RECORD VERSION

STATEMENT BY

LIEUTENANT GENERAL BRUCE T. CRAWFORD
ARMY CHIEF INFORMATION OFFICER/G-6

AND

MAJOR GENERAL JAMES J. MINGUS
U.S. ARMY MISSION COMMAND CENTER OF EXCELLENCE

AND

MR. GARY P. MARTIN
U.S. ARMY PROGRAM EXECUTIVE OFFICER,
COMMAND, CONTROL, AND COMMUNICATIONS-TACTICAL

BEFORE THE

SUBCOMMITTEE ON TACTICAL AIR AND LAND FORCES
COMMITTEE ON THE ARMED SERVICES
UNITED STATES HOUSE OF REPRESENTATIVES

ON

THE UNITED STATES ARMY NETWORK MODERNIZATION STRATEGY

FIRST SESSION, 115TH CONGRESS
SEPTEMBER 27, 2017

NOT FOR PUBLICATION UNTIL RELEASED BY THE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

Introduction

Chairman Turner, Ranking Member Tsongas, and distinguished members of the House Subcommittee on Tactical Air and Land Forces, thank you for your continued support for our Soldiers, Army Civilians, Families, and Veterans. It is an honor to address this subcommittee. On behalf of our Acting Secretary of the Army, the Honorable Ryan McCarthy, and our Chief of Staff, General Mark Milley, we thank you for the opportunity to provide an update on the new modernization path forward for the Army's Mission Command Tactical Network.

Our current Network does not meet our Warfighting needs now or in the projected future. To protect the homeland, foster security abroad, and win in current and future conflicts, Army forces must be able to fight, shoot, move, communicate, protect, and sustain. All of these capabilities require the ability to reliably communicate anywhere, anytime, across all domains and in any environment. The Army is committed to delivering a survivable, secure, mobile, and expeditionary network capable of providing situational awareness and joint interoperability to enable warfighters to fight and win against adversaries in all domains.

To get to a new modernization path forward, we must first understand the current network challenges and how we got here, along with the readiness challenges and the risk we face due to emerging threats. Based on these challenges and risks to the solider and the findings and recommendations from internal and external assessments, the Army plans to embark on a new network modernization path forward.

Current Network Challenges

The Army's current network was conceived, developed and fielded for the static environments of Iraq and Afghanistan but it does not meet the future warfighting needs of a high-end conflict. The network evolved over the past 16 years to address numerous challenges, including a common operating picture that could not be shared among all formations at echelon, data storage and transport challenges, warfighting systems that lacked the ability to work together, the absence of Coalition and Joint interoperability, and limited friendly force situational awareness tools. Since that time, industry has stepped forward to assist the Army and address these areas. Thanks to resourcing

provided by Congress, the Army was able to acquire technology to meet the mission requirements of the early 2000s in a static environment. This resulted in the network that we have today. Fortunately, our soldiers were operating in an environment where they were relatively uncontested in spectrum, cyber and space. Unfortunately, our current network is too complex, fragile, not sufficiently mobile nor expeditionary, and one that will not survive against current and future peer threats, or in contested environments. We find ourselves in a position now, within a new environment and facing new challenges, where our network is not user-friendly, intuitive, or flexible enough to support our mission in the most effective manner and demands a heavy reliance on industry field service representatives to operate and sustain these systems.

In addition to the emerging threats, we have also seen a commercial innovation explosion that accelerated at a rate with which our standard acquisition process could not keep pace. Future adversaries are not inhibited by the same processes, allowing them to better exploit new technology to their advantage.

Readiness Challenges

Based on the emerging threat and the explosion of technology, we are seeing a change in warfare of the future. As our 39th Chief of Staff of the Army, Gen. Mark Milley shared in his posture hearing in May, "the character of war does change on occasion. And one of the drivers – not the only driver – is technology." In other forums, he has elaborated that "we have new insights into the character of future conflict, and we have had glimpses of what our Army and its Soldier must be ready to do in the coming decade." Shifts in the character of war offer an opportunity: if we can anticipate or at least recognize them, we can adapt proactively, maintaining or regaining overmatch and forcing competitors to react to us.

