RECORD VERSION

STATEMENT BY

LIEUTENANT GENERAL ROBERT S. FERRELL
CHIEF INFORMATION OFFICER/G-6,
UNITED STATES ARMY

BEFORE THE

HOUSE ARMED SERVICES COMMITTEE
SUBCOMMITTEE ON INTELLIGENCE, EMERGING THREATS
AND CAPABILITIES

FIRST SESSION, 114TH CONGRESS

INFORMATION TECHNOLOGY INVESTMENTS AND PROGRAMS: SUPPORTING CURRENT OPERATIONS AND PLANNING FOR THE FUTURE

FEBRUARY 25, 2015

NOT FOR PUBLICATION UNTIL RELEASED BY THE
COMMITTEE ON ARMED SERVICES

STATEMENT BY

LIEUTENANT GENERAL ROBERT S. FERRELL

CHIEF INFORMATION OFFICER/G-6, UNITED STATES ARMY

Chairman Wilson, Ranking Member Langevin and other distinguished members of the committee –

Thank you for inviting me to speak to you today about the Army network and information technology. Much has changed since an Army CIO last testified in 2009 and I appreciate the opportunity to give the subcommittee an update.

Information technology and the network are at the heart of everything the Army does. Whether it's day-to-day business operations, such as paying service men and women, taking care of Families and running our installations; or training our Soldiers so that they are fully prepared and ready for anything we may ask of them; or executing the missions assigned by the president and our combatant commanders, to include combat, humanitarian, stability and support, and partner-building operations, the Army relies on the network and our IT systems to get it done. As we draw down end strength, we expect the role of the network to grow, particularly from an operational perspective. To remain effective on the battlefield and reduce the requirement for forward-deployed Soldiers, the Army will need more rigorous and realistic training, even better situational awareness and understanding, more effective mission command, a smaller logistical footprint and greater lethality. The network is key to achieving all of those objectives.

With that in mind, the Chief Information Officer/G-6 team this month completed and published the Army Network Campaign Plan. This plan, along with the accompanying implementation guidance for the near and mid terms, sets the path to providing the Army the network capability it will need to remain the world's preeminent land force. It was designed to support all aspects of the Army's new operating concept: provide a foundation for joint operations; deploy and transition rapidly; develop the situation in close contact; maneuver from multiple locations and domains; operate while dispersed yet maintain mutual support; integrate with our action partners; and present multiple dilemmas to the enemy. With sustained investment, we believe the Army will achieve the envisioned secure, integrated, global network by the end of fiscal year 2021.

It's important to first lay out the overall environment we expect to face. Taking our current global posture as a benchmark, we believe the Army will remain in high demand. As the chief of staff, Gen. Odierno, testified in January, the Army is fully engaged, with nearly 140,000 Soldiers and nine of our 10 division headquarters committed, deployed or forward-stationed in nearly 140 countries on six continents. Given the tumult in the Mideast, Southwest Asia, Africa and Europe, it is unlikely this operational tempo will decrease in the near future. Our adversaries are becoming more sophisticated and their access to cutting-edge technology, especially information technology, is getting easier. At the same time, that technology is evolving at a rate that outpaces our acquisition processes, making it difficult to keep our Soldiers equipped with the best available systems and capabilities. Additionally, the threat to DoD networks continues to intensify; the department is the target of millions of cyber intrusion attempts every day. As I'm sure you are aware, the

consequences of a successful attack could be quite severe. The backdrop to these conditions is a national fiscal picture that indicates lower budgets for the Army and DoD.

For the Army to achieve success in this environment and fulfill the training, operational and business requirements I described earlier, the network must have a very specific set of characteristics: worldwide reach, whether at home station, en route, upon early entry or in a mature theater of operations; guaranteed availability, regardless of the number of users or the location, to include the most austere operational conditions; and a level of security that protects the integrity of the network itself and the data it carries. The bottom line objective is to provide all authorized personnel access to the information, services and capabilities they need, anytime, anywhere.

To achieve this network, the Army Network Campaign Plan establishes five lines of effort (LOEs), or priorities. The first is to provide Signal capabilities to the entire force. This LOE will synchronize delivery of network capacity, security, services, training and doctrine. LOE 1 also will develop a Signal equipping strategy to deliver intuitive, secure, standards-based capabilities that are adaptive to the commander's requirements and integrated into the Common Operating Environment.

LOE 2 focuses on enhancing cybersecurity capabilities by optimizing defensive cyberspace operations and DoD Information Network operations. This LOE will improve the network defense posture by minimizing the attack surface, establishing physical path diversity at critical installations, strengthening data defenses and enhancing security

through cyber hygiene and best practices. The Army intends to transform cyberspace defensive operations by deploying capabilities that support cyberspace defense. We also will enhance cyberspace situational awareness by improving the cyber-sensing infrastructure, harnessing the power of Big Data analytics and expanding information sharing.

LOE 3 centers on increasing network throughput and ensuring sufficient computing infrastructure. This LOE will generate the "always on, always available," end-to-end transport infrastructure necessary to meet growing and evolving capacity demands. It also will shepherd the transition from disparate data processing and storage solutions to an optimized and responsive global computing and storage infrastructure. Additionally, this LOE will implement a standardized suite of centrally managed end-user devices to improve functionality and to enable a common user experience.

LOE 4 focuses on delivering a universal suite of IT services, to include voice, video, data retrieval and sharing, and collaboration, from the enterprise to the end user. Modernized enterprise services such as these will provide the Soldier and business user the ability to work in diverse environments without needing to learn how to use these new services after each relocation to a new geographic location or organization. Additionally, common collaborative services will help enable live, virtual and constructive training, split-based operations and global collaboration among regionally aligned forces.

LOE 5 will concentrate on strengthening network operations. This includes establishing an information exchange specification

framework and simplifying the design, assembly, transport and stand-up of mission-scaled networks. This LOE will set the requisites to enhance spectrum monitoring, assignment and de-confliction. It also will facilitate central oversight of network assets and mission readiness, creating full network situational awareness; and improve incident response and cybersecurity management services for the operating force.

The Army Network Campaign Plan near-term implementation guidance details activities planned for fiscal years 2015 and 2016. The mid-term guidance focuses on network capabilities for FY 2017-21. Together, these documents provide the blueprint for synchronizing Army network requirements with our planning and programming. Today, I would like to highlight a few of our most important efforts, some of which were under way before the campaign plan was developed but all of which feed the ultimate objective of a unified, agile, robust and secure network that fulfills the needs of our Soldiers and their leaders.

Building the Joint Information Environment (JIE)

DoD is in the process of realigning, restructuring and modernizing how the department's IT networks and systems are constructed, operated and defended. The concept is called the Joint Information Environment and it improves in many ways from previous network constructs. Its foundation is an open architecture, defined standards and specifications, shared IT infrastructure, and common ways of operating and defending all DoD networks.

Common services are provided at the enterprise level, to include Identity Access Management (IdAM) and mission-unique capabilities supplied by the components. The end result will be a functionally optimized, secure, interoperable and resilient environment.

Army network modernization efforts are the most visible and advanced component of DoD's JIE initiative. For example, the DoD CIO has designated the Army's Joint Regional Security Stack (JRSS) architecture as the department's enterprise solution for network security. JRSS performs firewall functions, intrusion detection and prevention, enterprise management, and virtual routing and forwarding. The stacks have path diversity and eliminate critical failure points, which will help assure timely delivery of crucial information to warfighters around the globe. Pairing Multi-Protocol Label Switching (MPLS), a virtual traffic management system, with the stacks will make data move faster and improve command and control, thereby significantly reducing the chances of information being stalled or lost due to high volume and congestion. In addition, by moving each Service from its own security architecture to JRSS, DoD is substantially shrinking the attack surface and reducing its IT infrastructure inventory.

The Army is teaming with the Air Force and the Defense Information Systems Agency (DISA) to execute the migration to JRSS. Currently, JRSS implementation is ongoing at more than a dozen sites in the continental United States and overseas. Migration of operational traffic to JRSS has begun in Joint Base San Antonio and will continue

throughout the southwest and southeast regions of the continental United States. Overseas, the Department will add an additional JRSS installation and begin migration of operational traffic in Europe. In Southwest Asia, we will complete three sites over the next three quarters. Overall, we expect to have 24 sites worldwide that will process both unclassified traffic and 25 sites for classified traffic. This reduces the surface attack area from over 1,000 separate security access points to less than 50, dramatically improving the cybersecurity posture of the network.

The Joint Information Environment will rely heavily on cloud computing. In partnership with DoD, DISA, the National Security Agency and the other Services, the Army helped shape development of DoD's initial cloud security architecture. Moving to cloud-based solutions will enable the Army to better focus limited resources on meeting evolving mission needs. Over time, this will significantly boost IT operational efficiency, improve mission effectiveness and position the Army to more quickly adopt innovative and emerging capabilities. The Army currently is implementing the necessary modernization plans and crafting processes and procedures to leverage commercial cloud service providers approved by DoD and the Federal Risk and Authorization Management Program (FedRAMP). We are on track to formally release our cloud computing strategy in March 2015. We'll follow that strategy with a cloud computing policy to guide how and where we host our enterprise resource planning and other mission-critical systems, which will be restricted to DoD-owned facilities.

Unified Capabilities (UC) are another element of the Army's implementation of JIE. UC will provide real-time communications, to include voice, video and data, from the enterprise level in partnership with DISA. By centralizing the provision of these services and integrating them through a joint construct, users will get more capability more quickly – all the way down to the tactical edge. Additionally, UC will greatly enhance our voice, video and data security. Currently, not all of our communication media leverage DoD Public Key Infrastructure (PKI) to ensure confidentiality, integrity and availability. In contrast, UC will be fully integrated with DoD PKI. The Army and DoD also expect UC to reduce costs, as the Department will be able to take advantage of its enterprise buying power and to divest expensive legacy infrastructure.

The Army is working to converge the disparate Reserve, National Guard and Corps of Engineer networks into the larger Army network to leverage common infrastructure and gain efficiencies. This supports JIE's realignment and restructuring objectives in that it collapses separate networks into a single standards-based network in order to achieve improved security, situational awareness and operational flexibility.

While originally begun to fulfill Presidential and Office of Management and Budget mandates to reduce the federal IT infrastructure inventory, data center consolidation also supports the Army's move to the Joint Information Environment. By decreasing the number of Army-owned data centers and moving as much data and as many applications as practicable into joint Core Data Centers, we are greatly improving the availability of key information to all mission

partners. Fewer data centers also means less risk of compromise to DoD and Army information and networks. Additionally, once the process is complete, the Army should reap substantial cost savings. The DoD CIO has directed that the Services close 60 percent of their data centers by FY18. As of the beginning of February, the Army had closed 305 data centers, which is 40 percent of our goal. I would like to note that budget constraints would adversely affect the Army's ability to achieve full compliance with this presidential initiative to cut operating costs and improve security and infrastructure efficiencies.

To take advantage of everything the JIE offers, the Army is expanding its infrastructure capacity – that is, the amount of traffic our network "pipes" can handle. By the end of FY16, the Army network backbone, which connects installations to the DoD Information Network, will be increased to 10 gigabits per second (gbps) with the capacity to increase to 100 gbps in the future.

Everything the Army is doing at the enterprise level and to construct the JIE feeds directly into preparing and enabling our tactical forces. Perhaps most importantly, these efforts will bring expeditionary mission command to fruition, which in turn will make the Army more expeditionary and more effective on the battlefield. The basic concept of expeditionary mission command is to give commanders the ability to continuously inform and influence their forces through all operational phases, to include while at home station, during training center rotations, while en route to a real-world mission and once they hit the ground. They also will be able to leverage intelligence processing, exploitation and dissemination services.

Enabling Expeditionary Mission Command

The Army network enables expeditionary mission command. Corps and divisions will use their home station mission command center to effectively execute mission command from home station for a broad array of missions.

En route mission command capabilities provide uninterrupted mission planning, synchronization and situational awareness while in transit to the operational theater. Our units will maintain situational understanding and, with that real-time knowledge, conduct adaptive planning while still in the air. The Army is leveraging combat-proven technologies developed by the Special Operations community and the Warfighter Information Network – Tactical program to provide this critical capability to the Global Response Force.

Transportable Tactical Command Communications (T2C2) will provide small teams and company-sized units a robust voice and data capability immediately upon arrival. The T2C2 solution will come in two mobile, modular, and scalable variants, one to support initial-entry teams and a second to support early-entry command posts.

Greater integration between the enterprise and tactical networks will help reduce gaps in connectivity during different stages of operations and enable the use of expeditionary mission command supported by reach-back to strategic assets and information.

Protecting and Defending the Network

An agile, global network won't be of much use to the Army, however, if it and the information it carries are not secure and trusted. Protecting the network and information plays into every choice we make about architecture, capability and use. That said, I would like to highlight a few of our most important security-related endeavors.

The Army is aggressively transitioning to the new DoD certification and accreditation process, known as the Risk Management Framework (RMF). The RMF uses the security controls identified in the Committee on National Security Systems baseline and follows the processes outlined by DoD and the National Institute of Standards and Technology. Importantly, the RMF makes DoD requirements and processes consistent with the rest of the federal government's, enabling reciprocity. It also expands certification and accreditation beyond information systems to cover all information technology, including applications and industrial control systems. The RMF enables continuous system monitoring, as well, which will give us our security posture in real time.

The Army is actively pursuing ways to track and counter the insider threat as part of improving our defense posture. The federal government mandated implementation of network auditing and monitoring capabilities to deter, detect and prevent malicious insider activity on classified networks. The Services and agencies also were directed to establish a centralized analysis, reporting and response capability (i.e., analytics hub) to analyze the collected information. The Army Protection Program supports development of the technical requirements, deployment plan and

funding strategy for such a capability to cover all generating and tactical force networks. Our blueprint will facilitate the sharing of counterintelligence, information assurance, law enforcement, human resource, security and other related information.

Additionally, the Army is leveraging DoD's Host-Based Security System Device Control Module to restrict system access to peripheral and other removable storage devices and media, such as USB drives, MP3 players and CDs/DVDs. We also are using the DoD Insider Threat Detection Service, which utilizes the classified network-based Cyber Situational Awareness Analytic Cloud to detect potential malicious behavior, such as log tampering, data exfiltration and external web server attacks.

While automated tools are critical to better network security, they do not obviate the need for a first-class military and civilian cyber workforce. The Army is standing up a robust Cyber Mission Force that eventually will be composed of 41 teams and more than 1,800 military cyber personnel. The teams fall into five categories: national mission, combat mission, national support, combat support and cyber protection. As of the end of January, 24 teams had reached initial operating capability. We expect all 41 to be at full or initial operating capability by the end of FY16.

On the civilian side, the Army must bring the cyber workforce to a level of maturity that matches the recently established military Career Field 17 (CF17). That means developing a training pipeline; shaping the Army's talent management strategy to meet the increasing demand for a

credentialed civilian cyberspace workforce; and promoting Army efforts to unify and cohesively manage the civilian cyberspace workforce across the entire DoD. Potential models for civilian cyber talent management include: position identifiers similar to the acquisition workforce management process; a new Cyber Career Path that draws in cross-disciplinary occupational series from other career programs; and/or a new Office of Personnel Management cyber designation that would offer incentive pay and equity across agencies.

The CIO/G-6 is supporting an overall effort to build the Army's civilian cyber cadre. Last month, we initiated two planning teams. Among their tasks is defining work roles and competency/training requirements for the civilian workforce; and identifying the composition and scope of cyber-related positions, to include nine series residing in seven Army Civilian Career Programs (Information Technology, Telecommunications, Electronics Engineer, Computer Engineer, Computer Scientist, Intelligence Operations, Security, Criminal Investigation and Operations Research). Two more planning teams will start work in the June 2015 timeframe. One will focus on building a common framework among the seven Career Programs to manage the human resources life cycle of civilian cyber workforce. The other will integrate Army efforts into a federal framework and seek formal recognition of the civilian cyber workforce from the Office of the Secretary of Defense and the Office of Personnel Management to address occupational series, special pay, hiring flexibilities, and incentives.

FY16 Budget Request

The Army's FY16 IT budget request totals $9.1 billion and emphasizes the initiatives and programs just described critical improvements to cyberspace operations, cyber mission forces, core mission services, IT infrastructure, training and readiness. The request focuses on thorough modernization of the institutional network infrastructure so that we can take full advantage of warfighter and business technology advances. Partnering with DISA and our sister Services, with the requested funding in FY16, we will be able to make substantial progress in the transition from our disjointed legacy systems to a unified, more secure and capable network. Army users and our mission partners will reap tangible benefits as bandwidth expands, security is strengthened and enterprise services and applications come online. Additionally, FY16 network infrastructure upgrades will ensure that the Army is positioned to support cloud-based enterprise business systems and the adoption of Unified Capabilities.

The Army has achieved significant cost savings and cost avoidance as a result of information technology management reforms in FY15 and leveraging Better Buying Power 3.0. Efficiencies identified are a result of deliberate reforms of IT governance structures: offering of flexible IT government contracts, consolidated purchases (bulk buys), issuance of standards, and maximizing the use of enterprise license agreements to achieve a single-interoperable secure network for deployment of information technology to modernize the network.

I know sequestration remains a topic of interest and the committee has asked about the impact of funding cuts. As General Odierno testified in January, under sequestration the Army would have to reduce spending

on network services and information insurance by almost $400 million in FY16. This would impact the Army's ability to sustain baseline network operations, which could, in turn, affect training, readiness and daily business activities. It also could impact our ability to maintain network security, which could create cyber vulnerabilities.

In closing, I would like to thank the committee for their support and the opportunity to appear today and discuss the importance of the Army network and information technology efforts. Information technology and the network are critical to the Army. Congressional support to our modernization efforts will ensure we can replace aging infrastructure, improve security through reducing access points and consolidate the Army's multiple networks into a single, seamless network that enables integrated strategic and tactical operations. It is imperative we deliver the network at the point of need, with the right bandwidth capacity, services and security to remain the world's preeminent land force.

I look forward to your questions.