have to "un-tag" the photo and possibly report it.

You control who can see the photos and videos you tagged to appear on your profile. Remember, the owner of a photo can still share that photo with people who are not your friends.

If you don't want your tag to appear, remove it from the photo or video itself. This will also prevent it from appearing on your profile. The "My Photos" service allows users to upload, store and view photos.

Users can append metadata to the photographs that allows other users to see who is in the photographs, and where in the photograph they are located. These tags can be cross-linked to user profiles, and searched from a search dialog. The only recourse a user has against an unwelcome Facebook photo posted by someone else, aside from asking them to remove it, is to manually remove the metadata tag of their name, individually, from each photograph. Users may disable


others' access to their Wall, but not to the Photos feature.

### Check-in Versus Tagging

So, since check-ins is also presumably mobile posts, wouldn't that also mean they exist outside a user's privacy settings? If so, this could be a big issue for Places; and defensible territory for Foursquare and Gowalla. The difference between being checked-in and being tagged can be confusing. If you're checked-in by yourself or by a friend, your presence at the location is visible to anyone that either you or your friend allows, based on your friend's and your privacy settings. Your name will show up on the location's Places page, if there is one, so everyone at the location can see that you're there. If you are tagged by a friend, your presence at the location is seen by your friends or whoever they allow to see their posts, subject to their (not your) privacy settings. Your friends' apps may be able to access information about your most recent check-in by default.


### Recommended Facebook Privacy Settings

Currently the information displayed in the search profile is limited to: your profile picture, a list of your friends, a link to add you as a friend, a link to send you a message, and a list of up to approximately 20 fan pages on which you are a member. To increase your privacy settings, it is necessary to select the custom settings and modify each setting individually. If you want to

**(Continued on page 46)**


**(Continued on page 45)**

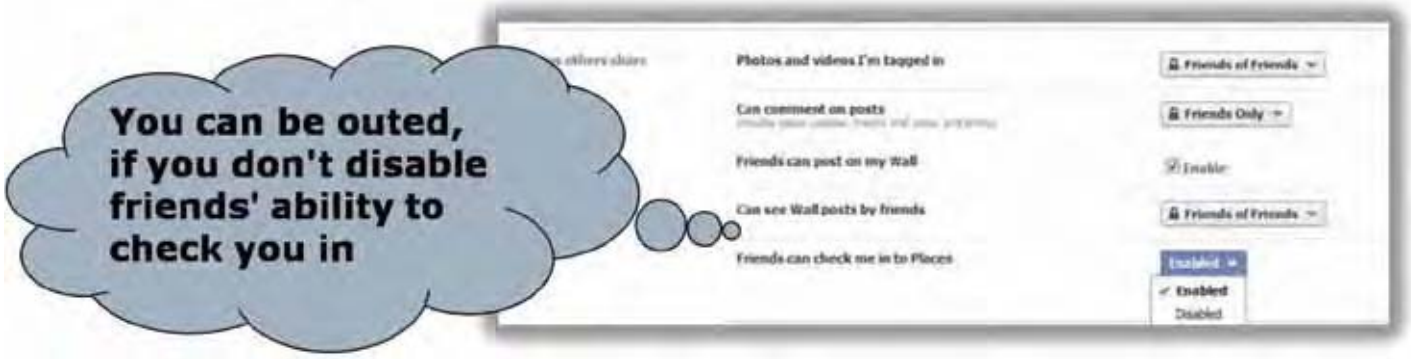
have full control over who sees your profile, meaning that only people you have chosen will be able to see any part of your profile, choose "Friends only." Towards the bottom of the settings, uncheck the box that states "Let friends of people tagged in my photos and posts see them." Then click on "Apply These Settings."

Many open source tools are available for use to help alleviate these problems in Facebook settings. Developer Matt Pizzimenti, cofounder of Olark.com, created an independent and open tool (Reclaim Privacy Scanner) for scanning your Facebook privacy settings. To keep the privacy scanner up-to-date, all development will remain open and transparent. Source code is maintained at http://github.com/mjpizz/reclaimprivacy and uses a JavaScript file named "privacyscanner.js" about 8,167 lines of code as of today. The tool is used for scanning Facebook privacy settings and fixing unexpected privacy holes. This scanner is not fully compatible with the latest Facebook privacy settings, so be sure you check your privacy settings manually yourself. The tool can be downloaded from http://www.reclaimprivacy.org.

Another open source tool named SaveFace, provided by Untangle is a simple to install bookmark utility that automatically resets Facebook settings to restore your privacy. SaveFace sets your privacy settings back to Friends only, for all the following: contact information, search settings, friends' tags and comments, personal information and posts. Best of all, it's free. Untangle collects no personal information from you or your Facebook when you use this bookmark utility. SaveFace can be downloaded from http://www3.untangle.com/saveface.

Here are some tips for using any social network:

- Set appropriate privacy and security controls; use complex passwords; separate e-mails
- Don't install third party applications from




sources you don't trust

- Only accept friend requests from people you know directly
- Read and understand privacy policy and terms of service carefully
- Consider everything public; be careful what you post
- More at: http://socialmediasecurity.com

For a more in-depth reference on Facebook privacy settings, one should visit http://www.wikihow.com/Manage-Facebook-Privacy-Options and http://www.facebook.com/fbprivacy.

## Conclusion

In an environment of growing Facebook information misuse, Facebook would do its users a great service to explain the dangers of security breaches and outside monitoring. Until the societal norms regarding this new use of computers become well-established, Facebook could clearly state that they can provide no guarantees regarding the security of their data, and that if users make their profiles public, all information contained therein may be viewed by anyone. Ultimately, lasting change in online privacy will only come from a gradual development of common sense regarding what is appropriate to post in social networking forums. Unfortunately, this is not an easy fix.

***CW3 Elbert Peak*** *is assigned as a cyber security instructor at the School of Information Technology, Fort Gordon, Ga. He recently completed a 10 month train-the-trainer program for the new Warrant Officer 255S Information Protection Technician MOS course. Since joining the Army in 1988, CW3 Peak has worked in many areas of information technology including networking, systems administration, and information assurance. He holds a Bachelor's degree in Computer Science from University of Maryland, a Master's degree in Computer Information Systems from Florida Institute of Technology, and a Master's degree in Software Engineering from California State University, Fullerton.*

# Cyberspace network operations technician (MOS 255Z)

*By CW5 Todd M. Boudreau*

This article details the events that shaped development of the Army's senior cyberspace network operations technicians, MOS 255Z and outlines the shifting responsibilities that are making repurposing of the MOS necessary.

## Where We Were

To understand the MOS 255Zs' evolution, it is essential to consider the legacy enlisted-level accessions MOS and identify some difficulties in the past. Then we will be able to share strategies for mitigating past deficiencies that evolve around the new concepts for W5 capper MOS 255Z.

Simply put, MOS 250N has primarily focused on the wide area network design and implementation. Most Signal warrant officers who have been in the field for the last decade recognize the clear line of demarcation between the 250N and the 251A. This line has been drawn between the WAN, or the outside network and the metropolitan, campus, and/or local area network (MAN/CAN/LAN), or the inside network. The line of effort for the 250N focuses on reach-back (or in some cases reach between) while the LOE for the 251A is on the "backside" network design and implementation, essentially connectivity within an organizational structure.

The problem at hand is that technology and current networking trends serve to blur these lines. For example, the DROID, one of the latest among the smart phones, has the ability to enable itself as a wireless fidelity hotspot. It then can be connected to (i.e., organizational structure) as well as networked through (i.e., reach-back). As the Army's premier cyberspace network management technicians begin to see these devices, technologies, and techniques on the modern cyberspace battlefield, they must embrace both aspects and take ownership of transport regardless of user, organization, or level of network.

MOS 251A technicians have primarily focused on data systems and data systems integration. However, such a focus has often required appreciable time and effort performing MAN/CAN/LAN design and implementation. Although networking basics are taught in both the Warrant Officer Basic Course and the Warrant Officer Advance Course, it has often left the 251As to learn and discover much on their own. This is because the immediate access layer and distribution layer network routers and switches that their application systems connect to in a MAN/CAN/LAN environment, have been viewed as a part of the 251A's system.

Concurrently, the MOS 254A environment has shifted from duties that were envisioned back in its inception to those which mirror the 251A. MOS 254A was designed to be the Signal technical expert in non-Signal, maneuver formations responsible for areas such as maneuver Signal operations, combat net radios, communications security, and Signal support to tactical operation centers. Since its inception, however, several significant shifts have occurred. First, the bandwidth and computing power of today's digital TOC has increased to equal (and in some cases surpass) that of the nominal center in which MOS 251A is found. Second, Army transformation and modularity have all but negated the terminology "non-Signal maneuver formation." The brigade combat team today has unique organic Signal support. Therefore, MOS 254A has shifted to overlap MOS 251A in more than 80% of all critical tasks. Today, when MOS 251A and 254A are both collocated in a section, the

**(Continued on page 36)**

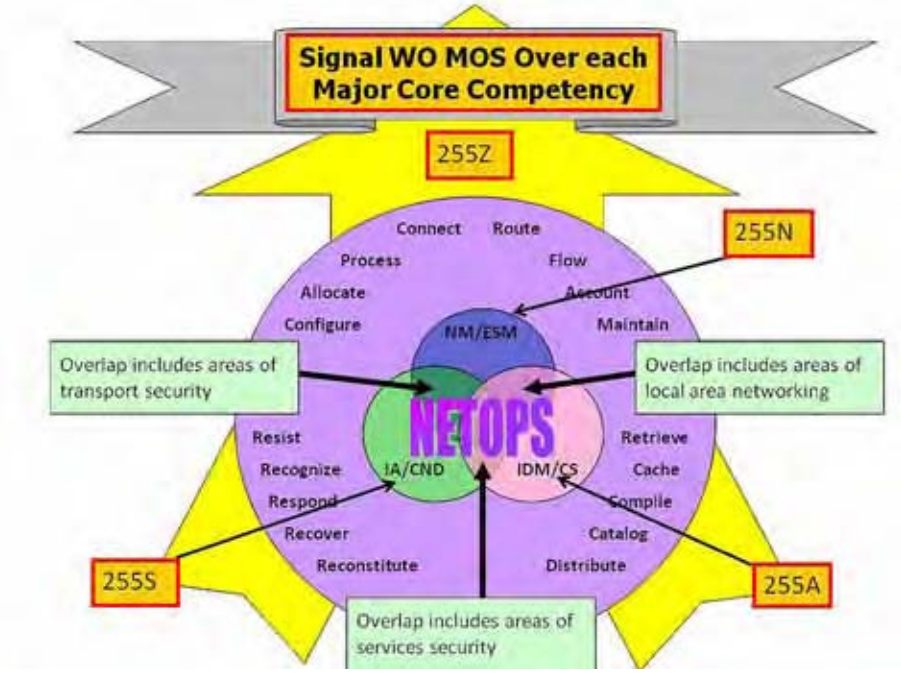



Figure 1

254A technician most often takes responsibility for the servers and services while the 251A technician takes ownership of IA.

Most of our 255Z technicians have progressed through career paths that often lacked true career progression as a goal, with a propensity to myopically move into a single-track. The small numbers of W5 authorizations in the Signal Regiment may have not only allowed this, but in some cases exasperated this. However today there is a huge shift in progressing from this point. Now Signal warrant officers are promoted to the rank of CW5 with extremely varied and diverse backgrounds. While the nominal senior CW4 has tracked within a single MOS, for the most part, the constantly changing world of cyberspace and the fact that many have found themselves having to learn the theory and skills of their sister MOS has created senior Signal warrant officers who are able to interact quite intelligently in each of the elements of NetOps. This has created a whole new dynamic in our senior Signal warrant officer population that is beneficial to the Signal Regiment and the Army as a whole.

A few other areas of influence affect our future. There is a massive change occurring in the OE in which we find ourselves. The OE which existed from the Korean War through the cold war era, was characterized as having predictable requirements, moving at a slow developmental pace of technology, and existing with a myriad of specialized expertise in single areas; often dislocated with each other. Subsequent to that period our OE has shifted to one of vastly unpredictable requirements, moving from fairly well known technologies to one of a rapid and dynamic pace of technological change. Today our OE shifts from understood and accepted cylinders of excellence to the necessity of highly specialized skills that also have a broader understanding of full spectrum operations (i.e., one that is prepared for and can em-

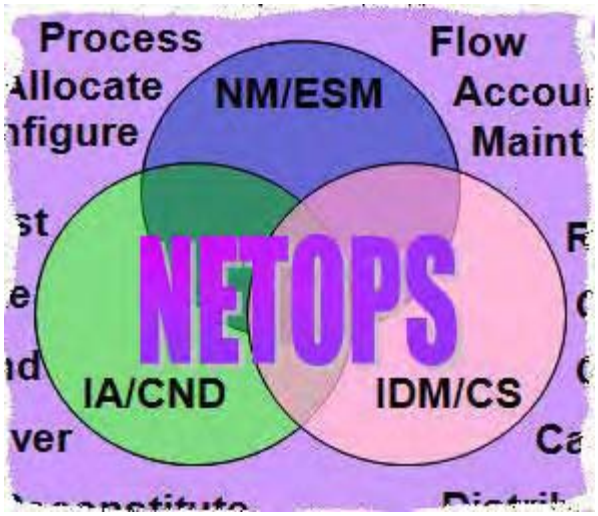



Figure 2

brace ambiguity, together). Finally, in today's state of constant military activity, our Army's senior leaders have declared that our OE will remain unpredictable with noted characteristics and influences such as the exponentially expanding role of technology, the necessity to understand and make use of cultural differences and influences, and the greater role of joint, interagency, intergovernmental, and multinational cooperation.

I learned new terminology at our Signal Center's Signal Conference last December. The acronym VUCA was used to express our new OE as Volatile, Uncertain, Complex, and Ambiguous. This change from predictable to unpredictable, from static to dynamic, from simple to complex requires a whole new way of growing our Army's senior leaders, including senior Signal warrant officers.

Today we must ask the question "Is our current Professional Military Education able to prepare our Army's warrant officers for such an OE?" And we also must ask ourselves, "Do we have formalized career paths, to properly grow and develop our Signal warrant officers in a manner that ensures they will have the requisite knowledge, skills, and attributes to be successful in senior positions where we are currently looking to assign them?"

Let's look more closely at these questions along with some related concerns.

## Where We Are Heading

MOS 255Z technicians, a W5 capper MOS for 255A, 255N, and 255S, will use decades of ever-widening NetOps experiences to focus past the individual applications, systems, and equipment to shape the intricacies of the interrelationships with the other NetOps elements. Such officers will be the true experts and masters in their craft and advisors to senior leadership on complex and complicated NetOps issues. As such, repurposed and properly developed MOS 255Z technicians will be the Army's premier technical and tactical advisors for full spectrum network operations at any echelon of command or support activity of the U.S. Army or joint staff sections assigned to theater combatant commanders or allied armies.

The NetOps construct includes all three elements in the cyberspace realm--CyCM, CyNM, and CyD. Although NetOps manifests itself only within the coordinated synergy of these three elements, the true goal is to center NetOps on the mission and intent of the war fighting commander. It is the ability to properly position the synergy of the NetOps center-of-mass that makes the 255Z a force multiplier and an invaluable asset. (See figure 1)

Serving at corps, ASCC, DRU, and joint levels, the 255Z provides leadership, guidance, technical input, and direction to subordinate elements, staff agencies, and field commanders while providing leader development, mentorship, advice, and counsel to NCOs, other WOs, and branch officers. MOS 255Zs have special mentorship responsibil-

**(Continued on page 50)**

(Continued from page 49)

ities for other WOs at all levels and provide essential advice to commanders on Signal technical and WO issues.

MOS 255Zs continue to sharpen their knowledge of personnel force integration functions for doctrine, training, and personnel as it pertains to the Signal Corps. In addition, 255Zs gain and maintain familiarity: (1) with the constitutional, statutory, and regulatory basis for the force projection Army and the capabilities that are sustained through management of doctrinal, organizational, and materiel change; (2) with Army organizational roles, functions, and missions, especially at the ACOM/ASCC/DRU and Army Secretariat/Staff levels; and (3) with the force management processes, from the determination of force requirements through the resourcing of requirements and the assessment of their utilization in order to accomplish Army functions and missions in a JIIM environment.

Until recently, we have had less than 15 CW5 positions in the Signal Regiment. (See figure 2). We were doing well to have 8-10 CW5s to put into them. Today, we are in the process of growing from 16 positions to 28-30 positions. We can do this for two reasons. First, 3.5 percent of a total warrant officer branch population can be W5 positions. Second, we have grown in our total population from less than 400 Signal warrant officer authorizations in the Active Component in 2001 to well over 800 today. We will do this, however, for two other reasons. First, we need to provide our highly qualified Signal warrant officers who have demonstrated potential the ability to compete for promotion in a reasonably competitive yet equitable manner. Second, many units are requesting a senior Signal warrant officer (i.e., CW5) due to the attributes displayed by our current population of CW5s.