Acting Secretary of the Army McCarthy, and Gen. Milley have also made it crystal clear across the Army that readiness is our number one priority. We must win the fight we are in, be ready to "fight tonight" against any adversary and posture the Army for the future fight. The network is a critical enabler for our Army to generate readiness and project forces and power from our posts, camps, bases and stations to the most remote and disadvantaged locations of the world.

Network Assessments

In the rapidly changing world of information technology, it is a best business practice to continuously assess technology and processes. To remain relevant and improve our ability to counter evolving threats we must review and adapt. Over the past year, the Chief of Staff of the Army led an assessment of the Army's network and modernization plans. These network assessments involved all four network mission areas – the Enterprise Information Environment Mission Area, Intelligence Mission Area, Business Mission Area and the focus of today's testimony, which is the Warfighting Mission Area.

The Army conducted this internal assessment in parallel with the study directed by Congress in the FY 2016 National Defense Authorization Act on the Army's tactical network, which was carried out by the Institute for Defense Analyses (IDA). The findings of the internal Army assessment were corroborated by the IDA study as well as feedback from Department of Defense testing agencies, combat training center rotations, joint exercises, and feedback from operational commanders. The internal and external assessments have revealed high risk challenges that we feel must be mitigated to enable our Army to "fight tonight" against peer adversaries. These findings documented significant challenges across four broad areas of network governance, requirements, acquisition, and innovation, which continue to negatively affect the Army's ability to provide its Warfighters with simple, intuitive, resilient and protected network-enabled capabilities.

Specifically, in the area of governance, the assessments revealed that the lack of a single Army network integrator has resulted in multiple "stove-piped" mission command systems and networks, with multiple, duplicative, and non-integrated information technology programs. This has yielded inadequate integration across the four mission areas, as well as poorly conceived network architectures, resulting in inefficiency and ineffective integration of readiness priorities.

These assessments also found that current requirement processes are not completely synchronized and integrated to ensure capabilities delivered adequately meet the operational needs of our warfighters. The studies found that the Army has

multiple methods for requirements development across the network mission areas, and lacked a central requirements clearinghouse to review and approve all submitted requirements. This resulted in unnecessary duplicative efforts. In addition, they identified our self-limiting, over-prescriptive requirements that reduced our ability to maximize use of available spectrum. The assessments noted an emphasis on technical specifications, rather than clearly defined operational requirements leading to disconnects between the acquisition community and the operational force.

Our current acquisition process does not allow the Army to rapidly acquire and integrate emerging capabilities, allowing the warfighter to keep pace with technology and stay ahead of the evolving threat. The current acquisition processes' traditional emphasis on a legacy program of record approach for developing, testing, and procuring mission command systems and applications has limited our ability to anticipate and rapidly integrate Joint and industry solutions through non-traditional acquisition models. This prevented the Army from effectively leveraging the exponential growth of investments by commercial industry partners over the past decade and capitalizing on the robust Research, Development, Testing and Evaluation (RDT&E) capabilities of our Joint partners. Additionally, the extensive developmental and operational testing required for programs of record has prolonged development and delayed delivery of network-enabled capabilities. The IDA study recommended a shift to a more flexible and agile acquisition process for information technology.

Finally, in the area of innovation, the assessments found that the Army is not capitalizing on industry best practices and must increase integration between developers and operators. This lack of direct engagement with the actual users of the network-enabled capabilities has reduced the Army's ability to assess and provide immediate feedback to the acquisition community in order to influence the development of improved solutions to network challenges.

The recent internal and external assessments has helped the Army better see ourselves and the conclusions we've come to are that the status quo is unacceptable. Our network has not sufficiently evolved over the past 16 years while we fought counter-terrorism and counter-insurgency wars in Afghanistan and Iraq. Therefore, the Army must adapt and change its mission command tactical network path forward to enable it

to fight and win the current fight while pivoting to a new modernization path that better postures our soldiers to be successful in the future fight.

