

# Signal Regiment personnel structure evolving to support changing operations

By Office Chief of Signal Staff

As our Army continues evolving to meet different requirements, U.S. Army Training and Doctrine Command leaders continue managing the changes through Doctrine Organization Training Materiel Leader Development Personnel and Facilities processes.

Any change in the way the Army does its business is managed through one or more of these "domains."

This article is about the "Personnel" domain and the Regiment's work in ensuring our Personnel structure is in full support of Army operations.

A significant driver of change in all of the DOTMLPF areas is cyberspace operations. Although

the characteristics and application of cyberspace terminology are still evolving, we do have Department of Defense definitions for cyberspace on cyberspace operations: Approved DoD Definition of Cyberspace (12 May 08) - a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

Approved DoD Definition of Cyberspace Operations (08 Oct 08) - the employment of cyberspace capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace. Such operations include computer network operations and

activities to operate and defend the Global Information Grid.

From these, you can see that the Signal Regiment plays a key role in this new domain.

One needs only to read the newspapers and journals in reference the development of new technologies and standards or the daily attacks on our networks to understand why leaders and managers in the Signal Regiment are working a number of initiatives to build, operate, and defend cyberspace.

None of this is a new concept to the Signal Corps.

Since its formation during the Civil War, the Signal Corps has been executing these types of functions.

We needed to occupy the hills to ensure a visual line of site for communications.

We installed a wired network when sufficient time was available to provide a more robust and secure means of communication. Even then, we used codes to protect the information that was being passed over our networks.

Today, this work continues much the same in concept but, of course, radically different in technology and scope.

This article primarily focuses on the Signal Regiment's mission to defend the network; but defending the network is only one piece of our Network Operations mission.

Beginning with our Branch 25 Signal Officer, we are pushing forward with a concept that will provide additional technical education. From lieutenants to colonels, Signal officers must always be leaders first and foremost. In order to lead in this increasingly technical environment, we want

UNCLASSIFIED



## Proposed Signal Regiment Holistic Officer Transformation

### Legacy "As-Is" Signal Regiment AOC

- 25A – Signal Officer
- 24A – Telecommunications Systems Engineering
- 53A – Information Systems Management

Submit DA Pam 611-21 Military Occupational Classification Structure (MOCS) Expedited Change Action **NLT 31 May 2013**

### Signal GO Guidance :

- Structure Officer AOC for Cyber
- BR25
  - More technical education and experience
  - Lead Mission Command and NETOPS integration
- FA53
  - More technical-engineering based (FA24 Like)
  - Enable knowledge management
  - Address cyber security

MOCS Action

### Notional Signal Regiment AOC:

- BR25 – Signal (2LT-COL)
  - 25A – Signal Operations
  - 25G – Network Integration (New)
  - 25Z – Signal Operations (immaterial @ COL)
- FA26 – Cyberspace Systems Engineering (CPT-COL)
  - 26A – Network Systems Engineering (old 24A)
  - 26B – Information Systems Engineering (old 53A)
  - 26C – Security Systems Engineering (New)
  - 26Z – Cyberspace Engineering (immaterial @ COL)

UNCLASSIFIED

to provide a better understanding of technical capabilities that can support a myriad of missions. Today our Functional Area 24, telecommunications engineers and Functional Area 53, information systems managers perform most of the complex planning and engineering of the network within the officer cohort.

In order to ensure our Signal Officers are better postured during the military decision making process to develop technical courses of action that support the commander's operational intent, we want to create a course that provides the right knowledge, skills, and abilities required to oversee the planning, engineering, installation, operation, and defense of friendly cyberspace.

It must be emphasized that the officer concept that follows is pre-decisional and more analysis and coordination is required before going final.

In order to drive more technical training for Branch 25, a new Area of Concentration would be created, 25G, network integration officer. The intent is to ensure that all of our branch 25 officers receive this training while en route to an assignment requiring those skills.

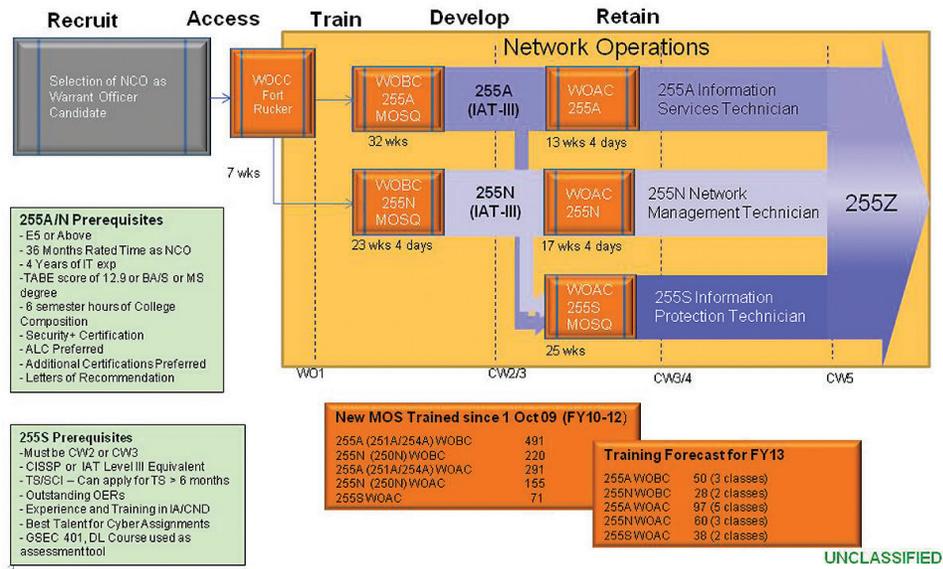
It is an important feature of this concept that once the officer receives the training and finishes the assignment, that officer is not restricted to only 25G assignments. He/she is able to be assigned to any 25 position. This will ensure that we continue producing officers with an increased level of skill, who will then be assigned throughout the Army. These officers will continue to be eligible and competitive for Central Select List positions which include command and key billets.

Our Functional Area officer structure will undergo a significant change. We will create a new Functional Area 26 cyberspace systems engineering, within which we will have three AOCs: AOC 26A will be our network systems engineer and closely aligned with our current FA24; and AOC 26B, information systems manager and drawn from our current FA 53. What is new is the creation of FA26C, security systems engineer.

This new AOC will also have the defense of the network as a primary focus. Our analysis shows that the career path for an officer desiring to be a 26C will incorporate skills acquired through assignments to both 26A and 26B positions. This ability to assign these officers still within the FA26 but also between



## Signal Warrant Officer Transformation (Implemented 1 Oct 12)



AOC 26A and B as required is a key feature to this realignment.

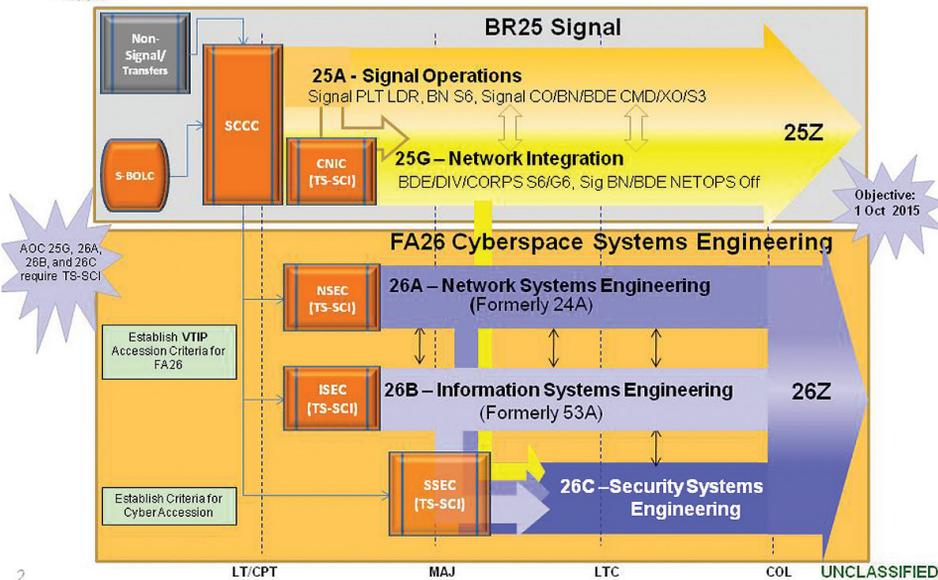
Planners within the SIGCoE recently completed what we called a Subject Matter Expert Panel which looked at the requirements and skill sets for these technically trained and educated leaders. It is important to note that the Chief of Signal MG LaWarren V. Patterson in his opening remarks to the Board challenged them to look as far into the future as their crystal ball would allow. The dynamic nature of information technology and the very challenges that new technology introduces require us to be proactive and agile so that we can ensure we are posturing our officers and the Army for success.

The transformation of our warrant officers is virtually complete. Effective 1 October 2012, a new warrant officer Military Occupational Specialty structure appeared in Army authorization documents. This transformation aligned a warrant officer with each component of NetOps: enterprise systems management (network management), content management (information services), and network assurance (cyber security). This personnel alignment maps precisely with the documented organizational structure for the corps/division G-6s and BCT/multifunctional brigade S-6s. Two of our warrant officer MOSs (255A and 255N) are refinements of the older version of our warrant officer structure in that the 255A's pri

(Continued on page 8)



## Revise BR 25 and Establish New Graduate Level Systems Engineering FA26



(Continued from page 7)

mary function is the information systems and the 255N's primary function is the network.

What is new is the 255S information protection warrant officer whose major focus is the defense of the network.

In our analysis, we determined that this area was becoming increasingly complex and capitalized on the skills and experiences that the 255A and the 255N were accruing so the 255S will be accessed at the CW3 grade from our other two warrant officer MOSs. This ensures that we have seasoned warrant officers focused on the defensive cyberspace operations mission. Assignments for this warrant officer will be down to the BCT level and all higher echelons to include national agency level.

Finally, our enlisted cohort will also undergo changes. An action has been submitted to TRADOC that will create the MOS 25D cyber network defender MOS. This enlisted Soldier will provide that backbone of support beginning at the BCT through to the highest echelons within the Army and joint level, DoD, and national agencies. Today, our MOS 25B, Information Technology Specialist, execute

some of these functions. The 25B, however, executes a broad range of requirements to include Systems Administrator, Network Administrator, Help desk, and more. The requirement is to have a Soldier who is dedicated to the mission of defending the network.

The creation of this MOS establishes a 'cradle to grave' career path that ensures a Soldier receives the right training and repetitive network defense assignments so the experience level of that Soldier grows with the ever changing mission. There will be five duty positions for the 25D: computer network defense infrastructure support, CND analyst, incident responder; CND auditor, and CND manager (E8/E9 level).

Similar to the accessions model discussed for the officers and warrant officers, this MOS will be an inter-service accession at staff sergeant from other specialties and based on proven performance and demonstrated level of skill. There will also be additional accession criteria for qualification. The Office Chief of Signal will be establishing a screening test to ensure the Soldiers accessed will be able to execute the complex demands of this MOS. Soldiers will also hold a current certification under either IAT Level II or IAM Level I IAW DoD 8570.01-M.

Although it is expected the vast majority of accession will come from our MOS 25B population, other Soldiers who have met the requirements in skill, leadership, duty performance and who are able to acquire a Top Secret clearance will be eligible.

If you are interested in these new professional opportunities, you need to seek out assignments that execute cyber security functions and acquire selected certifications. But as the officer AOCs and the enlisted MOSs do not exist yet, a call to HRC will not be productive. However additional information on the 25D MOS is available at the website: <https://www.us.army.mil/suite/page/838>

This process will take a few years and there will be a distribution of additional information as it is available.

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



### ACRONYM QuickScan

AOC - Area of Concentration  
 CND - Computer Network Defense  
 CSL - Central Select List  
 DoD - Department of Defense  
 DOTMLPF - Doctrine, Organization, Training, Materiel, Leader Development, Personnel, and Facilities  
 GIG - Global Information Grid  
 IT - Information technology  
 MOS - Military Occupational Speciality  
 NetOps - Network Operations  
 TRADOC - U.S. Army Training and Doctrine Command