

**RECORD VERSION**

**STATEMENT BY  
MICHAEL E. KRIEGER, SES  
DEPUTY CHIEF INFORMATION OFFICER/G-6  
UNITED STATES ARMY**

**BEFORE THE**

**HOUSE ARMED SERVICES COMMITTEE  
SUBCOMMITTEE ON TERRORISM, UNCONVENTIONAL THREATS,  
AND CAPABILITIES**

**UNITED STATES HOUSE OF REPRESENTATIVES**

**SECOND SESSION, 111TH CONGRESS**

**INFORMATION TECHNOLOGY**

**MAY 5, 2009**

**NOT FOR PUBLICATION  
UNTIL RELEASED BY THE  
COMMITTEE ON ARMED SERVICES**

**STATEMENT BY  
MICHAEL E. KRIEGER, SES  
UNITED STATES ARMY  
DEPUTY CHIEF INFORMATION OFFICER**

Good afternoon, Chairman Smith and distinguished members of the subcommittee. As the Deputy Chief Information Officer and Deputy G-6 for the U.S. Army, I am pleased to appear before the subcommittee today to discuss the Army's activities to enable operations in cyberspace, and to address the policy, management, and technical challenges to enhance mission assurance in Cyberspace as a Warfighting Domain.

Securing cyberspace is a major issue for the United States as articulated in the December 2008 Center for Strategic and International Studies report. This report confirmed what the U.S. Army has already assessed – every day there are new threats and attacks against our network. I want to assure the members of this subcommittee that the U.S. Army has and continues to take action to mitigate these threats and improve our mission assurance in cyberspace.

There are many policy, management, and technical challenges to improving the U.S. Army's cybersecurity. We echo General Chilton's statement when he testified to this Subcommittee on March 17<sup>th</sup> this year, that the biggest challenge lies in changing the culture – the need to think about cyberspace, not so much as a convenience, but as a military necessity.

The U.S. Army believes that cyberspace – the enterprise network – needs to be viewed as a critical enabler for the Warfighter. In this era of Persistent Conflict, the U.S. Army is in the process of transitioning to a

Continental U.S.- based Expeditionary Force. Our ability to support a Joint Force Commander is highly dependent on having a secure global network continuously available to the Warfighter.

To change the culture, the U.S. Army is revising policies, reviewing the management of our people, and transforming how we operate the U.S. Army's portion of the DoD Global Information Grid (GIG) known as LandWarNet. The U.S. Army is also enhancing our technical capabilities to better detect, assess and respond to cyberspace attacks. We are instilling the importance of cybersecurity at all levels of command, and are making great strides to operate, maintain, and defend our network as one enterprise from the core-to-the-edge.

## POLICY

To support an Expeditionary Force, the U.S. Army is fundamentally changing and adapting our institutions, including LandWarNet. On March 2, 2009, General Casey, the Chief of Staff of the U.S. Army, signed a memorandum to transform LandWarNet to deliver a global, standardized, protected, and economical network enterprise.

The U.S. Army is transforming LandWarNet to a new Global Network Enterprise Construct (GNEC). GNEC focuses on four principle objectives: (1) Operationalize LandWarNet, (2) Improve the LandWarNet defense posture, (3) Realize economies and efficiencies, and (4) Ensure Joint interoperability. These objectives will be accomplished through standardizing network operations (NetOps) processes and tools.

The U.S. Army has taken the lead on implementing many new policies to improve our cybersecurity. These policies concentrate on

protecting information, defending systems and networks, providing IA situational awareness, fostering innovation, and creating an empowered workforce. In Fiscal Year 2008 the U.S. Army led DoD on several strategic fronts to include:

- Developed and implemented an aggressive policy for encryption of Data at Rest (DAR) and Data in Motion, and currently leads DoD in the OMB mandated implementation of a DAR solution to protect sensitive information and mobile devices.
- Delivered the U.S. Army LandWarNet Information Assurance Architecture (LIAA). LIAA ensures a comprehensive LandWarNet IA Architecture that supports the DoD GIG IA Vision.
- Developed and implemented a four-phase IA compliance model and IA self-assessment checklist. This effort increases awareness, standardizes and validates IA compliance activities, and measures leader success in executing the command IA program.
- Influenced the tools selection and acquisition for DoD enterprise-wide network security solutions via our IA Approved Products List policy.
- Improved our Certification and Accreditation posture by mandating all systems be registered in the U.S. Army Portfolio Management System. As a result, the U.S. Army exceeded the Federal Information Security Management Act goal for Authorities to Operate.
- Led the execution and phased implementation of Homeland Security Presidential Directive-12 requirements for the implementation of Cryptographic Common Access Card logon.

- Partnered with OSD in support of the Comprehensive National Cybersecurity Initiative (CNCI) to draft policy to integrate Supply Chain Risk Management (SCRM) both into the procurement of Commercial Off-the-Shelf Software for the LandWarNet (and the GIG) as well as into program protection plans for major weapons systems. The intent is to improve the integrity of components used in DoD Systems, to establish a process to assess vulnerabilities, and gauge future resource requirements to mitigate the impact of supply chain risk.
- Developed a pilot process for SCRM with OSD, the other military components, and the Defense Intelligence Agency to: (1) develop a SCRM process which is scalable and relevant to meet the needs of DoD; (2) provide an initial assessment of the risk to DoD; and (3) gauge the resource and legal changes needed for a full-fledged SCRM process. The ultimate objective is to incorporate SCRM into the U.S. Army GNEC.
- Worked with the industrial base to protect the technologies used to build our future networks and other major weapons systems. In January 2008 we established the U.S. Army Defense Industrial Base Cyber Security Office (DIBCSO). DIBCSO's objective is to protect the technological superiority of U.S. Army weapons programs by managing the risks associated with the digitalization of information and the globalization of critical manufacturing capabilities. In its day-to-day mission, the DIBCSO drafts and revises U.S. Army policy and acquisition/contract procedures. These efforts maximize the protection of U.S. Army technologies within the contractor base, and are critical to current and future Warfighters.

## MANAGEMENT

The U.S. Army is changing its culture by relooking how we manage our people and the network. We are updating our training curriculum to support the new cyber-skills needed to operate, maintain, and defend our network. We have realigned organizations to streamline the command and control over the network.

Recent network events have highlighted the need for a well-trained workforce capable of operating, maintaining, and defending the network. As a result the U.S. Army is reviewing the development and tracking of its highly skilled workforce, and looking to update the Officer, Warrant Officer, and Enlisted Career Management Fields for conducting cyberspace operations.

The U.S. Army has a robust training program for our individual IA professionals and Cyber-Warriors. One initiative is our Mobile Training Teams that travel to sites around the Army to execute mandatory training, and validate the knowledge and skills of the U.S. Army's IA and Cyber-workforce.

Unit training for cyberspace operations is in its formative stages. To help mature unit training, the U.S. Army conducts cyber-specific exercises such as Bulwark Defender, Unified Quest, Talisman Saber, Austere Challenge, and Global Lightning. These exercises train units to operate, maintain, and defend the network from directed professional attacks, and results in improved procedures for communicating with other Services, agencies, and Combatant Commands (COCOM). These training

exercises also provide a forum to study future joint, interagency, intergovernmental, and multinational operations.

The U.S. Army continues to change how it manages its network. Network Enterprise Technology Command (NETCOM) is now designated as the single authority to operate, maintain, and defend the U.S. Army's generating force network. The U.S. Army has reorganized its forces to support the U.S. Strategic Command (USSTRATCOM), the COCOM for cyberspace operations. In addition, we are achieving unity of effort within the U.S. Army Staff by creating an Army Cyberspace Task Force.

The U.S. Army is currently the only Component in DoD that has its NetOps command, NETCOM, reporting to the Chief Information Officer. NETCOM operates a 24x7 Global Network Operations and Security Center (NOSC) that provides the technical control to each of the Army's Theater NOSCs who support the geographic COCOMs.

When we talk about operating, maintaining, and defending the network, we are really describing Computer Network Operations (CNO). There are three disciplines within CNO: Computer Network Defense (CND), Computer Network Attack (CNA), and Computer Network Exploitation (CNE).

To improve the command and control for CND, the U.S. Army recently realigned the local network providers, known as Directors of Information Management, to NETCOM. NETCOM is also designated the CND Service Provider for the U.S. Army. Significant NETCOM functions and responsibilities include:

- Operate, maintain, and defend LandWarNet and U.S. Army global enterprise services.
- Direct, monitor, and support enterprise management across the LandWarNet.
- Execute technical control and enforce compliance across the LandWarNet.

## TECHNICAL

The U.S. Army is addressing the many technical challenges we face through a number of initiatives to include:

- Selecting and deploying a DAR encryption solution for protecting sensitive data on mobile computing devices and removable media. The U.S. Army was instrumental in developing the technical requirements for the selection and subsequent award of the DOD DAR solution.
- Preventing pilfering of private or sensitive data by combing the Web for "at-risk" data through U.S. Army Web Risk Assessment Cells.
- Implementing the Information Assurance Vulnerability Management process to find, fix, report, and verify compliance with DOD mandates. The U.S. Army is using DOD automated scanning and remediation tools, innovative reporting capabilities, and increased compliance verification inspections.
- Securing two-way wireless devices and extending physical security measures to the DOD Smart Card technology. The U.S. Army has partnered with the National Security Agency (NSA) in developing the GIG IA Architecture.

- Deploying mobile wireless solutions which leverage NSA encryption devices such as SecNet 11 and SecNet 54. These devices reach back to the Warfighter Information Network-Tactical (WIN-T) in order connect back to the GIG. The U.S. Army is also deploying a Joint Tactical Radio System (JTRS) to provide secure voice and data capability at the Secret level to the Warfighter. For the future, the U.S. Army is evaluating the Secure Mobile Environment Portable Electronic Device (SME-PED) under contract with NSA. This device will deliver to the Warfighter secure voice communications at the Top Secret level and classified e-mail at the Secret level.

The U.S. Army expects that the Administration's budget request for Fiscal Year 2010 will fully support our cyberspace activities and include the resources necessary to effectively address our policy, management, and technical challenges. We are also confident that with your support, our GNEC strategy and initiatives will enhance mission assurance in Cyberspace as a Warfighting Domain.

In conclusion, the U.S. Army is taking and has taken action to mitigate the never ending cyberspace threats, and continue to improve our mission assurance in cyberspace. Using GNEC, the U.S. Army is addressing the challenge of changing the culture to view the network as a critical enabler for the Warfighter. The U.S. Army's commitment to transforming LandWarNet to an Army Enterprise will improve our network security posture as we aggressively work towards ensuring commanders have the ability to see, control, defend, and fight the network as one enterprise from the core-to-the-edge. By establishing a single focal point

for all cyberspace operations issues under the Army Cyberspace Task Force, we will provide the unity of command and effort needed to meet many of the cybersecurity issues the U.S. Army is facing today and will face in the future.

I would like to thank the subcommittee for affording me the opportunity to share the U.S. Army's activities to operate and enhance mission assurance in Cyberspace as a Warfighting Domain. Thank you.