Army Network Priorities

As the Army has looked at developing its new network path forward, we have focused on four priorities: command posts, tactical network transport, mission command systems, and interoperability. For command posts, the new path will seek to improve survivability and mobility. For tactical network transport, the Army will take steps to integrate multiple network transmission paths into a unified transport layer to increase survivability against evolving electronic warfare threats. For mission command systems, the Army will take steps aimed at delivering a common operating environment through a unified mission command suite of systems and applications. Finally, to improve our joint interoperability, the Army will integrate proven and available solutions starting in Fiscal Year 2018 being used today by some of our mission partners.

New Mission Command Tactical Network Path Forward

In assessing what is needed, the Army developed a set of first principles, characteristics, requirements and attributes that describe the objective network needed to enable the current fight while positioning for the future fight. To meet our needs, the Army extensively reviewed several potential courses of action to maximize operational results as quickly as possible and best align resources. These options ranged from maintaining the status quo to accelerating legacy capabilities to reinvesting to address the current threats.

After comprehensive senior Army leadership consideration and review of potential alternatives, the Army's new network modernization path forward will be to halt programs that do not remedy operational shortfalls identified by internal and external assessments, fix those programs required to "fight tonight" and then pivot to a new acquisition strategy of "adapt and buy" that allows for rapid insertion of new technologies. This requires us to leverage industry best practices by creating and enforcing a standards-based open architecture that is both coherent and flexible enough to define standards while not limiting possibilities for insertion of new technologies; and

alignment to new governance, acquisition reform, testing reciprocity, innovation venues, and initial 'adopt and buy' capabilities. This approach enables the Army to leverage resources and maximize network survivability, effectiveness and suitability. It also best supports what we consider to be the most pressing aspects of this effort, fixing our ability to "fight tonight," halting programs that are not needed, and pivoting to a modernization approach that better leverages available technologies and capabilities, while remaining good stewards of tax payer dollars. This path forward involves changes to Army structure and processes to address its shortfalls in governance, requirements, acquisition, and ability to leverage the innovation of the commercial sector.

In FY18, the Army will immediately halt procurement of the Mid-Tier Network Vehicular Radio (MNVR) and legacy Command Post of the Future (CPOF). The Army will also halt procurement of Warfighter Information Network-Tactical (WIN-T) Increment 2 at the end of FY18; however, there are purposed capabilities and elements of the overall WIN-T program that can be used and will be fielded to some of our formations through FY21. This approach allows the Army to reinvest $544.9M. This is not a request for "new money" but a realignment of existing resources. The Army will plan to apply $413.8M to fix the network's most pressing interoperability and security concerns, and $131.1M to "adapt and buy" better systems. The Army will reinvest the savings from WIN-T Increment 2, MNVR, and CPOF to fix the network by improving survivability to electronic warfare, cyber capabilities and the mobility of command posts. Furthermore, these savings will aim to improve Joint/coalition interoperability, simplify the network, and resolve incompatibilities in Mission Command systems between echelons in our warfighting formations.

The acquisition program office will fix programs required to "fight tonight" against a peer adversary and fix those programs that will be part of the Army's future vision. As part of our "adapt and buy" approach, the Army will leverage a modernization-in-service funding concept that provides increased flexibility to leverage available technology while fixing, upgrading and augmenting existing capabilities. The Army will maximize available Commercial-off-the-Shelf (COTS) and available solutions to improve the survivability and mobility of command posts. Use of existing joint COTS solutions will allow us to address some our most pressing joint interoperability issues. Additionally,

we will incorporate solutions to increase survivability against electronic warfare and cyber threats. In FY18, we will upgrade our Mission Command systems to deliver a common operating picture into a unified application suite. The Army will also deliver coalition and Joint radio gateways with access to tactical data links aimed at integrating air-to-ground communications to improve Joint and Army interoperability and close air support.