In the past, we have had Signal CW5 positions in Signal brigades and a smattering of other places around the Army and DoD organizations. We are moving and growing positions to the corps level and above. (See figures 3 and 4) Note that all "newly grown" positions require a "bill payer" position (i.e., one that is already authorized which must be converted to a CW5 position.)

## Signal WO Restructure: Current CW5 Positions

| | |
|---|---|
| US ARMY SIGNAL COE | REGIMENTAL CWO |
| US ARMY SIGNAL COE | OCOS CAREER PRG MGR |
| US ARMY SIGNAL COE | TECH DIR |
| 741 MI BN | COMSEC TECH |
| US ARMY ALLIED FORCES | COMSEC IMPLMT |
| US ARMY FORCES CMD | DATA PROC TECH |
| US FORCES KOREA CMD | OIC, COMSEC MGMT OFF |
| US ARMY CENTRAL CMD | MCP, SR SIG TECH |
| US ARMY EUROPEAN CMD | 7TH ARMY MCP, SR SIG TECH |
| US ARMY PACIFIC CMD | MCP, SR SIG TECH |
| US ARMY NET ENTPRS TECH CMD | 9TH SC(A), SR SIG TECH |
| 7TH SIGNAL CMD | SR SIG TECH |
| 7TH SIGNAL BDE (5SC(T)) | SR SIG TECH |
| 11TH SIGNAL BDE HHC | SR SIG TECH |
| 1ST SIGNAL BDE HHC | SR SIG TECH |
| 35TH SIGNAL BDE HHC | SR SIG TECH |

Figure 3

## Senior Cyberspace Network Operations Technicians: Masters of Their Arts

Who are these senior cyberspace network operations technicians that are being requested? What makes them such a desired commodity? First are their knowledge, skills, and attributes.

Today's senior Signal warrant officers are quite different from those of the past.

Today's senior Signal warrant officers are among the most experienced Army officers with more than a decade of combat operations under their belts. They have usually attended their WOAC, WOSC, and/or WOSSC) in the last four years, and thus are among the most experienced and highest educated our Army has ever seen.

Their knowledge in communications theory is unsurpassed. With the recent changes to WOBC and WOAC and the new WOSC branch follow-on course that will begin soon, it is only getting better. The practical skills these senior Signal warrant officers possess have been shaped and sharpened through over a decade of wartime experience. Finally, our professional development and the rise in overall professionalism within the warrant officer cohort have instilled a set of officer attributes that is unparalleled.

Our senior warrant officers are performing in a superlative manner even as they are handling more responsibilities and greater authority. They are not shunning such levels of responsibility, but instead are thriving on it.

Over and over again senior Army leaders (i.e., O-6 and above) have told me how the senior Signal

warrant officers not only bring practicality and relevancy into their organizations, but how they are often the unsung heroes who tackle any problem, no matter how complex, and provide some of the best solutions.

## So What is Left?

There is much left to be improved. Warrant officer education, professional development, and career opportunities still have much to be improved. The Military Occupational Classification Structure action that was submitted in 2009 to repurpose the Signal warrant officer MOS is only a beginning to the adjustments that need to be made to formulate better and more concise career paths to fully develop our senior warrant officers to their fullest potential.

Although it is improved, PME is another area that still requires much work to provide our future senior Signal warrant officers the level of education required to better prepare them to fulfill the duties and responsibilities that will be demanded of them.

Future senior warrant officers have a bright outlook for promotions and advancements.

In the career path, the on-going MOCS action has begun a three phase effort to better structure our Signal warrant officer career management field. It began by re-establishing specialized expertise in single areas. However, a great difference is that by following the NetOps construct these highly specialized areas mature into a required broader understanding of full spectrum operations (which also introduces greater ambiguity which much be addressed in the warrant officer's professional development). The goal is to grow our warrants into a systems integrator-manager role that can operate in either a joint, strategic, operational, or tactical arena. This is a role that requires greater JIIM/cultural understanding. Key developmental positions will be crucial to ensuring our future senior Signal warrant officers are fully developed and prepared to meet the highest command positions in our growing inventories.

Concurrently, our PME must provide our junior warrant officers a world class 'education' as they progress. Over the last two decades as a warrant officer I have seen our PME move from on-the-job training to a more formalized education system. Due to the dynamic pace of technological change, our current and future OE requirements mandate a formal education in theory and principles rather than hands-on or OJT. Furthermore, the expanded leadership roles of our current senior warrants, coupled with the constantly expanding technological infrastructure of our weapon systems and ill-structured problem sets they will face will make complex problem solving a critical skill by leaders who are increasingly comfortable with ambiguity. Senior warrant officer training must produce warrant grade officers who are adept with the conceptual, complex, and critical thinking skills to ensure they are adaptive, innovative, and creative thinkers.

Coupled with formalized PME and key developmental positions will be specialized training to include expanded training with Industry; advanced civil schooling; intermediate level education; and the School for Advanced Military Studies. Signal warrant officers already have a base of approved TWI programs. However, to better prepare our junior warrant officers for more of the critical senior positions, we need to look at doubling our current authorizations.

While warrant officers are included in the ACS program, not one has been funded according to any recent historical document. The ACS program not only acts as an incentive to keep some of our best Signal warrant officers, but it also provides critical graduate and post-graduate educational skills necessary to meet the demands of a number of our more specialized positions.

Finally, attendance at ILE at Fort Leavenworth, Kan., would not only prepare our senior warrant officers who are assigned to positions such as the CIO/G6, G3/5/7, and the G8, but it would be most appropriate. After all, the senior grade officers that sit to their left and right have all had the benefit of such an educational experience.

While rare, there are a very small number of high level highly specialized positions where SAMS attendance would round out the warrant officers' KSAs and prepare them to function at such a level and be of great benefit to the organization as well. These are not too lofty goals. We have had

**(Continued from page 52)**

**Signal WO Restructure:**
**CW5 Position Growth – Phase I**

| Phase 1 | |
|---|---|
| JOINT | |
| 1 | USCENTCOM |
| 2 | USEUCOM |
| 3 | USPACOM |
| 4 | USSOCOM |
| 5 | USAFRICOM |
| 6 | USCYBERCOM |
| 7 | SHAPE |
| 8 | CIO/G6 |
| ASCC | |
| 9 | USFORSCOM |
| 10 | USARCENT |
| 11 | USAREUR |
| 12 | USARPAC |
| 13 | USASOC |
| 14 | USARCYBER |
| 15 | INSCOM (704) |
| 16 | NETCOM |

| Phase 1 (cont.) | |
|---|---|
| ASCC | |
| 17 | 7TH SC(T) |
| 18 | 5TH SC(T) |
| 19 | 311th SC(T) |
| 20 | EUSA |
| CORPS | |
| 21 | I CORPS |
| 22 | III COPRS |
| 23 | XVIII CORPS |
| 24 | V CORPS |
| TRADOC | |
| 25 | RCWO |
| 26 | OCOS |
| 27 | SIT |
| 28 | CDID |

Figure 4

(Continued from page 51)

no less than 14 warrant officers attend ILE in the last three years (5 in 2009, 9 in 2010, and 3 in 2011). We currently have four warrant officers teaching logistics electives at the Command and General Staff College. We also have three warrant officers currently attending SAMS.

In conclusion, it is a fact that promotion to W5 has become a very competitive event due to the growth of the warrant officer cohort over the last 10 years. CW5(Ret) Andy Barr's article on page 16 addresses the changes in the promotion zones that have taken place to help grow senior warrant officers. He also spoke a little about the issues that we are beginning to face such as over strength of W4s and W5s in some branches. The Army is currently trying to balance several objectives: (1) to maintain the competitive nature of our senior promotions while (2) maintaining the potential for those who are best qualified to expect such future promotions and (3) maintain the average distribution grade matrix as required by law. To date, the Army has not reset the zones of consideration to meet the objectives described here. However, it has published an all ALARACT message that addresses the current backlog in PME and applies some very forceful language as to when warrant officers are expected to attend required training.

Finally, this year's promotion board will stress enforcement of the selective continuance requirement. The board has also lifted the suspension on SELCON for W4s who have been passed over twice for W5 (in an attempt to address numbers two and three above). The Army's goal is to reduce the W4 population in those branches that are over strength while maintaining a best qualified, competitive board process for those officers with the greatest potential for advancement. Currently, the Signal Regiment is still short W4s and W5s and as such should fare well through these shaping functions.

**Signal WO Restructure:**
**CW5 Position Growth – Phase II & III**

| Phase 2 | |
|---|---|
| JOINT | |
| 29 | USNORTHCOM |
| 30 | USFK |
| 31 | DISA |

| Phase 3 | |
|---|---|
| JOINT | |
| 32 | USSOUTHCOM |
| 33 | NSA |
| 34 | WHCA |
| ASCC | |
| 35 | USARNORTH |
| 36 | USARSOUTH |
| 37 | 335th SC(T) |
| 38 | AMC |
| 39 | USARAF |
| 40 | USARSTRAT |
| TRADOC | |
| 41 | HRC |

Figure 5

Join the Discussion
https://signallink.army.mil

## Acronym QuickScan

**ASCC** – Army Service Component Command
**BCT** – Brigade Combat Team
**CAN** – Campus Area Network
**CGSC** – Command and General Staff College
**CNR** – Combat Net Radio
**COMSEC** – Communications Security
**CyCM** – Cyberspace Content Management
**CyD** – Cyberspace Defense
**CyNetOps** – Cyberspace Network Operations
**CyNM** – Cyberspace Network Management
**CyNOT** – Cyberspace Network Operations Technician
**DoD** – Department of Defense
**DRU** – Direct Reporting Unit
**IA** – Information Assurance
**ILE** – Intermediate Level Education
**JIIM** – Joint, Interagency, Intergovernmental, and Multinational
**KSA** – Knowledge, Skill, and Attribute
**LAN** – Local Area Network
**LOE** – Line of Effort
**MAN** – Metropolitan Area Network
**MOCS** – Military Occupational Classification Structure
**MOS** – Military Occupational Specialty
**NCO** – Noncommissioned Officer
**NetOps** – Network operations
**OE** – Operational Environment
**OJT** – On the Job Training
**PME** – Professional Military Education
**SAMS** – School for Advanced Military Studies
TOC – Tactical Operation Center
**VUCA** – Volatile, Uncertain, Complex, and Ambiguous.
**WAN** – Wide Area Network
**WiFi** – Wireless Fidelity
**WOAC** – Warrant Officer Advance Course
**WOBC** – Warrant Officer Basic Course
**WOSC** – Warrant Officer Staff Course
**WOSSC** – Warrant Officer Senior Staff Course

# Warrant officer 255 series implementation

*By CW4 William Winkler and CW5 Todd M. Boudreau*

## Background

In the late 1990's the growth and implementation of technology at the tactical echelon created a vacuum of technical knowledge and support within these organizations. Reacting to the requirements of tactical and non-Signal unit commander's, the Signal Center created the 254A, Signal systems support technician, to serve as the single Signal technical expert within maneuver units. Primarily assessed from 25U's, the skill set and scope of the 254A was designed specifically to meet the needs of non-Signal organizations to include maneuver Signal operations, combat net radios, communications security, and Signal support to tactical operation centers. (See diagram 1)

However, in the mid 2000's the emphasis of information technology at the brigade level along with the transformation of the Army to a modular structure had a dramatic impact on the Signal warrant officer numbers, distribution, and purpose.

By placing both Military Occupational Specialty 250N and 254A in brigade combat teams, multi-functional support brigades, and other maneuver units, transformation essentially doubled Signal warrant officer numbers. Additionally the decentralization of systems and technology to the brigade level effectively forced the 254A to evolve from a CNR focused environment into one that is server based. The result of all these changes was that two MOS's were performing essentially the same functions while creating a gap in security and defense of our systems (i.e., MOS 251A and MOS 254A).

In organizations where both MOS 251A and 254A were assigned, the natural trend was for the 251A to focus on IA and some minor computer network defense tasks while the 254A focused on content management. However this was only applicable to a few fortunate organizations. Additionally this created a training issue for both MOS's. MOS 254A was not immersed in server systems to the extent of MOS 251A and MOS 251A was not adequately trained in computer network defense.

## Repurposing the Signal Warrant Officer

As a result of the gaps, overlaps, and redundancy in certain elements of NetOps created by transformation, technology evolution, and emerging threats to our systems, a Military Occupational Classification and Structure action was created and is currently being implemented with a final effective date of 1 October 2012. The MOCS action was designed to specifically rebalance the Signal warrant officer relevance, structure, duties, and Average Grade Distribution Matrix while also addressing current gaps within NetOps.

The MOCS action (see Diagram 2) called for the repurposing of the Signal warrant officer MOS into two enlisted-level accessions (i.e., W1) through W4 MOS. One was designed to cover network management core competency. The other developed to cover our content management core competency, along with an MOS (W3 through W4 only) which will also be created to cover the network defense core competency. The MOCS action maintained the current W5 capper MOS while renaming it from senior Signal systems technician to senior network operations technician.

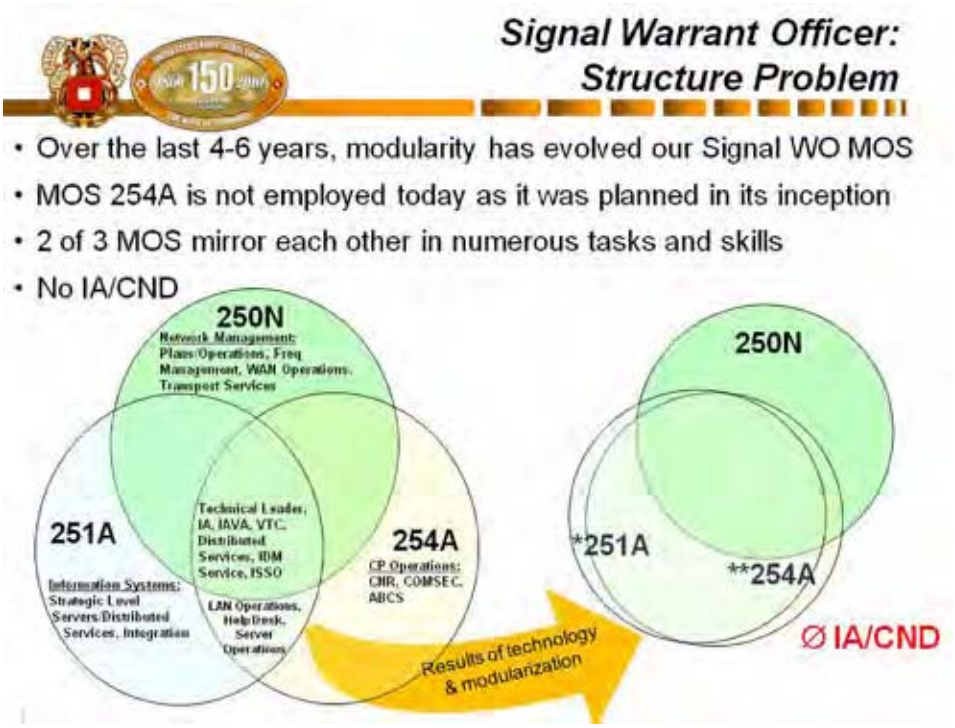



Diagram 1

## The Military Occupational Classification System Action

First is the migration and combination of MOS 251A and 254A to the newly created 255A (information services technician) who is responsible for

**(Continued on page 54)**

(Continued from page 53)

cyberspace content management. This action has already begun with the merging of our two Warrant Officer Basic and Warrant Officer Advance courses respectively) as well as changes in the prerequisites for accessions.

While MOS 254A was traditionally accessed from enlisted MOS 25U, the 255A prerequisites will be similar to the previous prerequisites for MOS 251A. The change in prerequisites is necessary to meet the role of the new MOS 255A and is not an attempt to exclude any particular MOS. Regardless of enlisted MOS, applicants must have content management (layer 7) type experience.

Merging these two MOS's into one that leverages the best of the two will create a warrant officer who is the true technical expert in information systems and services. Assignments for MOS 255A will begin at W2 in the S6 of BCTs and MFSBs, and then progress through division (W3) and corps (W4) to ASCC and joint (W4) positions. There are no active duty W1 positions.

Second is the migration of MOS 250N to 255N, network management technician. MOS 255N will serve as the Army's premier network transport technicians for voice, video, and data networks establishing and maintaining the transport layer environment of the Army's portion of the cyberspace domain through network management/enterprise systems management functions to include fault management, configuration management, auditing and accountability measures, maintaining performance standards, and implementing security measures at all levels in support of combat information superiority and command and control.

MOS 255N will begin at WO1 and conclude at CW4 and be responsible for cyberspace network management. Assignments for MOS 255N will begin at W2 in the S6 of BCTs and MFSBs, and then progress through division (W3) and corps (W4) to ASCC and joint (W4) positions.

The third change is the creation of MOS 255S, information protection technician. This change will provide commanders with a technician dedicated solely to the defense of systems as the warrant officer responsible for cyberspace defense. They will perform CND measures and advise IA functions to enable protection, detection, and reaction functions at all levels in support of combat information superiority. They will supervise and manage IA efforts, perform associated sub-elemental duties (e.g., CND), and enable non-lethal electronic protection efforts; they oversee associated personnel within the standards, transport, services, and applications layers of the network in order to achieve confidentiality, integrity, and availability of information, as well as the authentication and non-repudiation of users. MOS 255S will begin at CW3 and nominally access from MOS 255A and 255N.

As this new MOS matures, the Signal Regiment will meet its information and network protection requirements, close the gaps in our defenses, and provide a highly trained and highly competent cyberspace warrior adaptable for both cyberspace defense and offense. Assignments for MOS 255S will begin at W3 in the S6 of BCT (which will also place a senior warrant officer into the BCT S6 to mentor and further train the junior warrant officers) and progress through division (W4) and corps (W4) to ASCC and joint (W4) positions.

Fourth and finally is the name change of 255Z from senior Signal systems technician to senior network operations technician. MOS 255Z will remain as the Signal warrant officer capper MOS, serve exclusively at the grade of CW5, and function as the technical and tactical advisors for full spectrum network operations at any echelon of command or support activity of the U.S. Army or joint staff sections assigned to theater combatant commanders or allied armies. These officers provide leadership, guidance, technical input, and direction to subordinate elements, staff agencies, and field commanders up to and including theater Army level.

Additionally this MOCS action is also a grade plate roll down for Signal warrant officer authorizations. This action was necessary due to the AGDM for Signal warrant officers being distorted and way out of tolerance. (See diagram 3) Traditionally, the Regiment has had difficulty maintaining our W3 and W4 numbers.

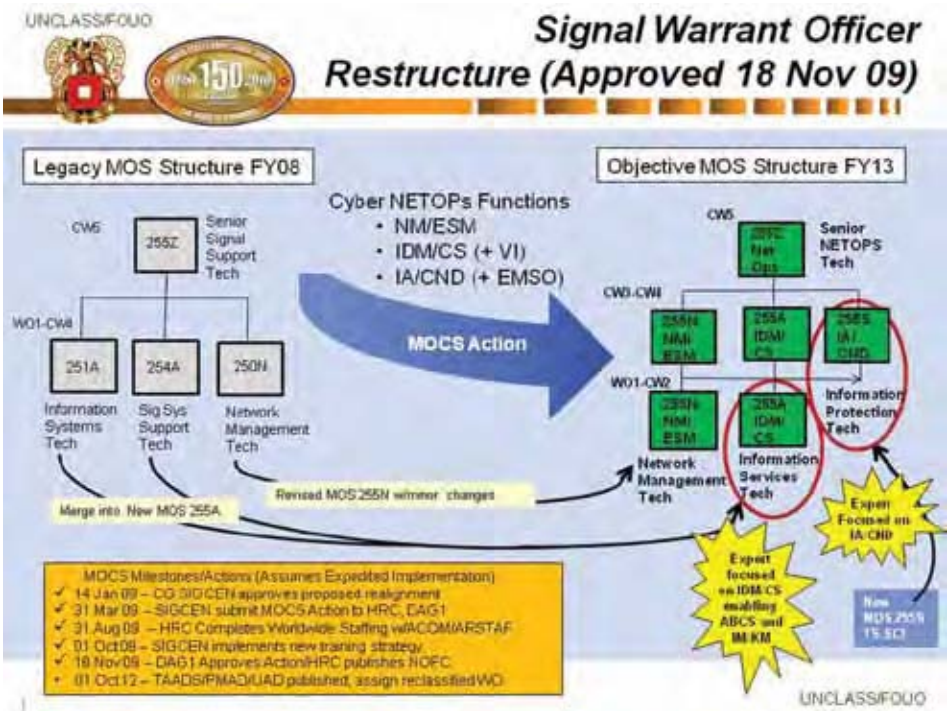



Diagram 2

The grade roll down will actually align us closer to our actual strength. Bottom line is the grade roll down and optimization of our AGMD will have neither an impact on our current population nor on future promotion potential. However it will allow for better utilization and development of our Signal warrant officers.

## Where We Are Today

All of these changes will take effect no later than 1 October 2012, our intent is to expedite the action for full implementation in early FY12. Several changes have already begun. The prerequisites for MOS 251A and 254A have already changed and are now identical. Training for MOS 251A and 254A has been revised and merged into one class for WOBC and WOAC. Digital TOC and systems-of-systems experiential training is already implemented.

We are also working a plan with civilian industry to implement an intense, high-end, cyberspace security (i.e., CyD) qualification course for 255S and several pilot courses are being conducted. A minimum of 96 IA and COMSEC positions are being eliminated and will shift to MOS 255S.

## The Way Ahead

This is a fairly substantial action that will impact our entire population. With such comprehensive changes, some smaller elements of the action may miss the mark. Glitches with the MOCS action were expected and some have already been identified and vetted throughout the process. Upon completion and full implementation of the MOCS action there will be a series of ensuing actions to fine-tune the changes. Some positions may require additional changes while others may be added. We also anticipate changes in our W5 structure as well as growth on 255S requirements.

## Conclusion

While this action is not the conclusive solution to the Signal warrant officer structure, it is a major enhancement that will strengthen the relevance and capabilities of our Signal warrant officers. It will provide commanders, G6s, S6s, and other senior leaders with a powerful team of well-trained, seasoned Signal warrant officers who are essential to successful network-enabled war fighting operations.


Diagram 3

***CW4 William Winkler*** *is currently assigned as the Signal Regiment warrant officer personnel developer (Proponent) at SCOE, Fort Gordon, GA. His previous assignments include 1st ID, 2nd ID, 3rd ID, 82nd Airborne Division, 35th Signal Brigade, Joint Communications Unit, and the Asymmetric Warfare Group. CW4 Winkler has multiple deployments and overseas assignments to include Iraq, Afghanistan, Qatar, Bosnia, Korea, and Germany. He is a graduate of Basic Airborne course, Air Assault Course, SERE, Army Force Management Course, and Warrant Officer Senior Staff Course. CW4 Winkler holds a Bachelor of Science degree from the University of Maryland, College Park in Information Systems, and a Master of Science degree in Information Technology Management from Touro University. He has 25 years of military service with 14 years as a warrant officer.*

## Acronym QuickScan

**AGDM** – Average Grade Distribution Matrix
**BCT** – Brigade Combat Team
**CM** – Content Management
**CND** – Computer Network Defense
**CNR** – Combat Net Radios
**COMSEC** – Communications Security
**CyCM** – Cyberspace Content Management
**CyD** – Cyberspace Defense
**CyNM** – Cyberspace Network Management
**ESM** – Enterprise Systems Management
**IA** – Information Assurance
**IT** – Information technology
**MOCS** – Military Occupational Classification and Structure
**MOS** – Military Occupational Specialty
**MFSB** – Multi-Functional Support Brigades
**ND** – Network Defense
**NetOps** – Network Operations
**NM** – Network Management
**SoS** – Systems-of-Systems
**TOC** – Tactical Operation Centers
WOAC – Warrant Officer Advance Course
**WOBC** – Warrant Officer Basic Course

# Senior warrant officer specialized positions

*By CW4 William Winkler and CW5 Todd M. Boudreau*

This is a primer on what Signal warrant officers can expect in assignments.

Frequently, junior Signal warrant officers express the idea that they are not in control of their career or can only work within the constraints of the assignments they have been given. However, that is not the reality. When a W2 or W3 actively seeks out opportunities beyond traditional assignments that he/she is legitimately qualified to fill, these challenges frequently result in further opportunities later in the career. Whether selected or not, volunteering for challenging, selective or special assignments and training almost always open doors to follow-on prospects.

It is no coincidence that the majority of Signal warrant officers' initial assignments and W1/W2 positions are at the brigade level. Additionally, a substantial percentage of W3 positions are focused in and around divisions. This immersion is the nexus where many Signal warrant officers cultivate their technical aptitude and skills. However, at the W3 grade, Signal warrant officer assignments and opportunities begin to dramatically expand beyond the divisions. And while there are just a handful of assignments at W3 or below that necessitate unique attributes or experiences, often the experience and exposure of Signal warrant officers in these early assignments will cast their competency for many of the senior Signal warrant officer positions in their future.

## Forming Nominal Career Paths

During the most recent Signal conference at Fort Gordon, it was acknowledged that the Regiment historically has not developed Signal warrant officer for key positions. With a few exceptions, there simply were not enough positions or warrant officers to justify the identification and coding required to manage these positions. Even the Regimental chief warrant officer position did not exist prior to 1999. The Regiment was habitually under strength and senior warrant officers sustained only a handful of W5's in the population. But with the rapid growth and relevance of Signal warrant officers, key developmental positions are now a necessity. There are now senior Signal warrant officers in all facets of the DoD, DA staff, training centers, cyberspace, special mission units, and senior Signal organizations. Demand is expected to continue.

For the first time, the Signal Regiment W5 grade is healthy and W5 positions are currently expanding to support all major combatant commands. As Signal warrant officers become more relevant and demand increases, more key positions are bound to evolve.

So the question is, "Does the Signal Regiment need to identify key positions, document those positions, and associate them to a specific career map or training requirement?" If so, what are those positions and what is the professional development requirement? Also, which senior positions will rely on traditional Professional Military Education and the new WOSC follow-on course?


## Specialized Positions

All positions are to some extent different, and as such there is no training that will prepare an officer for all they need to know for any specific job. However, the intent for determining key positions is not to create 900 key developmental positions.

The Signal Regiment is focusing on a handful of positions that are both critical and outside the mainstream of what traditional Signal warrant officers do. Some positions certainly will provide requisite experience on which more specialized jobs rely. In other words, there is not a traditional career course or PME providing adequate experiences and training required to draw from while performing duties

associated with the position. One such example would be the DA G8 or G3 in which Signal warrant officers function at the O5/O6 level on a very senior staff that is immersed in strategy, policy, acquisition, and programs at the macro level. While our other than warrant Signal officers have the benefit of extensive training in their intermediate level education, our warrant officers are left to figure it out for themselves. Maybe such warrant officers should be afforded the opportunity to attend ILE and be assigned in more junior staff positions before being thrust into a DoD or DA staff level position.

Other scenarios may include the special operations command preferring a senior warrant with special operations experience or the newly established Army cyber command and/or its parent joint cyber command requiring a Signal warrant officer who has developed his/her talent in the computer network defense domain.

Recently, the Signal Regiment conducted a W5 assignment board which consisted of several Signal two star general officers. While this procedure was intended to move W5s based upon matching the officers' competence to the position and the units' mission, it was not necessarily meant to imply all W5 positions a key or nominative position. Reality is that with a small number of W5s projected and the demand for senior Signal warrant officers increasing, the process currently is more priority based than nominative based. This was the first attempt at this type of process for senior Signal warrant officers. The projected growth of the senior warrant officer grades further validates the requirement to tag and map out key developmental positions.

## Training with Industry and Advanced Civil Schooling

Currently, PME is the primary developmental process for Signal warrant officer positions. As it is further developed, it should meet the educational requirement for most of our positions. Additionally, the new WOSC follow-on course is designed to fill the training gap and provide training and development for the majority of our senior positions.

For key positions outside the mainstream, the Signal Regiment has relied on training with industry as a prerequisite to an assignment, essentially linking the assignment to a TWI requirement. While this has worked well for some of the School of Information Technology and Capabilities Development Integration Directorate positions (both located at Fort Gordon, Ga.), with only five opportunities annually, TWI alone will not meet all key position requirements.

Another method is to leverage advanced civil schooling to positions. For example, the Signal Regiment may determine that the SIT technical director obtain a graduate degree in education prior to fulfilling that assignment. This is actually similar to what branch and functional area officers do now. This is the most viable option to expand the linking of key positions and training requirements.

## Conclusion

The process must be accomplished sensibly, if the Signal Regiment is going to employ key positions and key developmental positions as a tool to both determine training requirements and formally link the position to the prerequisite training and experience.

Positions must be vetted through some predetermined process at the Signal Center and socialized with our senior Signal leaders before attempting to change any requirements or authorization documents. One possible solution is a site selection board consisting of all the Signal W5s.

Regardless of how these positions are identified, the number of positions must remain small enough to ensure resources can be obtained and it can be managed effectively. Validity in the program must be maintained.

***CW4 William Winkler*** *is currently assigned as the Signal Regiment warrant officer personnel developer (proponent) at SCOE, Fort Gordon, Ga. His previous assignments include 1st ID, 2nd ID, 3rd ID, 82nd Airborne Division, 35th Signal Brigade, Joint Communications Unit, and the Asymmetric Warfare Group. CW4 Winkler has multiple deployments and overseas assignments to include Iraq, Afghanistan, Qatar, Bosnia, Korea, and Germany. He is a graduate of Basic Airborne course, Air Assault Course, SERE, Army Force Management Course, and Warrant Officer Senior Staff Course. CW4 Winkler holds a Bachelor of Science degree from the University of Maryland, College Park in Information Systems, and a Master of Science degree in Information Technology Management from Touro University. He has 25 years of military service with 14 years as a warrant officer.*

## Acronym QuickScan

**ARCYBER** – Army Cyber Command
**CND** – Computer Network Defense
**COCOM** – Combatant Command
**CYBERCOM** – Cyber Command
**DA** – Department of the Army
**DoD** – Department of Defense
**RCWO** – Regimental Chief Warrant Officer
**PME** – Professional Military Education
**SOCOM** – Special Operations Command
**TWI** – Training With Industry
**WOSC** – Warrant Officer Staff Course

# Mentorship builds a legacy

*By CW4 Roy L. Rucker Sr.*

Effective mentorship among Signal warrant officers can build a legacy leading to a more effective Signal Regiment.

I have heard many senior leaders say through the years, "I wish I would have known what I know now," or "if only someone would have guided me in the right direction."

How many times have you said this to yourself? If you could look back now and watch yourself being developed years ago, and take the knowledge, skills, attributes, and experience you have today and mentor your younger self, what level of development could you provide to yourself in order to improve the professional you have become today?

Let me encourage you to accept the responsibility of developing positive professional mentorship relationships.

Mentorship is defined as the voluntary developmental relationship that exists between a person of greater experience and a person of lesser experience that is characterized by mutual trust and respect (AR 600-100).

This trusting relationship provides a non-threatening environment in which a mentee, can seek advice. When done correctly the process aids the mentee in reaching full professional potential.

## Role of the Mentor

The mentor serves a very powerful role in the relationship. He/she sets the stage to provide either positive or negative guid-

**Senior warrant officers regularly provide mentor time with warrant officer candidates during the Warrant Officer Basic Course.**

ance that will impact the life of those mentored.

For anyone who is willing to accept the mentor role, you must ensure that you are representing the positive aspects of being a mentor. Before seeking out mentees or becoming a mentor you should ensure that you are willing to serve in the role all the time. Start by making yourself approachable and are willing to voluntarily provide advice and guidance for situations you feel require it. Most of the time this can be done in your work environment simply by offering advice to fellow junior and senior warrant officers. If you continue to be this type of person you will eventually build a reputation that fosters an environment where people will want to seek you out for guidance.

Next you should be the person or role model that not only can tell a mentee how to perform properly but you should be practicing what you advise as well. Always demonstrate the image of what right looks like. No one respects or seeks out a hypocrite.

Good mentors are great listeners. Be willing to set your agenda aside and give a proper ear to the concerns of the mentee. This will allow you to provide the appropriate counseling at the right time.

Everyone can't be a mentor. If you are one of the people who does not have the temperament to build relationships, be the good steward and pass that potential mentee on to someone who has the desire.

Always be willing to share the information that put you where you are today. You knowledge and encouragement have the potential to propel the mentee to greater levels of achievement. If you are chosen as a mentor, ensure that you can provide the knowledge and guidance that's being required. You can't teach, coach, and mentor if you don't have the proper knowledge. You will only serve to be a detriment to a potentially great future leader.

The process is much like that of a journey. In a journey you need some critical information to be successful. Where are you trying to get? Where are you currently? What are the critical waypoints that will make the journey successful? The mentor helps the mentee to answer these questions.

## Mentee Responsibility

The relationship also has requirements for the mentee. The person advice should be receptive to guidance and advice. This means regularly assessing ones strengths and weaknesses and knowing when to seek advice. A mentor's time is precious and being on time for sessions should be well respected. Always remember that mentorship is a two way relationship and it's perfectly okay for you to approach a mentor and not just wait for a mentor to take an interest in you and your career. Also remember mentorship is not limited to technical guidance but can be a relationship that will help you grow in your personal life as well.

Your mentor is not there to solve all of your problems or to manage your life. The mentor is like a sign post that gives directions at critical junctures. It is still up to you to give a 100% effort to the development of your own career. Be willing to take constructive criticism that may help you identify hurdles that stand between you and a stellar career.

Be open and take ownership. Be ready to learn, not just do.

As a good mentee, remember to use the advice you are given and be vigilant with reporting the outcome of your failures and successes to your mentor. This will serve to make the mentorship relationship stronger.

## Mentorship Legacy

Just a short while ago the question was asked, "Is mentorship broken within the warrant officer Corps?" My answer to that would be a very convincing... NO!!! I don't feel it's broken, I just think it's a work in progress that needs more energizing. We, as leaders/mentors, should strive to create a culture and climate that fosters learning and development for the legacy that will be gifted to future warrant officers.

The whole purpose of building a mentorship legacy, for junior warrant officers, is to establish a strong family that will leave each generation of leaders in a much better environment than the one before it. One mentor, one person, can change a life forever. I urge you to be that one person.

***CW4 Roy L. Rucker Sr.*** *has severed as the LandWarNet Tactical Division branch chief in the 106th Signal Brigade, San Antonio, Texas since October 2008. His previous assignment at the 13th ESC, Fort Hood, Texas was as the G6 and senior network technician. He has more than 21 years of military service and currently mentors 42 warrant officers, officers and Soldiers.*

# Signal life in the logistics lane

*By CW2 Juan M. Dorado and CW2 James E.A. Richards*

Every Signal Soldier should have an understanding of the logistics system employed with the Regiment.

The Sustainment Automation Support Management Office supports all logistics automation systems, or Standard Army Management Information Systems within a brigade. In simplest terms, the SASMO is a collage of different military occupational specialties, clustered together, to provide both technical and functional support for those systems and the logisticians that use them. The recently changed acronym for years was known as "CSSAMO" or "Combat Service Support Automations Management Office" until "Combat Service Support" was replaced by "Sustainment" in Field Manual 4-0. Table 1 shows a list of supported systems, their functional areas, class of supply supported (if applicable) and the MOS that applies to that system for support and/or operation.

The size of a SASMO section is directly dependent on the type of unit being supported. The numbers can range from a section four to more than 20. For example, the Army evaluation task force has four Soldiers, 3rd Infantry Brigade Combat Team, 1st Armored Division has 10 Soldiers; and both 1st Combat Aviation Brigade, 1st Infantry Division and 2nd Heavy Brigade Combat Team, 1st Armored Division have 18 Soldiers. In a deployed environment the SASMO typically interfaces with a communications-electronics command logistics assistance representative to request support for specific systems. The SASMO may also work directly with system a field support representative, depending on the urgency of support required.

In garrison these same support entities still exist, but may not be as readily accessible (except for major exercises or significant system failures). Regardless of LAR or FSR availability, there are still installation or division level entities that exist to support logistics automation functions, such as Army field support battalions or installation SASMOs, division command maintenance evaluation and training teams, and of course SASMOs in sister brigades. For system defects

**SASMO Soldier orienting a directional grid antenna for a Combat Service Support Automated Information System.**

| *System* | *Functional Area* | *MOS* |
|---|---|---|
| **AIT** | **Unit Inventory Management** | **92Y** |
| **BCS3** | **Logistics Tracking/Reporting** | **92A, Any** |
| **CAISI** | **Wireless LAN extension** | **25B** |
| **MC4** | **Medical Records Management/Class VIII** | **68G, 25B** |
| **MROCS** | **Warehouse Inventory Management** | **25B, 92A** |
| **MTS** | **Logistics/Movement Tracking** | **92A, Any** |
| **PBUSE** | **Supply Ordering/Class II** | **92Y** |
| **SAAS-MOD** | **Ammunition Supply/Tracking/Class V** | **89A** |
| **SAMS-E** | **Maintenance Management/ Class IX** | **92A** |
| **SARSS1** | **Materiel Requisition Hub** | **92A** |
| **TC-AIMS II** | **Transportation** | **88N** |
| **VSAT** | **Point of Presence** | **25B** |

Table 1: STAMIS functional area and MOS mapping

and other problems that require escalation to the product/program manager, the Software Engineering Center-Lee Sustainment Support System for the Single Interface to the field help desk, functions as a gateway for strategic reach back to system developers.

## MOS Stir-Fry

Signal warrant officers assigned to the SASMO are currently MOS 251A. On almost every technical forum and mailing list, there is at least one grievance from a technical Signal expert on an aspect of logistics automation that just does not meet the standard. CW4 William Winkler, who is the Signal warrant officer personnel developer, recently reminded that same 251A (Information Systems Technician) community that 42% of the slots for the MOS are actually SASMO slots, created and funded by Combined Arms Support Command. SASMO technicians typically serve as the officer-in-charge, and generally serve in CW2 or CW3 slots. This means that almost half of the graduating warrants will be detailed into positions not views as career enhancing slots.

As a new 251A, entering the SASMO can seem overwhelming. Besides the demanding information technology and leadership skills required doing the job, the 251A comes into the section typically knowing little about section operations. The logistics world is a diverse and dynamic environment with its own language and culture. Learning the logistics lingo is a critical part of the steep learning curve necessary to logistics operations. Adding to the problem is an array of new systems, each having its own distinct configuration requirements. This provides a challenge to even the most talented Signal leader. However, with time, self study, and a lot of coaching and mentoring from the senior logistics staff in the support operations section, a new 251A can gain the logistics knowledge required to Signal logisticians in accomplishing their varied missions.

There are no management tools fielded with any systems that the SASMO supports. Although this may seem to be a downfall, it is actually a beneficial. The SASMO gains a lot of creative freedoms in implementing different aspects of network management, information assurance, and information management. This fosters an environment of learning and exploration, in an effort to find the best way to perform management functions with limited resources. Every MOS in the SASMO benefits from this type of freedom since there is an abundance of overlap in most systems the SASMO supports.

The systems interface with either the Combat Service Support - Very Small Aperture Terminal or Combat Service Support Automated Information Systems Interface. Regardless of MOS, Soldiers in the section must be familiar with networking basics.

One of the most significantly positive aspects of SASMO is the simplicity of the network architecture. For instance the CSS-VSAT is a nearly completely automatic Ku-band satellite terminal that provides IP network transport. It fits in four transit cases that load comfortable into a small utility vehicle. It can be set up in about 20 minutes and even comes with voice over Internet protocol phones that can call other CSS-VSAT VoIP phones. The best part about CSS-VSAT is that it is usable by people who have no experience with satellite equipment or IP networking. Even when it breaks, CSS-SATCOM has a large contingent of support contractors who always respond within 24 hours to fix a terminal.

The CAISI is another great example of a simplified network capability. It provides local range extension for ethernet, and can be configured with a laptop and a 14-slide, screenshot-by-screenshot presentation. While these technologies may be elementary to a 251A, the miracle of these incarnations of the technology is that our 92A, 88N, 68G, 92Y, and 25B MOS Soldiers can all employ them effectively.

A SASMO technician is stretched to evolve beyond our Signal expertise. Supported Soldiers come from every MOS and functional area that the STAMIS requires, including that supply, maintenance, ammunition, medical administration, or movement. The SASMO technician is required to develop creative ways to keep those Soldiers from suffering professional atrophy as a result of being assigned to SASMO. Not only did we not know anything about the non-Signal MOS Soldiers, but often they were mid-career Soldiers. Agreements with various other shops led to finding more senior mentors from within the SPO, or just releasing them for school. An assortment of solutions added to a unique brand of professional development. This was a challenge that SASMO Soldiers met with enthusiasm.

## Hope for the Future

Even with admittedly exceptional support, the logistics community makes available, the simplified systems architecture, and the broadening opportunities, SASMO still has room for improvement. There are several significant goals driving the future.

## SASMO-oriented training

Often, we face a technical problem having received the same training as an operator for a system, only with a lot less experience on the system. This assumes that knowledge of the processes or information manipulation performed by the system is not necessary to fully understand the problem. Requirements documents for systems acquisition should be modified to mandate SASMO-oriented training that focuses on learning how to operate the system first, then how to remediate system-specific problems. Currently, almost no training exists that specifically teaches troubleshooting or demonstrates an engineer-level perspective of the system. These are both skill sets the SASMO has to develop on the job.

Enterprise Management at the local level

One tool missing from the STAMIS architecture is an

**(Continued on page 62)**

(Continued from page 61)

enterprise management solution that can be administered at the local level. Something like a Windows Server on each CSS-VSAT put together in a brigade combat team to form a domain would provide centralized management of user accounts, operating system updates, virus definition updates, and even disaster recovery capabilities, all at the SASMO level. As it is, all user accounts are local to each computer, and all software and virus definition updates are manually completed on each computer. We know how to set this up, and we could locally procure all the necessary hardware and software, but as tightly as the STAMIS software itself is configuration/managed, it is desirable that the next generations of the systems are better integrated with each other.

## Personnel

Often the SASMO does not get personnel selection priority. Our commands tended to select personnel with a focus on operations sections, leaving the SASMO lacking people with the experience needed to function as sustainment to operations. This type of staffing methodology succeeds only under the most ideal conditions and leaves customers exposed in the event of catastrophic system failure. Operations only continue within the capacity of sustainment, and we hope future commands realize this and invest personnel resources accordingly.

## SASMO Career Management

Our training experience includes the one-month resident SASMO course at Fort Lee, Va., in the case of CW2 Richards and both of us have been to New Equipment Training ("System Training" in Acquisition terminology). But the nature of SASMO makes the eight-month 251A Warrant Officer Basic Course overkill, and the one-month SASMO course lacking. We also do not know whether our next assignment will be SASMO or not. If it is, then we can continue developing in this half-logistics, half-Signal specialty. When we return to our MOS roots, then we will be far less prepared than our contemporaries who spent time in pure Signal positions.

The Medical Service Corps branch has a warrant MOS 670A or health services maintenance technician that performs a SASMO-like role for the Army Medical Department. That MOS is managed in the role for an entire career. If a 251A spends the majority of his or her career in SASMO, it is reasonable to integrate into the Acquisition process at some point, either in technology development or system design phases (Pre-Milestone A).

***CW2 Juan M. Dorado*** *has been assigned to the 125th Brigade Support Battalion, 3rd Infantry Brigade Combat Team, 1st Armored Division since February 2009. He previously served as the SASMO technician with the Combat Aviation Brigade, 1st Infantry Division in Iraq in 2008. Before being appointed as a Warrant Officer in 2007, Mr. Dorado held the MOS of 25B. He is currently enrolled in the Computer Studies Bachelors degree program with the University of Maryland. He holds certifications in Security and Network+, MCITP, and MCTS.*

***CW2 James Richards*** *was appointed in 2006 and holds a Bachelor of Arts in Computer Science from Cornell University, as well as the CISSP certification. He started his career as a Signal Officer in 2002, serving as the G3 Automations Branch Chief for the 311th Signal Command, then as a network engineer for the 261st Signal Brigade. In 2009, he served as a WAN/LAN Technician for the Victory CAN sites in Iraq. Most recently, he was assigned as SASMO for 5th Brigade, 1st Armored Division, and is currently assigned as SASMO for 2nd Brigade, 1st Armored Division.*

## Acronym QuickScan

**AIT -**Automatic Identification Technology
**BCS3** - Battle Command Sustainment Support System
**CAISI** - Combat Service Support Automated Information Systems Interface
**CASCOM** - Combined Arms Support Command
**CSSAMO** - Combat Service Support Automation Management Office
**FM** - Field Manual
FSR Field Support Representative
**IP** - Internet Protocol
**IT** - Information Technology
**LAR** - Logistics Assistance Representative
**MC4** - Medical Communications for Combat Casualty Care
**MOS** - Military Occupational Specialty
**MROCS** - Materiel Release Order Control System
**MTS** - Movement Tracking System
**PBUSE** - Property Book Unit Supply Enhanced
**SAAS-MOD** - Standard Army Ammunition System - Modernization
**SAMS-E** - Standard Army Maintenance System - Enhanced
SARSS1Standard Army Retail Supply System
**SASMO** - Sustainment Automation Support Management Office
**SATCOM** - Satellite Communications
**SEC-Lee** - Software Engineering Center - Lee
**SPO** - Support Operations
**STAMIS** - Standard Army Management Information Systems
**TC-AIMS II** - Transportation Coordinator's Automated Information for Movement System II
**TDY** - Temporary Duty
**VoIP** - Voice Over Internet Protocol
**VSAT** - Very Small Aperture Terminal

# Signal warrant officers forging new relationships in nontraditional roles

*By CW2 Kenneth Jenkins and CW2 Matthew Jeffcoat*

Signal warrant officers are serving key roles in an ever-widening arena of non-traditional postings.

Over the past four years the Army's criminal investigation units have extended communication between their law enforcement assets due to change of the unit's Modification Table of Organization and Equipment. A Signal warrant officer has been added to the 6th Military Police Group-Criminal Investigation Division, located at Joint Base Lewis McChord and the 3rd MP Group-CID, located at Fort Gillem, Ga. The groups' overall automations support to the units' special agents in the field has been improved.

One of the main functions of the Signal warrant officer is to enable rapid, robust and reliable communications for the unit whether it is a Stryker brigade or a criminal investigation group.

While investigations may be processed locally, when there is need for additional resources or more support, the agents in the field or investigative operations can count on being able to reach out to those senior agents and staff wherever they might be. The video teleconferencing systems have been revamped to support secure VTC and are leaning forward to be ready for the switch from integrated services digital network to Internet protocol.

Haphazard replacement of equipment has been streamlined into an item-for-item swap regulated at the group level and validated against documented requirements coordinated through operations channels. As part of the organizational inspection program, the S6 shop has visited every battalion in order to inspect and assist with policy compliance and leveraging current technology to optimize battalion detachments support.

The group S6 is where the Signal warrant officer resides. In this position the Signal warrant officer coordinates with the network enterprise centers of all of the detachments. This includes 24 NECs along with Hawaii, Alaska, Korea, and Japan. Warrant officers working alongside CID agents have a unique perspective that brings valuable feedback to quickly resolve questions and develop new capabilities. Additionally, the units' computer crimes coordinators have specialized technical abilities in the field of digital forensics.

This is just one example of the relevancy of the Signal warrant officer outside the traditional Signal unit position. More and more we find non-Signal units relying on the complex technology that Signal warrant officers are trained and ready to plan, install, maintain, operate, and administer.

## Acronym QuickScan

**CID** – Criminal Investigation Division
**IP** – Internet Protocol
**ISDN** – Integrated Services Digital Network
**MP** – Military Police
**NEC** – Network Enterprise Center
**VTC** – Video Teleconference

# A profession of arms

*By CW5 Troy A. DeGolyer, CW5 Johnny Silva, CW4 Diedra A. DeWitt, CW4 Meaghan M. Hatfield, CW4 Heber L. Hyde, CW4 Patrick J. Muenks, CW4 Curtis L. Newkirk, and CW4 Mark A. Seels*

In a group dynamic senior warrant officers distilled the essence of the current Army warrant officer cohort in the aftermath of a decade of persistent conflict.

The research and analysis was conducted by the authors while part of a study group consisting of Warrant Officer Senior Staff Course students. This team of students determined that the values sustaining the warrant officer cohort are consistent with those of the Army as a whole.

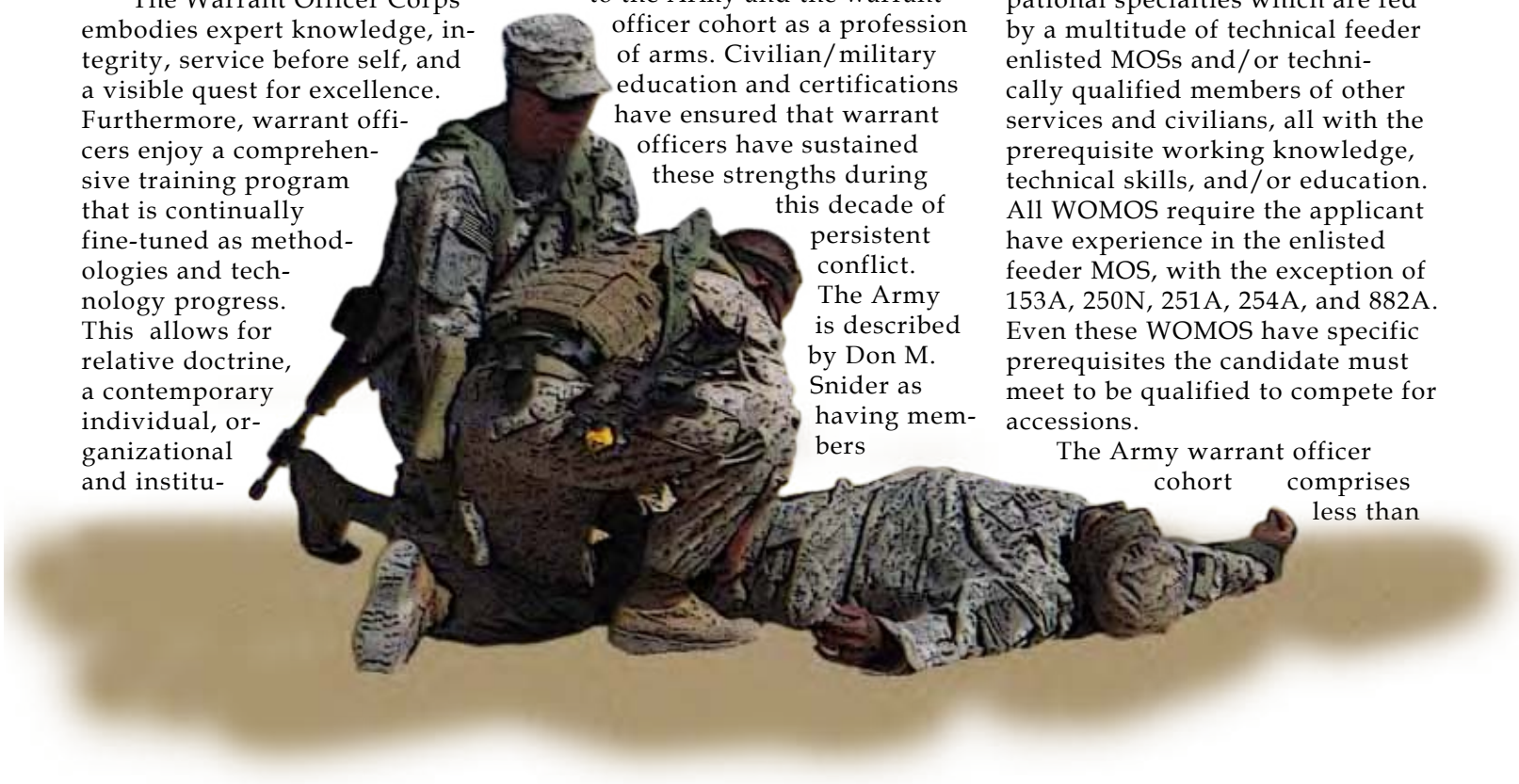
The Warrant Officer Corps embodies expert knowledge, integrity, service before self, and a visible quest for excellence. Furthermore, warrant officers enjoy a comprehensive training program that is continually fine-tuned as methodologies and technology progress. This allows for relative doctrine, a contemporary individual, organizational and institutional development processes, and the appropriate integration of the warrant officer cohort with the Army's internal and external environments. These indispensable elements apply to the warrant officer in a technical professional that is further correctly identified as a "profession of arms."

## Warrant Officers as a Profession of Arms in Relationship to the Military Technical Capacity

GEN Ronald R. Fogleman, U.S. Air Force chief of staff (1994-97) identified the common strengths within the profession of arms as integrity first, service before self, and excellence in all we do. These certainly apply wholeheartedly to the Army and the warrant officer cohort as a profession of arms. Civilian/military education and certifications have ensured that warrant officers have sustained these strengths during this decade of persistent conflict. The Army is described by Don M. Snider as having members that have expertise in service, knowledge, and having a professional military ethic that is tested and certified. These are elements that also apply to the warrant officer as a member of the Armed Forces and as a profession of arms.

To become a warrant officer, an individual must be physically and mentally fit, an outstanding Soldier and adept in his/her specialty. Recruitment into the warrant officer cohort is voluntary. However all volunteers are not accepted. Each candidate must undergo a rigorous validation process prior to entering the Warrant Officer Candidate School. This process ensures that only the most technically qualified applicants are selected. Currently there are 46 warrant officer military occupational specialties which are fed by a multitude of technical feeder enlisted MOSs and/or technically qualified members of other services and civilians, all with the prerequisite working knowledge, technical skills, and/or education. All WOMOS require the applicant have experience in the enlisted feeder MOS, with the exception of 153A, 250N, 251A, 254A, and 882A. Even these WOMOS have specific prerequisites the candidate must meet to be qualified to compete for accessions.

The Army warrant officer cohort comprises less than



**Signal warrant officers regularly train in all phases of warrior skills relevant to the profession of arms as well as high technology aspects of modern communications.**

three percent of the total Army. Although small in size, the level of responsibility is immense and only the very best will be selected to become warrant officers. Warrant officers are technical and tactical leaders who specialize, throughout an entire career, in a specific technical area. Expert knowledge within the warrant officer cohort is achieved through ongoing professional military education, degree completion programs, training with industry, mentorship, and various certification programs. Warrant officers' exceptional range in skills are developed over time, increased with technical experience, enhanced with specific technical focus and training, enforced with professional and civilian education, and sustained through civilian certifications which ensures their individual technical proficiency. These efforts are reflective of U.S. Army Training and Doctrine Command Pamphlet (PAM) 525-3-1 as it describes success in future Army operations, stating that a broad training enterprise develops and sustains the tactical and technical competence that builds both confidence and agility.

Branch proponents develop and update the WOBC training and technical certification standards to ensure that all warrant officers attain the degree of technical competence needed to perform in their WOMOS at the platoon through battalion levels. Don M. Snider Council for American Private Education notes that the Army tests and certifies its members. This can be applied to warrant officer education and certification program. Snider says, "The Army tests and certifies its members to ensure each meets the standards (both competence/expertise and morality/character) of the profession before being granted status as a full member of the profession as well as at each successive level of promotion/advancement. It maintains systems to train and educate individuals in a trainee or apprenticeship status until professional standards can be met."

All WOMOS receive strenuous training and participate in certification programs. For example, warrant officer aviators receive training that meets or exceeds the requirements by Federal Aviation Administration. Signal warrant officers are certified with a litany of commercial certifications such as project management professional, Microsoft's certified systems engineers, A+, Cisco certified network associates, Microsoft certified systems administrator, Security+ and certified information systems security professional to name a few which are easily compared to the civilian professions. These are listed as the top 10 technology certifications in information technology, based upon a survey of 17,000 civilian technology professionals. Acquisitions, Military Intelligence, Military Investigations, Special Forces, and Military Culinary professionals as well as other WOMOS, all have programs which are comparable to their civilian professional counterpart. The Bureau of Labor Statistics predicts that computer and mathematical occupations will add 785,700 new jobs by 2018. These technical professionals often come from the military ranks. This is verifiable as the Army has experienced a loss of personnel to the civilian work force as these personnel transition with ease due to the technical knowledge and professional skills gained during their military service.

From accession and attendance at WOCS to attendance at WOSSC, doctrinal guidance is established for each phase of warrant officer training. It is constantly changing to keep up with global situations and to gain accreditation. The doctrinal data is derived from TRADOC, feeder MOS, the 46 WOMOS, and the training centers at Fort Rucker, Ala. Training also reflects changing requirements from the various proponent/branch training centers (Warrant Officer Basic and Advance Course (WOBC and WOAC respectively).

With the success and history of the Army warrant officer at each capacity, the doctrine that guides the training is adequate. This doctrine is constantly changing in order to stay abreast of the needs of that capacity. The changes are dictated by the MOS proponent and technological advances in a particular MOS or training level.

TRADOC serves as the change agent for the Army's Human Capital Enterprise. Most of the assessment and certification of individual capacity occurs during institutional training, but this alone does not completely prepare the future force. Career colleges and proponent schools have a slow change life cycle. Field level pushback, lessons learned and unit tactics, techniques and procedures validate current practices. The Army needs to examine new models for assessment and certification. The warrant officer cohort is the best positioned agent to support change within the Army professions of arms.

The Army is a highly specialized, self-regulating profession tasked by its citizenry as a trusted defender of the Constitution. Army leaders and all members adhere to a strict code of moral conduct. The Army is an element of the joint force exerting necessary power in the science of war to protect the American way of life against all enemies, foreign and domestic.

Current and future operational environments place heavy reliance on the capacities of the human dimension. This is due in large part to a need for the Army to conduct full spectrum operations in an ever changing and challenging OE. Field Manual (FM) 7-0, Training for Full Spectrum Operations, addresses the fundamentals of training modular, expeditionary Army forces for simultaneous offensive, defensive, and stability or civil support operations in an era of persistent conflict. TRADOC PAM

**(Continued on page 66)**

**Senior warrant officers attending their Professioinal Military Education course at the Warrant Officer Career College.**

**(Continued from page 65)**

525-3-7-01, The U.S. Army Study of the Human Dimension in the Future, focuses attention on the human dimensional components of Soldier moral, cognitive, and physical behavior necessary for Army organizational development and performance essential to raise, prepare, and employ future landpower. The document states that current trends in the global and domestic OE will challenge the United States' ability to maintain a future responsive, professional, all-volunteer Force.

The human element is the key to the Army's future. The Soldier is the centerpiece of transformation. Faced with continuous employment across the full range of military operations, the Army will require extraordinary strength in moral, physical, and cognitive components of its professional force. Developing a professionally competent Army requires attention to the cognitive component of the human dimension. Critical competencies of Soldiers must be identified as well as the processes and tools needed to build these competencies. TRADOC leaders indicate the most influencing Army resource lies in modular, tailored, accessible, and realistic training and leader education. Conventional practices must be revised. It's no longer good enough to simply train to a task. This order of learning is too elementary.

Army professionals must be innovative critical thinkers capable of sustaining high tactical, technical, and cultural intellect consistent and adaptive to all potential OE; particularly in respect to joint, interagency, intergovernmental and multinational operations. The advancement of technology is rapid. New equipment fielding is persistent. TTPs are constantly being refined as new threats evolve. TRADOC leaders have implemented appropriate self examination of the HCE to form institutional change that will have a significant impact on assessing and certifying the competence and overall intellectual/cognitive capabilities within our Army of professionals.

The branch/proponents and professional military schools should collaborate across cohorts to understand the present TLE transformation that must occur. The warrant officer cohort is well advised to implement Recommendation 104 of the 2002 Warrant Officer Army Training and Leader Development Panel which advises us to "…develop and implement an integrated system for all Army officers that accounts for common direct leader skills and actions required by the Army Vision and full spectrum operations in the contemporary operational environment." It continues, "This education system must also meet the training and leader development requirements of Army officers by branch, grade position, specialty, functional area, and assignment." This document seems to be the most comprehensive study on behalf of the warrant officer cohort and should be re-examined to determine if these recommendations are still valid. And if they are

valid, why have they not been acted upon?

LTG [U.S. Army-Ret James C.] Riley (2002) in his presentation of the ATLDP-Warrant Officers, highlights the conclusion that the "Warrant Officer Education System fails to meet the needs of the Army and warrant officers and requires thorough revision." The report further concludes that warrant officer training and skills must be related to grade and position rather than linked to promotion and that the WOES must provide the right training at the right time. Furthermore, a system must be in place that promotes self-development.

It is widely acknowledged that the warrant officer cohort brings a high level of technical expertise to the profession of arms. However, too frequently this becomes the sole defining characteristic of the cohort and thus limits its full degree of military/technical capacity. Mistakenly, the warrant officer cohort is guilty of a narrow interpretation of military/technical capacity. Often warrant officers describes themselves from a single dimension of technical expertise rather than what the profession of arms demands – a highly specialized expert officer, leader, and trainer fully competent in technical, tactical, and leadership skills.

Expert knowledge must transcend all cohorts and is not only measured as an individual quality, but also should be exhibited as a collective unit quality. Warrant officers must possess the technical and leader skills that make them the innovative integrators and dynamic teachers characterized by the definition of the warrant officer of the "Future Force" in Department of the Army (DA) PAM 600-3. The warrant officer professional is critical to promoting the level of technical expertise demanded by the Army profession of arms. FM 6-22 Army Leadership makes note of the fact cohorts differ in the magnitude of responsibility vested in them. It is incumbent upon the warrant officer cohort to perform the appropriate self-examination to ensure it is contributing to the overall strength of assigned commands through its high degree of specialization and leader skills.

Efforts are not adequately shaping the leadership and technical competence necessary for future full spectrum operations according to needs assessed in current HCE studies. The level of responsibility vested in the warrant officer dictates a high-level of intellectual capacity. The warrant officer of today must be a self aware and adaptive learner. This characteristic requires conceptual components of intelligence such as mental agility, sound judgment, innovation, interpersonal tact, and domain knowledge.

Historically, domain knowledge is a position of warrant officer strength. However, it requires possessing facts, beliefs, and logical assumptions beyond core technical proficiency. Warrant officers should seek mastery of domain knowledge. This entails mastery of tactical, technical, joint, cultural and geopolitical knowledge. Warrant officers, like leaders from other cohorts, have careers where learning is the product of immersion in three environments: institutional training and education (PME and technical branch proponent), operational assignments, and self-development.

Self-development is continuous. It involves the individual with support of first-line leaders and commanders. It results in a broadened focus where leaders become independent learners. And it includes both civilian and military education.

Military institution training and PME in conjunction with operational assignments will not totally ensure Army warrant officers sustain the degree of competency needed. Unfortunately, self-development participation is often adversely impacted by unit operational pace. The present WOES and operational assignments are not developing leadership and technical abilities adequately. There is an atrophy of technical expertise due to stagnation in assignments and evolving technology. As a consequence, warrant officers are not receiving the training necessary to remain current in their technical disciplines. Efforts must be explored to provide for greater self-development to bridge the gap between warrant officer institutional and unit training experiences.

The current warrant officer assessment undertaken advocates a new breed of warrant officer leader. As a cohort, can we accept something less than this new hybrid of "super professional?" The answer to this question is yes. It is unrealistic to expect that the volunteer force will generate warrant officer branch cohorts capable of identical tactical, technical, teacher/trainer, leadership and cognitive skill sets. We each possess different strengths and weaknesses. Perhaps rather than organizational excellence being the offshoot of individual capacity, we need to adjust our thinking to team excellence as the fundamental building block in our profession of arms. We need only exam the success of our Special Operations Forces to see the effectiveness of this model.

The Army has been very successful in managing this integration strategy which includes the integration and interface of initiatives and requirements across the command, its component commands, fellow combatant commands and multinational partners. Our Army must be balanced. We must be organized to be versatile; deployable enough to be expeditionary; responsive enough to be agile; pre-

**(Continued on page 68)**

(Continued from page 67)

cise enough to be lethal; robust and protected enough to be sustainable; and flexible enough to be interoperable with a wide range of partners.

These are the defining qualities of a balanced Army. They describe not only the operating force, but also the generating force. This forms the basis of this modernization strategy.

The imperative for the Army is that we must continuously and aggressively modernize our capabilities to ensure we remain the dominant force, capable of operating in all environments across the full spectrum of conflict, including: prevailing in protracted counterinsurgency campaigns; helping other nations build capacity; assuring our friends and allies; supporting civil authorities; and defeating varying threats.

Army leaders are beginning to give troops some flexibility in adjusting approaches to better suit uncertain conditions at the tactical, operational, and strategic levels. The Army uses the term 'decentralization' in this context. Decentralization may allow for greater flexibility of action within stabilization and counter insurgency operations. Improved military education in the more traditional sense – in leadership training as well as more formal trade training – will remain essential for militaries to manage the ever changing environments in the world.

There exist signs and symptoms of exhaustion, depression, and stress across mental, social, and physical boundaries. We understand that stress is tension produced by conditions in the work environment making negative impacts on ones psychological or emotional well-being. The widely accepted causes of stress in military life are attributable to such things as deployments overseas, exposure to combat, education and training and the threat of bodily harm. The periodic permanent change of station, stationing of personnel overseas, and lack of control over duty assignments are other examples of factors that may affect the mental health of its members.

This team of researchers discovered another unique stressor often missed. Through less than optimal levels of education and training, warrant officers have difficulty keeping pace with the new technology that the Army acquires from the civilian community. Commanders in the past have been viewed as non-supportive in allowing the senior warrant officers the time and funds necessary to seek and obtain the appropriate education and training required to meet the level of understanding needed to accomplish their assigned missions. Education and training on the latest technologies has come at a very high cost to units. This increases the stress on the technical advisor to inform the command or produce a result that is acceptable to the commander's intent or requirement.

## Moral and Ethical Capacity

The military profession requires Soldiers to discharge their professional duties in a moral and ethical manner. Army leaders in particular are obligated to the American people to maintain professional competence and personal character. As members of the profession of arms, leaders must exhibit the qualities which mark service in the military as a truly professional endeavor. These qualities include a code of professional conduct, a high degree of competence based on established and well regulated examinations of skill, education, and performance, and self-regulation to purge those members who fail to meet standards or demonstrate required professional knowledge. Like other professions such as medicine and law, the military also requires institutional training to develop a broad range of skills and a commitment to continuous education.

Successful Army leaders have consistently promoted strong morale, cohesion, and mental preparation in their subordinates. In units with strong bonds, warrant officers reflect their leader's professional values and report that core Soldier values are very important to them. Without such bonding and positive leadership, some otherwise highly cohesive units have adopted dysfunctional norms and behaviors. This socialization process reflects the Soldier's internalization of these values as his or her own.

This includes a variety of scenarios such as leadership in an organization, lack of knowledge and/or experience conducive to the assignment, lack of education, personal value system, strength of character, pay disparity between "O grade" officers and "W grade" officers (and professional expectations are on a higher level at times for warrant officer – i.e. working in "O grade" position or commensurate responsibility but huge pay disparity). Moral/ethical stressors can be levied at individual, organizational or institutional levels.

The Army develops warrant officers as leaders and technicians who embody the highest standards of moral and ethical conduct. Warrant officers must internalize, demonstrate and sustain a warrior ethos that insists upon commitment to core institutional values. The strengths that have sustained the warrant officer cohort are consistent with those of the Army as they envelope leadership, expert knowledge, integrity, service before self, and excellence. These indispensable elements apply to the warrant officer as leaders and technical professionals identifying them as a profession of arms.

The Co-Authors of this article consist of a profes-

sional group of warrant officers, who recently graduated from the Warrant Officer Senior Staff Course. Their combined total military experience is equivalent to 249 combined years of Army service.

***CW4 Diedra A. DeWitt*** *is a Quartermaster Warrant Officer (920A) and is currently assigned as a career manager at Human Resources Command at Fort Knox, Ky. She holds a Bachelor of Arts in History from Taylor University and a Masters in Business Administration from Indiana Institute of Technology. She currently has 30 total years of military service, with 19 years as a Warrant Officer.*

***CW4 Meaghan Hatfield*** *is currently assigned as a warrant officer career manager, HRCoE, Fort Knox, Ky. She has been in the Human Resources field for 29 years, holding positions at company, battalion, brigade, PERSCOM and Human Resources Command level as well as Acting S1, MILPO and the 301st Maneuver Enhancement Brigade, Fort Lewis, Wash. She holds a Master of Science degree in Behavioral Science from Cameron University.*

***CW4 Patrick Muenks*** *holds a Bachelor of Science degree and Masters of Education degree from the University of Missouri. He has completed 24 years service in the aviation career field as an aviation safety officer, instructor pilot and maintenance test pilot and 18 years as a warrant officer. CW4 Muenks is a member of the Missouri Army National Guard assigned as the Aviation Materiel Officer for HHD, 1107th Aviation Group. He is also employed as a full-time military technician currently serving as an Instructor Pilot for the Christopher S. Bond Army Aviation Support Facility, Fort Leonard Wood, Mo.*

***CW4 Curtis Newkirk*** *is currently assigned to the Army Test and Evaluation Command/Army Evaluation Center, Alexandria, Va. He is a graduate of the Basic Airborne Course, the Warrant Officer Senior Staff Course and holds a Bachelor of Science Degree in History from Methodist University in North Carolina. He has 29 total years of military service, with 15 years as a warrant officer.*

***CW4 Mark A. Seels*** *is a SIGINT warrant officer (352N) and is currently assigned as the 470th Military Intelligence Brigade intelligence collection manager at Fort Sam Houston, Texas. He currently has 24 total years of military service with 12 years as a warrant officer.*

***CW5 Heber L. Hyde*** *is an ordinance warrant officer (915E) and is currently transitioning into the position as command chief warrant officer for the Utah National Guard, Draper, Utah. He has 23 years as a Warrant Officer with a total of 36 years service in the Army.*

***CW5 Troy A. DeGolyer*** *holds the MOS AH-64D SP/IE/GFR and is currently assigned as the Mobile Assistance Team chief, 21st Cavalry Brigade (Air Combat), Fort Hood, Texas. He has 23 total years of Army Service with 22 of those as a warrant officer.*

***CW5 Johnny Silva*** *is an aviation maintenance warrant officer (151AE) and is currently assigned as the aviation material officer at Camp Humphrey, Korea. He holds a Masters of Criminal Justice from Tiffin University. He currently has 27 total years of military service with 15 years as a Warrant Officer.*

## ACRONYM QuickScan

**ATLDP –** Army Training and Leader Development Panel
**CAPE –** Council for American Private Education
**COCOM –** Combatant Command
**COIN –** Counter Insurgency
**DA –** Department of the Army
**FM –** Field Manual
**GTA –** Graphic Training Aid
**HCE –** Human Capital Enterprise
**JAG –** Judge Advocate General
**JIIM –** Joint, Interagency, Intergovernmental and Multinational
**MOS –** Military Occupational Specialty
**OE –** Operational Environment
**PAM –** Pamphlet
**PME –** Professional Military Education
**TLE –** Training and Leader Education
**TRADOC –** Training and Doctrine Command
**TTP –** Tactics, Techniques, and Procedures
**WOAC –** Warrant Officer Basic Advance Course
**WOBC –** Warrant Officer Basic Course
**WOCS –** Warrant Officer Candidate School
**WOES –** Warrant Officer Education System
**WOMOS –** Warrant Officer Military Occupational Specialties
**WOSC –** Warrant Officer Staff Course
**WOSSC –** Warrant Officer Senior Staff Course

# Creating MSOffice SharePoint service account managers without providing excessive control

*By CW3 Eric Bray*

Microsoft Office SharePoint Service provides an easy, web based platform for users to collaborate on the web, but efficient user management out of the box is lacking.

As an automations chief with only a handful of administrators – few with any MOSS training or experience - I cannot afford to give away unrestricted permissions to subordinate personnel simply to add users to our portal site. My unit has close to 7000 personnel in dispersed geographic locations throughout the world. It is inefficient to require system administrators to manage portal accounts all day as users relocate. If we allow subordinate personnel the right to add users, we risk creating more work for system administrators because of the need to maintain acceptable knowledge management practices. Poor KM discipline leads to SharePoint sprawl with data spreading out in a disordered fashion.

Over the last 18 months, my team has been working with a new work flow server by K2 called BlackPearl. The BlackPearl server is a workflow application that can be installed as a standalone server, or on the backside of a Web front end. In our case, the software is installed on the back end of SharePoint. We are still using MOSS07 but plan to upgrade in the next year. Presently we have created several business Process Automations. However, the process we are covering in this article is known as "On boarding." Figure 1 below is a depiction of On boarding which allows non-systems administrators to manage and create accounts with the right permissions without losing control of the website and reducing overall Sprawl.

The requirements for this workflow are twofold. First, on tactical platforms, we need to give new users the ability to request a new account with full access rights (Active Directory, Exchange, MOSS, and Adobe Connect or AC) to a non-classified Internet protocol router/ secure Internet protocol router platform by way of a Web page. We are still testing this process and have achieved with great success even though a few bugs remain. Overall we have greatly reduced account creation and processing time on deployments. This request is auctioned, and accuracy is verified, by the knowledge management representative, but access is not granted until a review is completed by the system administration or help desk personnel. Secondly, on reach back systems, the workflow must also provide portal access to our subordinate users who are not in the same AD forest.

The current solution on


Figure 1. Onboarding

our NIPR reach back system (the latter) allows a KMR to go to a portal site, and authorize a user "registration access" rights in our portal. This is accomplished by way of audience based participation. Presently this process is on a separate site collection where the user can only see the acceptable use policy and request access by filling out the information required to establish a user account. No personal identifiable information is allowed. This information provides basic contact information and the fields necessary to complete a DA 2875 – System Authorization Request as a paperless process.

To better illustrate the workload, our chemical, biological, radiological, nuclear, and high yield explosives net portal has the root site (approximately 7 main groups), approximately 20 section sites (at least three groups per site); each section having anywhere from several to 10 sub-sites or "Shops" (at least 3 groups per shop also). At this time, we have about 300 SharePoint groups to manage on this server alone.

A visitor only gets read access to the root, section, and shop sites. The standard user gets root site (read), section (read/write), and shop level (read/write) access. The KMR (account / content manager) has the same as a standard account, plus the ability to approve new users for read/write access to designated sites. The CBRNE net site is designed to filter information – usable and relevant information – into decision making material. Therefore, site design is maintained at the KM level and none of the users have the ability to change the site (in order to avoid "sprawl"). We will have internal sites later to enhance and enable creativity, but we just have not yet built that out.

***CW3 Eric Bray*** *began his military career as an MLRS fire direction specialist in Field Artillery in 1996. In 2000, he transitioned to Aviation as a Blackhawk pilot. He deployed in support of OIF three times. In 2008, he transitioned to Signal as a 254A. CW3 Bray is MSCA, MSCE, and Security Plus certified and is responsible for ensuring mission critical communications servers are up, secure and accessible to Soldiers of the 20th Support Command, subordinate units and inter-agency partners. He is the chief of automations, knowledge management for the 20th Support Command and is currently working business process automations via workflow servers.*

## ACRONYM QuickScan

**AC** – Adobe Connect
**AD** – Active Directory
**AKO** – Army Knowledge Online
**AUP** – Acceptable Use Policy
**BPA** – Business Process Automation
**CBRNE** – Chemical, Biological, Radiological, Nuclear, and High Yield Explosives
**KM** – Knowledge Management
**KMR** – Knowledge Management Representative
**MOSS** – Microsoft Office SharePoint Service
**NIPR** – Non-classified Internet Protocol Router Network
**PII** – Personal Identifiable Information
**SAAR** – System Authorization Request
**SIPR** – Secure Internet Protocol Router Network
**SysAdmin** – System Administrator
**WF** – Windows Workflow Foundation

# Network Enterprise Centers help units prepare for war long before they arrive downrange

*By CW3 Jason Dunn*

Today units have the authority to train in garrison with their battlefield command and control system servers. They can have them physically plugged into the garrison installation campus area network using the network enterprise center provided backbone. This can be accomplished if the unit coordinates with the NEC and follows the guidelines established by TA 2006-006, dated May 2007. This applies to all operational forces; that is, any element that has a deployable requirement.

Technical Authority 2006-006 is the TA signed by Network Enterprise Technology Command providing the technical guidance for properly connecting tactical units into a NEC. Copies of this document can be found by contacting AKO, at the link below or your theater Signal brigade/strategic Signal brigade, respective theater Signal command, NETCOM G5, or the author of this document. (https://www.us.army.mil/suite/doc/22333422). The TA effectively lays out the procedures and requirements that must be met by the OF unit before being allowed to connect in garrison to the ICAN. Under this guidance all NEC's are required to accommodate OF information technology needs. This does not give the OF the authority to connect everything,, but it does provide specific guidance for program manager fielded systems and several other scenario's that directly support war fighter needs. All systems must be on the CoN list and must be IA compliant. Visit the link: https://www.us.army.mil/suite/page/137030.

The TA has good overall detail, but can be confusing to new readers. One of the key requirements of approval to connect is ensuring a healthy IA posture. This can be accomplished through the service level agreement or a memorandum of agreement that is completed between the OF and the network service provider.

In the SLA/MOA, it should be specifically spelled out how a unit will ensure IA compliance through detailed scans and how these scans will be reported to the installation IAM, and exactly which tools will be used. There are two acceptable methods to accomplish this. One method allows the NEC access to conduct scans and the other is for the unit to conduct routine internal scans and forward the results to the

**Signal Soldiers with the 3rd Armored Cavalry Regiment and 63rd Expeditionary Signal Battalion setting up a communications site at the National Training Center.**

installation IAM. While both methods have merit, I would encourage every S6 to conduct and report his/her own scans. This will allow units to become very familiar with the process and help sustain this capability with operations and training when the unit deploys. Either method will need to be clearly articulated and agreed upon by the both the unit S6 and the IAM. Note if an agreement cannot be met on this or any related issue, then the supporting theater Signal brigade/command should be notified and a request for further guidance generated. Often a simple phone call between the network enterprise support team leadership, brigade, or Signal command, and the NEC / OF can quickly resolve any discrepancy.

Other key components of the TA are the issue of "persistent, but nearly empty state" of the AD organizational unit structure. This basically means that the current AD OU structure should only have a few administration accounts populated. The original intent was OF units who needed to deploy to the field for any operations or training would coordinate with NEC and receive a copy of their user populated garrison OU's via an approved provisioning tool (e.g., Electronic Data Systems – Provisioning) prior to movement. This would be done in conjunction with the de-advertisement of the IP scope and other pre-movement requirements. Obviously this inhibits rapid deployment capability. It is under review to be completely removed in the next iteration of the TA.

At this time, the current OU provisioning tool, EDS-P has not been approved by the CIO-G6. Thus units will continue operating a fully populated OU structure. However, just because units will have fully functional servers and full OU structures, does not mean that units should replace their NEC as the primary service provider. The TA does not support an OF unit being its own service provider while in garrison. This does provide a means for your systems to maintain a "fight upon arrival" capable and that a small number of system administrators should be both training and maintaining these servers on a regular basis. It is NOT the intent of FORSCOM or NETCOM for any unit to operate as its primary service provider while in garrison. These systems should always be online and updating. Server training in garrison is highly recommended and encouraged.

TA 2006-006 is currently under revision. Updated drafts are under development by NETCOM G5 and should be up for approval soon. A working group was established and input was provided by 7TH Signal Command, FORSCOM, PEO-C3T, and others to help develop a revised version that is more current with our current systems and structures. NETCOM G5 has the lead to refresh the TA and publish expanded guidance. Until the new TA is published, NEC's are still referring to the original copy signed by BG [Carroll F.] Pollett [commanding general U.S. Army Network Enterprise Technology command] in May 2007. This version has many antiquated names and does not reflect the current naming structure of NETCOM and FORSCOM. All references to regional chief information operations should be replaced by strategic Signal brigade. All references to department of information management should be replaced by NEC. Also deployable forces are currently being referred to as operation forces.

***CW3 Jason K. Dunn*** *is assigned as the current operations technician for the 93rd Signal Brigade (Strategic), 7th Signal Command, Fort Eustis, Va. He has served as an S6 technician and specialist in the 1st, 2nd, 3rd, and 25th Infantry Divisions. He spent 27 months in Iraq as part of OIF III and V as a member of 3rd BCT, 3ID. He will complete his bachelor's degree in IT management from AMU this year. He spent nine years as a 31U/25U prior to his appointment as a warrant officer in 2004. He graduated the Warrant Officer Advanced Course in 2009.*

## ACRONYM QuickScan

**AD** – Active Directory
**ATC** – Approval to Connect
**BG** – Brigadier General
**BCCS** – Battlefield Command and Control System
**BDE** - Brigade
**CMD** – Command
**CoN** – Certificate of Networthiness
**DF**- Deployable Forces (replaced by OF in newer versions)
**DOIM** – Department of Information Management
**EDS-P** – Electronic Data Systems – Provisioning
**FOB** – Forward Operations Base
**FORSCOM** – Forces Command
**FY** – Fiscal Year
**IA** – Information Assurance
**IAM** – Information Assurance Manager
**ICAN** – Installation Campus Area Network
**IT** – Information Technology
**MOA** – Memorandum of Agreement
**NEC** – Network Enterprise Center
**NEST** – Network Enterprise Support Team
**NETCOM** – Network Enterprise Technology Command
**OF** – Operational Force
**OU** – Organizational Unit
**PM** – Program Manager
**RCIO** – Regional Chief Information Operations
**SC** – Signal Command
**SLA** – Service Level Agreement
**SSB** – Strategic Signal Brigade
**TA** – Technical Authority

# ESB network management paradigm shifts

*By CW2 Joshua Callahan*

Leaders of the Signal Regiment have made it clear that they want to encourage creative solutions for future programs and technologies that improve shortfalls with today's units and systems.

The expeditionary Signal battalion has been fully engaged in the operational battle order since July 2007. The operational requirements have ranged from assignments supporting regiments at the headquarters level, military transition teams, brigade combat teams augmentation and Striker BCTs, to joint support with Homeland Defense/Homeland Security missions. The ESB has also provided strategic support to tactical technical control facilities. To provide this support they have been detailed into every level including, team, expeditionary Signal company, battalion minus and everywhere in between.

The job of network operations over the past few years has been difficult and frustrating. The amount of tools available is not the issue. The major concern is determination of "who's in control and who's responsible?" The known assumption is that the battalion staff will always go where the battalion commander goes, and with that staff comprises the NETOPS section. As network managers, one of our many responsibilities is to provide the commander networked command and control world-wide. No matter where the commander is, or where command assets are located, providing situational awareness and/or network management for the commander is essential.

Using the recent operational tempo of one ESB over a two year span, one can gain an understanding of how disassociated the unit can become. Immediately after being fielded Joint Network Node equipment, one unit deployed to Iraq as a battalion minus for 15 months. Another ESC, which deployed a few months earlier, supported a regimental headquarters for 15 months. The battalion's mission was multifaceted, providing support across three separate divisions as well as connectivity between "strategic" TCFs in-country. The battalion then redeployed to the United States and was hurriedly pushed through the reset program in order to provide support for an 18-month joint task force-civil support chemical, biological, radiological, nuclear, and high yield explosives mission. The previously deployed ESC was tasked yet again to prepare for yet another deployment in support of a Regimental headquarters. This was separate from the battalion and the battalion's Army Force Generation cycle. Once the battalion completed the 18-month JTF-CS mission, its remaining two ESCs were tasked to deploy to two separate theaters supporting two separate missions.

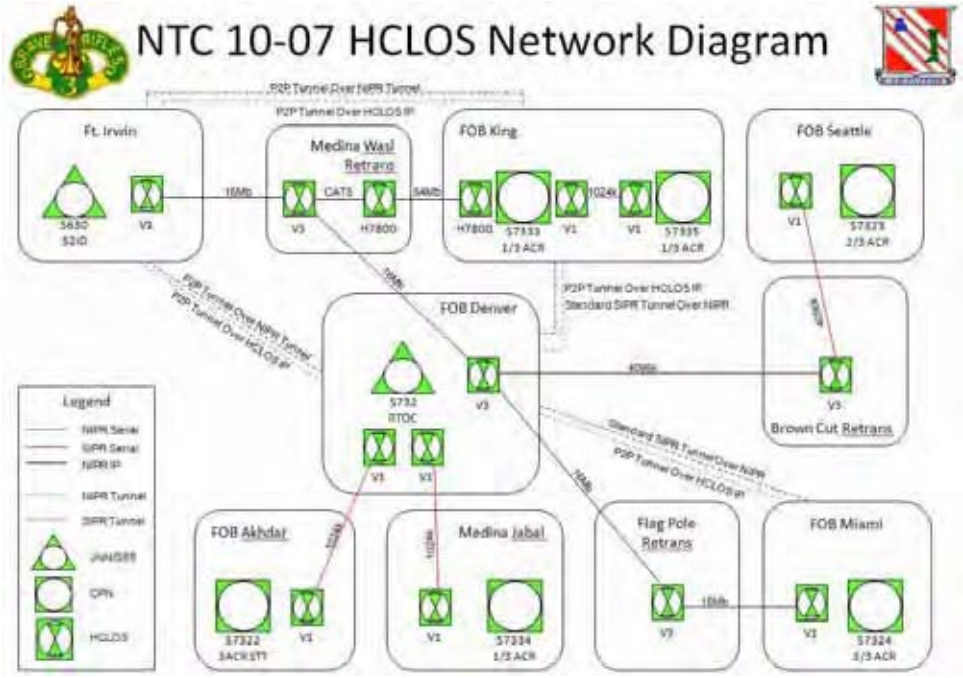



Diagram 1

In light of this operational tempo, technical and personnel changes could go a long way in providing a more solid network C2 for an ESB commander whose assets are continually engaged in missions across the globe.

First, each ESC should be assigned a WO1/CW2 255N. An ESC's BCT (which is smaller in asset size) is afforded a 255N. If an ESC can deploy autonomous from the battalion it seems reasonable that it should be afforded no less. The recent Signal Functional Area Assessment recommended course of action, currently out for world-wide staffing, suggests this personnel move within the ESB.

Second, an ESB could establish a network operations center at its home station, utilizing the

Global Network Enterprise Construct. Doing this would provide situational awareness for a commander whose assets can be engaged in separate missions across the globe at any given time. The GNEC provides a global plug-and-play ability to connect to Army, joint and commercial networks through all phases of joint operations. Leveraging this capability will enable an ESB commander to maintain a sufficient level of situational awareness regardless of where command assets are throughout the world. This capability increases exponentially when an ESB runs concurrent missions in both CONUS and overseas. The degrees by which a commander maintains network C2 can be adjusted and maintained from one central location. In addition, by maintaining a home station NOC, the battalion can afford those key individuals the opportunity to maintain perishable skills operating the battalion level NETOPS suite of equipment. It also allows for the equipment to stay current and updated on key patches, Information Assurance Vulnerability Alert updates, etc. The equipment would always "remain on," maintaining a constant state of readiness should the NETOPS cell need to deploy from its home station.

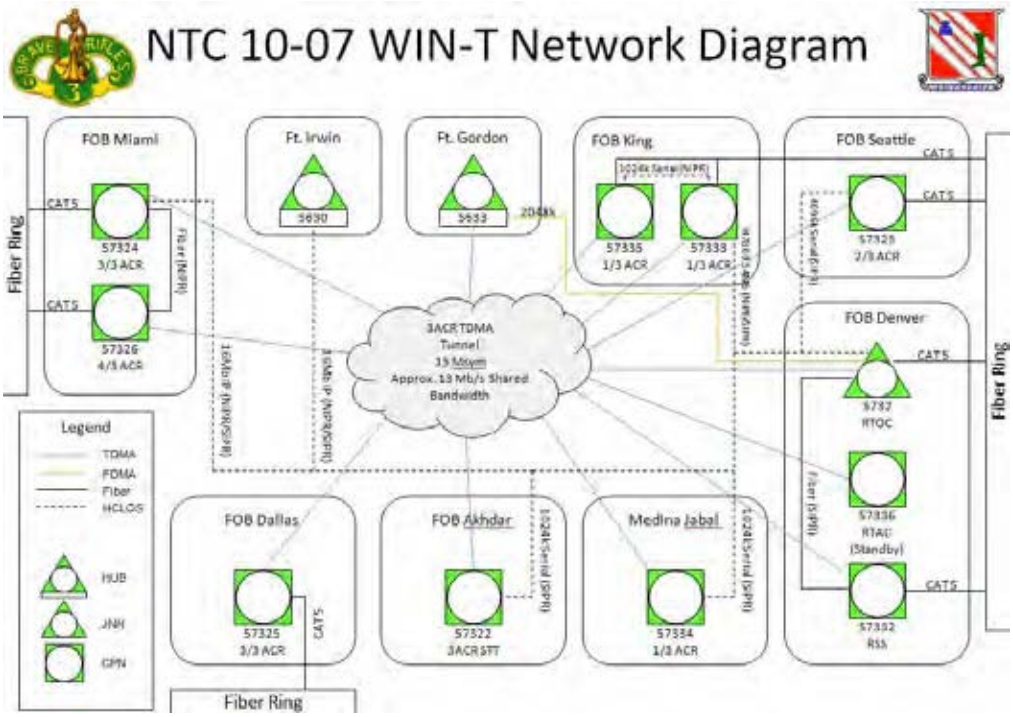



Diagram 2

In the current operational environment NETOPS control for non-organic Signal units is being pulled away from the battalions and brigades and continues to be consolidated at the higher, joint levels. This will not always be the case, however, as situations compel the need to be prepared for a push into a new engagement, to fight in an unconventional conflict, or provide support to the ongoing HLD/HLS missions. With these possibilities at hand the ESB's NETOPS must be prepared and capable to provide the commander solid and thorough network C2 anywhere, at anytime, and to any degree.

***CW2 Joshua Callahan*** *has served as an instructor/ writer for the School of Information Technology, Fort Gordon, Ga., since October 2009. He recently was assigned as a training with industry officer working with General Dynamics C4 Systems. Prior to that CW2 Callahan was the network management technician for the 63rd Expeditionary Signal Battalion Fort Gordon, were he fielded and deployed for 15 months with the Army's first ESB.*

## Acronym QuickScan

**ARFORGEN** – Army Force Generation
**BCT** – Brigade Combat Team
**BN** – Battalion
**BDE** – Brigade
**C2** – Command and Control
**CBRNE** – Chemical, Biological, Radiological, Nuclear, and High Yield Explosives
**CONUS** – Continental United States
**ESB** – Expeditionary Signal Battalion
**ESC** – Expeditionary Signal Company
**FAA** – Functional Area Assessment
**GNE** – Global Network Enterprise
**GNEC** – Global Network Enterprise Construct
**HLD** – Homeland Defense
**HLS** – Homeland Security
**HQ** – Headquarters
**IAVA** – Information Assurance Vulnerability Alert
**JNN** – Joint Network Node
**JTF-CS** – Joint Task Force-Civil Support
**MiTT** – Military Transition Team
**NETOPS** – Network Operations
**NOC** – Network Operations Center
**TCF** – Technical Control Facility

# Charging toward an even brighter future

*By CW4 Richard C. Myers and CW5 Todd M. Boudreau*

Not the same, but equal is a good way to describe the warrant officer corps in relation to our O-grade cohorts.

Members of the Warrant Officer Career College in collaboration with the Senior Warrant Officer Advisory Council are continuing efforts to ensure the understanding that we are not trying to become the same as our O-grade officer counterparts, but rather seeking to be treated with equal recognition in all aspects such as protocol, etiquette, housing, and evaluation reporting, etc.

## The Problem at Hand

Since its formal inception on July 9th, 1918 the Army warrant officer rank has existed in a state of ambiguity. In fact, in 1921 there was one rank (the Eagle Rising) with two pay grades. Years later, the Career Compensation Act of 1949 provided two new pay rates for warrant officers. The designations of warrant officer junior grade and chief warrant officer were retained. However, the grade of chief warrant officer was provided with pay rates of W2, W3 and W4. Throughout this period it was commonplace to associate all warrant officers as equal regardless of pay rate.

A whole new era for warrant officers began when the Army chief of staff chartered the Department of the Army Total Warrant Officer Study Group in September 1984. This was the first DA-level comprehensive study of warrant officer management. A key element of TWOS was coding of positions in authorization documents by rank. This provided a distinct requirement and clearly recognized the progressive increase in expertise and responsibility.

The Army has made tremendous strides with the formal integration of warrant officers into the officer corps. In fact, the Army has combined the officer and warrant officer corps in many areas, such as Professional Military Education, Officer Evaluation Reports, and wearing of branch insignia. This integration is in keeping with the recommendations outlined in the July 2002 Chief of Staff of the Army chartered Army Training and Leader Development Panel-Warrant Officer Study Final Report. Nonetheless, this merger is only partially complete.

One critical aspect of the effort to form a single officer corps that the Army has not formally addressed is the delineation of the precedence of WO ranks in numerous publications (e.g., DA Pamphlet 600-60).

The truth of the matter is that times are changing faster now for the warrant officer cohort than at any other time in the Army's history. Senior warrant officers are serving at all levels of command to include the Army chief of staff level where the senior warrant officer advisor serves as an AXO to the CSA.

The U.S. Army National Guard, U.S. Army Reserves, and all states have command chief warrant officers. Each branch has a CWOB or regimental chief warrant officer. The WOCC has a senior warrant officer deputy commandant. The Combined Arms Command has a command warrant officer. Special Forces has a regimental and group chief warrant officer.

Senior warrant officers fill numerous other high-level strategic and operational level positions. However, the Army has not formally acknowledged these significant historical gains by updating its regulations. Indisputably, the warrant officer role and level of responsibility has expanded greatly. Current protocols do not appropriately reflect those changes.

The lack of official clarification of warrant officer precedence in Army regulations sets a stage for inconsistent treatment of warrant officers from one installation to the next. Installations normally address order of precedence in installation standing operating procedures. The lack of clarity and standardization for warrant officer precedence is not merely an issue of recognition or equity. Rather, it affects a multitude of duty roles and responsibilities such as staff duty, field officer of the day, inspector general activities, financial liability officers, and investigating officers, etc.

Based on the decision by Army leaders that warrant officers will be fully integrated into the officer corps, integration actions should go forward in a deliberate, formal, and meaningful manner. The delineation of precedence should address how warrant officers will be categorized by rank with respect to officer utilization and recognition. The questions of duty rosters, boards (e.g. administrative action, courts martial, etc.) and housing authorizations should be addressed.

## What Has Changed and What it Means

There have been a number of small changes over the last several years that appear very promising to the WOCC/SWOAC and all warrant officers. One example is outlined in DA PAM 420-1-1 (Housing Management). In the past, all warrant officers were characterized as company grade officers. In most cases this works well. Many post commanders, however, would offer field grade officer housing to W3s and above; but not all.

The current regulation now delineates tri-service-sizing benchmarks by pay grade and number of bedrooms under five categories: (1) General/flag officer (O-7 and above); (2) Senior officer (O-6); (3) Field grade officers (O-4 and O-5), warrant officers (WO4 and WO5), and senior Non-Commissioned Officer (NCO) (E-9); (4) Company grade officers (O-1 through O-3), warrant officers (WO1 through WO3), and senior NCOs (E-7 and E-8); and (5) Junior NCOs (E-5 and E-6) and private (E-1) through corporal/specialist (E-4).

While some have said this is a success story and the beginnings of a formal delineation of precedence for warrant officer ranks, a closer look indicates several inadequacies (similar to the inadequacies of Army Regulation (AR) 420-1). One recommendation by the WOCC/SWOAC is for CW5s serving as regimental chief warrant officers, chief warrant officer of the branches, the command chief warrant officer of the reserves, the command chief warrant officer of the National Guard, or in any of the three- and four-star nominative positions should be considered key and essential personnel and, therefore, accorded senior grade housing.

Additionally noted is an officer in the grade of CW3 who would (under the old informal system) often be assigned field grade housing. So, in the case of housing, W3s are given company grade officer correlation while W4s and W5s are afforded field grade officer correlation. That does not make W4s and W5s field grade officers. We are not the same; nor should we be. I, even as the RCWO, do not have anywhere near the same level of responsibility (or authority) as a battalion or brigade commander. However, even though we are not the same, this division begins to provide an equality in delineations with the w-grade ranks as compared to the o-grade and enlisted ranks. (Should this be inequality?

But what about the W3? AR 623-3 (Evaluation Reporting System) mandates the use of the Developmental Support Form (DA) Form 67-9-1a) to support developmental actions and integrate it with performance for officers in the rank CPT/LT (company grade officers) and warrant officers in the rank of CW2/WO1. The only place in official Army guidance that specifically addresses the point of delineation precedence by rank is in the mandate for the implementation and use of the Developmental Support Form. The use of the DSF as outlined in AR 623-3 and DA PAM 623-3, Chapter 2-2, for all company grade officers is mandated. Company grade officers were identified in the instructions as WO1s, CW2s, 2LTs, 1LTs, and CPTs. Thus, based on the DSF implementation guidance, WO1s and CW2s are considered equivalent to company grade officers while all CW3s, CW4s, and CW5s are categorized as possessing significant experience and, although not identified as field grade or higher officers (i.e., not the same), implicitly recognized as being equivalent to field grade officers (but equal). The intent of the DSF is widely understood and, although it was not intended as a tool to identify an officer's standing within the officer corps, it does demonstrate the awareness and appreciation the Army has for warrant officers' vast experience.

Furthermore, AR 623-3 states that Part VIIb will not be completed on MGs, CPTs, LTs, CW5s, CW2s, and WO1s. An electronically generated label that states "No Box Check" will be placed over the boxes in Part VIIb by HQDA. This section of AR 623-3 makes a number of critical points relative to precedence of officer ranks.

First, it clearly infers that WO1/CW2 are equivalent to company grade officers by allowing the rater and senior rater the opportunity to develop and mentor young officers without the worry of "Box Checks."

Secondly, it infers that the ranks of CW3 and CW4 closely correlate to the ranks of MAJ and LTC in terms of status. Both have matured within their functional areas by serving in a variety of professionally rewarding positions that are ultimately preparing them to serve in senior level military positions.

Finally, CW5s, similar to MGs, do not receive a "Box Check" on evaluation reports. Evaluations are not required for CW5s serving in nominative three-star and four-star level positions. Regardless of the level at which they serve, CW5s have reached the pinnacle of their profession. This regulation recognizes that success.

Another recommendation the WOCC/SWOAC is offering suggests that all regulations and publications conform to the following equivalency standard: (1) WO1/CW2: Company Grade Officers (2LT

**(Continued on page 78)**

(Continued from page 77)

through CPT), (2) CW3/CW4: Field Grade Officers (MAJ/LTC), and (3) CW5: Senior Grade Officers (COL).

AR 600-89 (GEN Douglas MacArthur Leadership Award Program) is another benchmark for use in such delineation of warrant officer ranks. According to this AR candidates must meet the following criteria: (1) be company grade officers in the rank of second lieutenant (2LT), first lieutenant (1LT), captain (CPT), warrant officer one (WO1), or chief warrant officer two (CW2) in the U.S. Army. Captains or CW2s must not be on a promotion list to major or CW3, respectively, as of 31 December of the calendar year considered. The nomination criterion clearly eliminates the possibility of CW3 and above competing for the GDMLAP even though there is no formal recognition of warrant officers of any rank as field grade officers. The WOCC/SWOAC agrees that W3s and above should not be eligible for the GDMLAP. However, we do seek formal recognition in appropriate regulations identifying W3 and above as possessing a correlation to field grade status; again, not the same, but equal.

AR 385-10 (The Army Safety Program) currently reads, "The president of the board will be a field grade officer (W4/W5 is considered field grade) or an Army civilian, familiar with the type of operation, in the grade of GS–12 or higher." AR 385-10 is one more reference that supports the WOCC/SWOAC position on formal delineation of precedence of w-grade ranks. Specifically, this regulation recognizes "W4/W5" as equivalent to field grade as well as GS-12 or higher. When considered with other regulations such as DA PAM 600-60 (A Guide to Protocol and Etiquette for Official Entertainment) where warrant officers are placed lower in order of precedence than GS-7s, the inconsistency becomes apparent. This inconsistency fosters confusion and widespread misunderstanding about the order of precedence for warrant officers. The WOCC/SWOAC recommendation is to replace "W4/W5" with "CW3 thru CW5" and use the order of precedence outlined in this regulation to update DA PAM 600-60 as noted below.

## What Has Not Changed and What it Means

AR 420-1 (Army Facilities Management) still maintains family housing designations for occupancy as follows: (1) General and flag officers (O10 through O7); (2) Senior grade officers (O6); (3) Field grade officers (O5, O4, CW5, and CW4); and (4) Company grade officers (O3 through O1, CW3 through WO1). As noted above, this structure is incongruent with that provided in other publications. This type of disparity continues to create confusion as to the recognition of warrant officers. This supports the perception that the warrant officer cohort is simply an appendage of the officer corps that, as a whole, is not fully integrated.

AR 15-6 (Procedures for Investigation Officers and Boards of Officers) currently reads, "Who may be appointed. Investigating officers and board members shall be those persons who, in the opinion of the appointing authority, are best qualified for the duty by reason of their education, training, experience, length of service and temperament. (1) Except as provided in paragraph 5–1e, only commissioned officers, warrant officers, or Department of the Army civilian employees permanently assigned to a position graded as a GS–13 or above will be appointed as investigating officers or voting members of boards." The wording of this paragraph places warrant officers in the same category as GS-13s, clearly supporting that warrant officers should not be placed in order of precedence below GS-7s as is done in DA PAM 600-60. Again, placement of WOs at different precedence levels in different Army publications makes it extremely difficult to identify the warrant officers' standing within the Army. This regulation's implication that WO1s are equivalent to GS-13s appears to be appropriate in that many GS-13 civil service jobs are non-supervisory journeyman, whereas their professional supervisory equivalent is a WO1 (for example, the 1811GS-13 Criminal Investigator as compared to the 311A Army Criminal Investigator).

The WOCC/SWOAC considers AR 15-6 another success story in that it supports our request for formal delineation of order of precedence for warrant officer ranks. The wording of the regulation acknowledges that warrant officers are professional Soldiers who possess the prerequisite leadership attributes and characteristics to execute sensitive duties such as investigating officers' duties. However, the term "commissioned or warrant officers" should be changed to "O-grade or W-grade officers" as all warrant officers in the grade of CW2 and above are commissioned officers. The current wording creates confusion.

AR 600-60 (Physical Performance Evaluation System) states that the convening authority will ensure all cases forwarded by the MOS/Medical Retention Board are reviewed. The review of the cases may be delegated to an officer on the MMRB convening authority's staff in the grade of major or higher or CW4. Again, this regulation correlates a warrant officer rank with that of a field grade officer. However, the use of CW4 in lieu of MAJ is inconsistent with the whole of the WOCC/SWOAC's premise and the recommended order of precedence and as such CW4 should be replaced by CW3.

These are not all of the publications the WOCC/SWOAC is reviewing, nor are these all recommended changes. Field Manual

22-6 (Guard Duty), AR 20-1 (Inspector General Activities and Procedures), AR 570-4 (Manpower Management), AR 405-7 (Facilities and Areas Policies), DA PAM 735-5 (Financial Liability Officer's Guide), and AR 27-10 (Military Justice) are also being reviewed with numerous changes recommended due to their inconsistencies, errors in wording, and equating W5s with O3s and GS-10s, for example.

One final example is relevant. DA PAM 600-60 (A Guide to Protocol and Etiquette for Official Entertainment) contains a table which lists the precedence of civilian and military persons and places all warrant officers under VIP Code 8 of 8, between second lieutenants / GS-07s and master sergeants. Based on this pamphlet, WO1 through CW5 are categorized as one entity and accorded a lower precedence than 2LTs and GS-7s. However, command sergeants major and all of the O-grade officers are individually broken out.

As highlighted throughout this article and validated by numerous regulations, CW3s and CW4s routinely supervise and rate civilian employees. CW5s are nominated to serve as the RCWO/CWOB for school commandants, usually a commanding general, in 15 Army branches, and the Army chief of staff has senior warrant officer advisor. In essence, the CW5 RCWO/CWOB is entitled to no true protocol etiquette, although the other two members of the command team –CG and CSM--receive full protocol privileges at functions which they all attend.

The reality for warrant officers is that we regularly experience protocol issues, even ones as simple as seating arrangements at military ceremonies, funding for attending official military events, and billeting while on TDY. Installation protocol personnel routinely lack the guidance to appropriately delineate treatment of warrant officers. In most cases protocol personnel fail to acknowledge warrant officers at all.

I am extremely proud to say that the Signal Center of Excellence command group protocol team members have done their utmost to take care of me as well as all other warrant officers visiting Fort Gordon. When one considers the fact that DA PAM 600-60 suggests that the RCWO of the Signal Regiment serving at the two-star level is accorded a lower precedence than a 2LT serving as a platoon leader, it becomes extremely evident that the pamphlet is outdated.

This failure to specify an order of precedence for warrant officer ranks in keeping with their designation as officers and their levels of responsibility continues to drive a wedge among cohorts. The recognition warrant officers receive for rising to the top of their profession is decidedly unequal. This is incongruent with delineation of order of precedence for other cohorts. Unless the Army directly and specifically addresses these issues, the inconsistency will continue. The WOCC/SWOAC will continue addressing these issues.

In DA PAM 600-60 we recommend that the protocol precedence for warrant officers be addressed using the company grade, field grade, and senior grade officers construct outlined below and that positions such as RCWO and all nominative positions be addressed as is done with CSM duty positions.

Recommended Changes to Appendix D Precedence List: warrant officer ranks should be broken down individually with the recommended equivalency listed below:

WO1: Company Grade Officers Equivalent to 1LT Falling Under VIP Code 8

CW2: Company Grade Officers Equivalent to CPT Falling Under VIP Code 8

CW3: Field Grade Officers Equivalent to MAJ Falling Under VIP Code 8

CW4: Field Grade Officers Equivalent to LTC Falling Under VIP Code 8

CW5: Senior Officers Equivalent to COL Falling Under VIP Code 7

Specific Position Precedence:

011A Nominative Positions equal to the level for which they serve

Senior Warrant Officer Advisor to the CSA: VIP Code 4 (Same as SMA)

Senior Warrant Officer Advisor to VCSA: VIP Code 5

Senior Warrant Officer Advisor to the Secretary of the Army: VIP Code 5

Deputy Commandant Warrant Officer Career College: VIP Code 7

CASCOM Senior Warrant Officer: VIP Code 7

Regimental Chief Warrant Officers/Chief Warrant Officers of the Branch: VIP Code: 7

Chief Warrant Officers of the State: VIP Code: 7

## Some Final Thoughts

The formal integration of warrant officers into the officer corps as outlined in the July 2002 Army chief of staff chartered ATLDP-WO Study resulted in a need for the Army to re-examine its established system for recognizing warrant officers. According to US Code Title 10, Subtitle B, Part II, Chapter 345, Section 3575 "Warrant officers rank next below second lieutenants and rank among themselves within each warrant officer grade under regulations to be prescribed by the Secretary of the Army."

It is acknowledged that the warrant officer cohort fully understands that a newly commissioned 2LT will always outrank the most senior CW5 in the same manner that the 2LT outranks the SMA. However, those fortunate enough to have achieved noteworthy ranks such as general officers, colonels, lieutenant colonels, sergeant major of the Army,

**(Continued on page 80)**

(Continued from page 79)

command sergeant major, and sergeant major are all accorded honorary privileges that CW3s, CW4s, and CW5s are not accorded.

The premise of recognition sought refers to whatever duty or responsibility is accorded that status – field officer of the day, housing, parking, event protocol, and etiquette, not seniority in rank. By standardizing protocol regulations, the Army will remove the current inconsistencies for warrant officers in comparison to the officer and noncommissioned officer cohorts. Therefore, the purpose of the WOCC/SWOAC emphasis is to obtain CSA approval to update all regulations, pamphlets, and policies regarding the formal delineation of the precedence of Army warrant officers.

Formally addressing this issue will require a significant cultural change for the Army including officers, warrant officers, NCOS, and civilians. It was the ATLDP-WO Study Final Report, which highlighted the necessity for cultural change to how warrant officers are recognized, utilized, managed, and educated. In support of our request for clarification of warrant officer precedence the ATLDP-WO study states, "It is also about the practices and policies that dilute their efforts and detract from their remarkable, selfless, and honorable service to the Nation." Additionally, the report discusses how the Army must implement the ATLDP recommendations in their entirety to receive the synergistic benefits. Therefore, correcting the warrant officer precedence disparity is a significant step toward meeting the recommendation of this report and an essential ingredient to successfully integrating warrant officers into the larger officer corps.

## What This Will Mean

If approved, there will be a requirement to update Army as well as local regulations and policies. There is no impact on equipment, funding, environment, or stationing. The major impact will be on the utilization of warrant officers. A subset of this recommendation will be an unambiguous order of precedence that establishes distinction amongst ranks within the warrant officers cohort.

In the past, warrant officer ranks have been bundled together as one rank whereas the other cohorts specifically address their senior personnel and the recognition of each of those ranks. By clarifying order of precedence for warrant officers, the Army would pave the way for warrant officers to truly become a part of the greater officer corps. This would ultimately impact the warrant officer component of the officer corps significantly, clearly conveying the message that warrant officers truly are integrated and, as such, professionals that the Army values and recognizes.

Those of us who are "Quiet Professionals" stand ready to continue our service to our Soldiers, commanders, our Army, and this great Nation. We serve with honor and take great pride in our contributions as Soldiers and warrant officers. However, we are convinced that the lack of Army-wide understanding of the level of expertise and experience that we bring to the table negatively impacts our ability to fully serve at the level and to the degree to which we are capable. Because of this conviction, we humbly request that the Army's senior leadership continue and, if possible, accelerate the positive progression toward formally recognizing warrant officers' standing among the other cohorts. Toward that end, revision of DA PAM 600-60 should be a matter of urgency. If the Army is to successfully integrate the warrant officer cohort into the Officer Corps, it must revise/rewrite this pamphlet immediately.

This ongoing concern is not about becoming the same as any other cohort, but rather seeks equality in setting a formal recognition of delineation within the warrant officer ranks.

It would be unfortunate to take away from this article the idea that the warrant officer cohort is looking for a set of increasing privileges. This is far more encompassing than privileges. This is a necessary step toward clarification, recognition and duty. With the earned position of senior rank, warrant officers must be empowered to assume greater responsibility and exercise greater authority

In a previous letter to the Regiment in the front of the *Army Communicator*, I related how on several occasions my flight reservations were bungled, during my travels through Kuwait, Afghanistan, and Iraq. However, as a CW5, I was also given a seat on the flight because I was afforded category 1 status on military flights. This status has always been extended to colonels, sergeants major and command sergeants major, but not always for CW5s.

Some might view this as a privilege. However, my itinerary was packed with visits to senior level commanders and operating units. The daily battle rhythm was interrupted to meet my published itinerary. Therefore, I was responsible to be where I was supposed to be, when I was supposed to be there.

In other words, there is more at stake here than a parking spot at the post exchange.

***CW4 Richard C. Myers*** *is currently assigned as the proponent officer at the Warrant Officer Career College, Fort Rucker, Ala. His previous assignments include 1st ID, 1st AD, 3rd ID, 4th ID, and 24th ID. CW4 Myers has multiple deployments and overseas assignments to include Iraq, Kuwait, Kosovo, and Germany. He is a graduate of ILE, Army Force Management Course, and Warrant Officer Senior Staff Course. CW4 Myers holds a Master of Business Administration from Touro University. He has 22 years of military service with 13 years as a warrant officer.*

**Author Credit**

*Several articles in this edition are written or edited by* ***CW5 Todd M. Boudreau.***

*CW5 Boudreau is the third Signal Regimental chief warrant officer.*

*Previously he served as the Signal warrant officer proponent manager, Office Chief of Signal, U.S. Army Signal Center of Excellence and Fort Gordon, Ga.*

*He enlisted in the Army in 1983 and attended Strategic Microwave Maintainer-Repairer (26V) advanced individual training at Fort Gordon.*

*Before his appointment as a warrant officer, he completed the Primary Leadership Development Course, Noncommissioned Officer Academy, Camp Jackson, South Korea, and the Basic Noncommissioned Officer Course, Noncommissioned Officer Academy, Fort Gordon. He received his warrant officer appointment in 1990.*

*His enlisted assignments include the 36th Signal Battalion, Korea and the Alternate National Military Command Center (Site-R), Md. His past warrant officer assignments include maintenance officer for the 6th Theater Signal Command, Saudi Arabia; station manager for the Fort Detrick Satellite Complex, Md; training, advising and counseling officer at Fort Rucker, Ala; officer in charge of the Standardized Tactical Entry Point and Communications Complex at Fort Buckner, Okinawa, Japan; communications officer for the Supreme Allied Commander, Supreme Headquarters Allied Powers Europe, Belgium; and satellite systems engineering officer, Defense Information Systems Agency Europe, Stuttgart, Germany.*

*CW5 Boudreau is a recipient of the Bronze Star Medal, two Defense Meritorious Service Medals, five Army Meritorious Service Medals, two Army Commendation Medals, three Army Achievement Medals, two Army Good Conduct Medals, National Defense Service Medal with Bronze Star, Southwest Asia Medal with three Bronze Service Stars, Global War on Terrorism Service Medal, Korea Defense Service Medal, Saudi/Kuwait Liberation Medal, Kuwait Liberation Medal, Meritorious Unit Citation, Army Superior Unit Award, Military Outstanding Volunteerism Medal, and the Drivers/Mechanics Badge. He also received the Signal Corps Regimental Association's Order of Mercury.*

*He is married to the former Soonja Yoon and has two sons, Patrick who is a senior Airman currently stationed in Korea and Jesse who works as the floor manager of the Panzer Kaserne Service Federal Credit Union.*

*CW5 Boudreau also serves as the associate pastor for Augusta First Assembly of God.*

# We want to hear from you!

Opinions and comments from *Army Communicator* readers are highly valued. If you have a question or an opinion about something you read in Army Communicator, send an e-mail to the editor at ACeditor@conus.army.mil. Please include your full name and unit. Items may be published and are subject to editing for style, clarity, accuracy, length and propriety.

You can also visit https://signallink.army.mil to join an online discussion allowing you to go directly to an article and follow the string of comments. Voice your opinion or suggest areas of concern for future coverage. This evolving beta test site is designed to make it quick and easy for you to connect your ideas for improving the information provided.

You, *Army Communicator* reader are our most important resource. How are we doing? How can we serve you better?

DEPARTMENT OF THE ARMY
ARMY COMMUNICATOR
USASC&FG
ATTN: ATZH-POM
Fort Gordon, Georgia 30905-5301

OFFICIAL BUSINESS
ISSN 0362-5745

PERIODICALS
Postage and fees paid
at Augusta, Georgia and
additional cities

"I take all knowledge to be my province. For knowledge, too, is itself a power."

*- Sir Francis Bacon*

**LTC Roberta Samuels**
Knowledge Mgmt Officer
101st Airborne Division
Afghanistan

***Read in the next edition of the Army Communicator how LTC Samuels continues making an impact as the Signal Regiment explores its role in Knowledge Management.***

# ARMY COMMUNICATOR

Signal Towers, Room 713
Fort Gordon, Georgia 30905-5301

PIN:100795-000