

# USER COMPLIANCE IMPROVEMENT

By Grace E.H. Dalton

An innovative project at Network Enterprise Technology Command/9th Signal Command (Army) (NETCOM/9th SC(A)) has boosted information technology user compliance with Department of Defense and Army elevated-privileges requirements. NETCOM/9th SC(A)'s Information Assurance (IA) division – at the direction of senior leadership and Assistant Chief of Staff (ACofS) G-6, Stacy Ware - streamlined, consolidated, and replaced elevated privilege account creation processes at NETCOM Headquarters. The command forecasts even better compliance figures as the Army transitions to global enterprise operations.

“We are very excited about implementing this new and simplified procedure,” said Eric Tobias, NETCOM/9th SC(A)'s IA division chief and manager. “This novel process combines several compliance policies and streamlines them into one basic course of action. The end result enables the IT user to comply with the mandated elevated privileges requirements with a higher degree of conformity.”

NETCOM HQ defines privileged users as account holders with elevated privileges (e.g., escalated privileges, administrative privileges, and administrative rights). Privileged users perform mission-critical functions associated with system administration, network administration, database administration, system vulnerability assessments, web development, and web maintenance.

Evolving position responsibilities coupled with the emergence of the global enterprise created gaps in the elevated account creation and maintenance processes for those holding such privileges. Paperwork routing among the NETCOM HQ directorates became non-standardized, and the roles and responsibilities of employees in requesting and maintaining elevated privileges became primarily tacit. Now NETCOM HQ regulations and supporting documentation (to include the Acceptable Use Policy and Non-Disclosure Agreement blend several process documents into concise instruction for the requestor. Further, the process is documented and tracked, so employees' certifications and profiles are maintained as information management officer and IA security officer duties rotate to other individuals. NETCOM Regulation 25-4 and the NETCOM Elevated Privilege Tactics, Techniques, and Procedures document is a combined effort of the NETCOM 9th SC(A) ACofS, G-6 IA Division and the Fort Huachuca Network Enterprise Center IA Division.

“The standardization of processes and commonly used forms, like the Acceptable Use Policy are critical in ensuring seamless transitioning and processing of personnel across the Army,” said David Dillard, NETCOM/9th SC(A) deputy IA manager. Currently, many installations use their own version of the AUP or access request which defeats this standardization across the Global Network Enterprise Construct.”

The elevated account creation process is undergoing a

Rehearsal of Concept drill with selected directorates. The lessons learned will be used to refine the documents. Influence from all groups provides NETCOM HQ employees with customer-focused procedures, versus documents that take a purely academic standpoint.

To increase user compliance with DoD and Army requirements for elevated privileges, the ACofS, G-6 IA Division along with the Training Readiness Officer of the newly created Cyber Division have teamed to populate NETCOM HQ profiles and certifications within the Army Training and Certification Tracking System. Incorporating ATCTS into the process is important to hold elevated privilege account holders responsible for documentation and certification. Plans are also underway to include ATCTS in the employee in- and out-processing checklist at NETCOM HQ. In addition, monthly IMO and IASO meetings with the ACofS, G-6 IA Division will be held to ensure those having IMO and IASO duties remain familiar with the process, are updated on new policy developments and training, and adhere to DoD and Army requirements, ultimately strengthening NETCOM HQ's security posture.

Documenting the elevated privilege account creation process within NETCOM HQ ensures separation of duties on the network and reduces risk across the enterprise. Once the process is refined, document routing within the command will become automated. The process will minimize risk to LandWarNet by limiting elevated privileges, and maintaining the certifications to hold those rights. In time, NETCOM HQ's processes will help fulfill obligations, such as elevated privilege requests and maintenance, required for missions across the Army.

*Grace E. H. Dalton is currently with the Department of the Army, CIO/G6. She is a graduate of the Army Knowledge Leader program, an intensive 18 month IT management and leadership development program during which she held rotations with NETCOM 9th SC(A), ARNGRC, RDECOM, and HQDA CIO/G6. She holds a Master of Science in Information Assurance degree from Norwich University and is an associate of (ISC)2 towards CISSP.*

## ACRONYM QuickScan

**ACofS** – Assistant Chief of Staff  
**ATCTS** – Army Training & Certification Tracking System  
**AUP** – Acceptable Use Policy  
**IA** – Information Assurance  
**IASO** – Information Assurance security officer  
**IMO** – Information Management Officer  
**NEC** – Network Enterprise Center  
**NDA** – Non-Disclosure Agreement  
**ROC** – Rehearsal of Concept  
**TPP** – Tactics, Techniques, and Procedures