The Army's pivot to an "adapt and buy" acquisition approach will enable us to deliver a "future state" network to counter the high-end threats and to keep pace with technology. This new approach will help us leverage proven Joint, Special Operations Forces (SOF), and industry solutions that are readily available. It is important that we partner with Congress and industry and encourage experimentation and demonstration. The Army's intent is to develop programs only when necessary and to use innovation and rapid prototyping with operational units to speed up the procurement cycle and keep pace with technology.

To mitigate oversight-related risk identified in the IDA study, the Army will provide clear governance and unity of command by establishing a senior review group, the Information Technology Oversight Council (ITOC), co-chaired by the Under Secretary of the Army and the Vice Chief of Staff of the Army. This council will integrate activities and assessments across all four network mission areas, provide guidance and direction, prioritize investments, and allocate resources. To improve horizontal integration, the Army is establishing Cross Functional Teams that will support integrated requirements, focused procurement as well as increased leadership for experimentation, demonstrations and evaluations by operational units. Finally, to improve standards and architecture governance, the Army has designated the Army Chief Information Officer (CIO)/G-6, to be the lead integrator for Army IT integration and governance.

Recognizing the importance of establishing a more synchronized and integrated network requirements validation system, all Army mission command and network requirements will now be synchronized and integrated by the Mission Command Center of Excellence (MCCoE), with the Cyber Center of Excellence (CCoE) as a supporting command. To address the issue of network standardization, the Army CIO/G-6 will establish a standards-based network architecture for programs to use as a baseline to

modernize. Mission command systems will now have operational, threat-based requirements, rather than just technical requirements to address this shortfall from the studies. Finally, Army Assistant Chief of Staff for Operations will have the final authority and responsibility for reviewing, prioritizing, aligning and validating requirements with operational needs.

The new network path forward acquisition approach aligns to the priorities laid out in acquisition reform to focus on ensuring the warfighter has the network they need. The future network must be built with real-time feedback from Soldiers on the ground and immediately address jamming, cyber, electronic warfare, power and spectrum consumption, joint and interagency interoperability, and air-to-ground communications shortfalls. In the near term, the Army will focus on a less-complex tactical network, moving complexity to the enterprise, freeing up Soldiers to focus on warfighting tasks rather than integrating information technology. This improves current network capability that includes satellite communications, network mobility and security, tactical radios, mission command applications and Position, Navigation and Timing capacity.

The new path will also improve innovation and the synchronization of acquisition and testing of new systems with the warfighter through greater experimentation and demonstration. Systems will be sent to operational units during development to obtain their assessments and to gain their immediate feedback.

Conclusion

We sincerely appreciate the opportunity to describe for you the Army's new mission command tactical network path forward. We are committed to constantly seeking better ways to fix what we have to enable the current fight and to prepare for the future fight. The Army has taken the first steps towards improving its processes for acquiring its mission command tactical networks. The results of the internal Army assessment of networks, the IDA study, and multiple Army deep dives with the Acting Secretary of the Army and our Chief of Staff to assess current capabilities and gaps have provided the Army with a clear picture of where it is, and where it needs to go. By establishing this new network path forward, the Army is redefining the way it does business.

Rep. Mac Thornberry recently stated, "America faces a wider array of serious threats to our security than at any other time in our history. Maintaining our technological edge is central to our ability to meet those threats and to defend the country. Unfortunately, technological change is outpacing our ability to field cutting edge equipment for our troops." Our network "must enable" mission command and our future network, not encumber it, as well as ensure our leaders and soldiers can outthink and out-decide any future adversary.

Our new governance and requirements initiatives and processes, as well as the focus on a halt, fix, and pivot to "adapt and buy" strategy will align to acquisition reform efforts, make the Army more agile, help us keep pace with technology to counter current and future threats, and provide our soldiers with the best information technology we can to enable them to "fight tonight" and win our Nation's wars.

We must continue to posture the Army to capitalize on technological advances, and to influence, shape, and leverage the innovation of industry. This new path helps us do exactly that.

Mr. Chairman and distinguished Members of the Subcommittee, we sincerely appreciate your commitment and strong support for our brave men and women in uniform, our Army Civilians, and their Families.

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu