United States Government Accountability Office

GAO

Report to Congressional Requesters

January 2013

ARMY NETWORKS

Size and Scope of Modernization Investment Merit Increased Oversight

GAO-13-179

January 2013

GAO Accountability * Integrity * Reliability

Highlights

Highlights of GAO-13-179, a report to congressional requesters

ARMY NETWORKS

Size and Scope of Modernization Investment Merit Increased Oversight

Why GAO Did This Study

For nearly 20 years, the Army has had limited success in developing an information network—sensors, software, and radios—to give soldiers the exact information they need, when they need it, in any environment. Such a network is expected to improve situational awareness and decision making in combat. Under its network modernization strategy, the Army is implementing a new agile process intended to leverage industry technology solutions. The Army estimates that it will require about $3.8 billion in fiscal 2013. As requested, this report addresses the extent to which (1) the Army's network strategy and agile process addresses cost, technology maturity, security, and readiness; and (2) the Army's strategy faces other risks and challenges. To conduct this work, GAO analyzed key documents, observed testing activities, and interviewed acquisition officials.

What GAO Recommends

To help ensure adequate oversight, GAO recommends that the Secretary of Defense (1) define quantifiable outcome-based performance metrics for network equipment; (2) develop a plan for future network evaluations to determine if those measures have been met; and (3) evaluate fielded network performance and make recommendations for adjustments, as necessary. GAO also recommends that the Secretary of Defense consolidate Army tactical network budget elements and justifications into a single area of the Army budget submittal. DOD generally concurred with these recommendations and stated that it has initiated actions to address several of the challenges identified in the report.

View GAO-13-179. For more information, contact Belva M. Martin at (202) 512-4841 or martinb@gao.gov.

What GAO Found

The Army has taken a number of steps to begin executing its network strategy and agile process, including establishing a baseline network architecture for Army communications. The Army's agile process involves seven phases and three decision points to allow officials to quickly evaluate emerging networking technologies to determine if they address capability gaps and can be deployed to the field. However, the network strategy is still evolving and the Army has not yet executed one full cycle of the agile process. The Army's strategy addresses some aspects of cost, technology maturity, security, and readiness, but as implementation is still under way, data for assessing progress are not available at this time. Nevertheless, the Army is beginning to spend billions of dollars netting together dozens of disparate systems to form a network that is intended to enhance warfighter effectiveness and survivability. Specifically, the Army has identified that over $3 billion will be needed each year on an indefinite basis for investments in networking capabilities, potentially making it one of the Army's most costly investments. To help determine that technologies meet prescribed levels of technical maturity, the Army has established a laboratory-based screening process for evaluating technologies, and those that show promise move to evaluations in a realistic environment with soldiers and testers. To help provide security and information assurance, the Army is working with contractors and the National Security Agency to obtain appropriate certifications prior to fielding new networking technologies. Furthermore, the Army is attempting to align the procurement and fielding of networking systems with the relatively fixed schedules for equipping and training units before they are deployed. The challenge will be to ensure that the equipment being sent to the field has been thoroughly demonstrated and that fielding decisions are not made solely to accommodate deployment cycles.

The overall scope and cost of the Army's new network strategy, as well as other factors unique to the strategy, present significant risks and challenges and deserve high-level oversight attention by both the Army and the Department of Defense (DOD). For example, the Army wants to field smaller quantities with greater frequency to be able to take advantage of new and improved capabilities as they become available, thus avoiding long-term procurements of outdated technology and potentially helping to realize savings in development, testing, and maintenance costs. However, the Army is still weighing funding and contracting options that would allow it to accomplish this goal while adhering to established acquisition and budget processes that may require long lead time to acquire these technologies. DOD guidance calls for measuring actual contributions of information technology portfolios, which includes the Army network, against established outcome-based performance measures to determine improved capability and allow for adjustments in the mix of portfolio investments. Senior DOD officials provided extensive input on the soundness of individual network components and the schedule for fielding equipment and have offered that future evaluations in an operational environment present a good opportunity to evaluate the overall performance of the network. However, the Army and DOD have not yet fully defined quantifiable network performance measures or plans to periodically review and evaluate the actual effectiveness of new Army network capabilities. Inadequate oversight of the portfolio could put the investment at risk. Finally, budget justification and other planning materials for network equipment—over 50 research and development and procurement budget elements—are not organized to provide insight into the budget for and affordability of the entire network. Given the magnitude and financial commitment envisioned, a consolidated reporting and budgeting framework could yield more consistency and clarity in the justifications for Army network initiatives and facilitate congressional oversight.

Contents

Figures

Abbreviations

COE	Common Operating Environment
DOD	Department of Defense
DP	Decision Point
IT	Information Technology
JIIM	Joint, Interagency, Intergovernmental, and Multinational
NIE	Network Integration Evaluation
TRL	Technology Readiness Level
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

January 10, 2013

The Honorable Howard P. "Buck" McKeon
House of Representatives

The Honorable Adam Smith
House of Representatives

For nearly two decades, the Army has had various initiatives under way to improve situational awareness and enhance the decision making of soldiers and commanders through the increased use of information technology. While these initiatives resulted in some capability advancements in the Army's network capabilities, they fell far short of their objectives, resulting in what the Army believes is a loosely coordinated set of disparate sensors, applications, and services as opposed to a networked system of weapons and other equipment. The Army is now implementing a new agile process, through which it will seek to leverage industry solutions with less systems development by the Army in modernizing its tactical network to give soldiers the exact information they need, when they need it, in any environment. Under this process, the Army plans to field smaller quantities more frequently, allowing it to procure and field new and improved capabilities as they become available. Army officials believe this would allow the Army to avoid long-term procurements of outdated technology and potentially help realize savings in development, testing, and maintenance costs. Army leadership has identified the network as the service's number one modernization priority and estimates that it will require $3.8 billion in fiscal 2013 funding for its network initiatives.

Because of the network's importance, the ambitious nature of the current network modernization strategy, and the department's track record with system acquisitions over the past decade, you asked us to examine various elements of the new process the Army is using to acquire network capabilities. As agreed with committee staff, we will address issues related to the acquisition process, evaluation of new and current network capabilities, and current plans to purchase radios and other communications equipment in phases. In this first report, we address (1) the extent to which the Army's network modernization strategy and agile process addresses cost, technology maturity, security, and readiness; and (2) other risks and challenges facing implementation of the Army's network strategy and agile process.

To conduct this work, we reviewed the Army's approach to modernizing network equipment and evaluated it against DOD policies and best practices. We observed testing, visited laboratory facilities, interviewed acquisition and test officials, and analyzed key documentation. A detailed description of our scope and methodology is included in appendix I.

We conducted this performance audit from February 2012 to January 2013 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Over the last two decades, the Army began transforming its warfighting capabilities to more effectively counter a broad and complex set of potential threats with smaller, adaptable, more agile and deployable brigade combat teams. The Army wanted the force components—soldiers, platforms, weapons, and sensors—to be "net-centric," that is, closely linked and able to operate seamlessly together. The Army took initial steps toward transformation through its Digitization program in the 1990s by installing computers, software, and interfaces to communications systems on Abrams tanks, Bradley fighting vehicles, and other vehicles in selected units that enable both in-theater and higher commands to share battlefield data with lower-level units.

About 10 years ago, the Army envisioned the Future Combat System as the culminating stage in the Army's ongoing transformation to a lighter, more agile and capable force. Future Combat System was a large and complex development effort to provide a networked family of weapons and other systems for the future force. Ultimately, the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD (AT&L)) issued an acquisition decision memorandum that canceled the Future Combat System development effort. Subsequently, the Army established the Early-Infantry Brigade Combat Team program to demonstrate, among other things, improved network technology and sensors that had been part of the Future Combat System. However, faced with disappointing test results and high costs, DOD directed the Army to cease these developmental efforts, eventually canceling the program in February 2011.

Over the last decade, most network improvements fielded by the Army were focused on supporting operations in Iraq and Afghanistan and were expensive and time consuming. The Army's development and fielding efforts for network technologies were not well synchronized. Funding and timelines for network-related programs were rarely, if ever, aligned. Capabilities were fielded piecemeal and integration with existing technology was largely the responsibility of the user. Current battle command network components were developed to address a range of capabilities and have resulted in what the Army believes is a loosely coordinated set of disparate sensors, applications, services, and transport (i.e., the means of moving information). The decade of conflict also provided the Army with a set of "lessons learned" that have shaped the adoption of the new approach intended to accelerate the introduction of advanced information technology capabilities to the warfighter, especially those engaged at the tactical edge (i.e., the forward battle lines). In December 2011, Army leaders finalized the Network-enabled Mission Command Initial Capabilities Document, which serves as a foundational document in support of Army Network Modernization and describes the essential network capabilities required. We have included a listing of the essential network capabilities in appendix II. These capabilities support an Army mission command capability defined by a coherent network of command posts, aerial and ground platforms, manned and unmanned sensors, and dismounted soldiers that are linked by an integrated suite of mission command systems and connected by a robust transport layer capable of delivering voice, data, imagery, and video to the tactical edge. The Initial Capabilities Document also defined scores of capability gaps that exist with current Army networks. We have included a listing of the highest priority capability gaps in appendix III.

The Army's network modernization strategy focuses on addressing four factors that Army leaders believe are at the root of the Army's network challenges:

- a lack of common technical standards,
- unsynchronized acquisition timelines,
- no visibility at the enterprise (top) level, and
- test and acquisition processes that they believe result in the fielding of outdated technology.

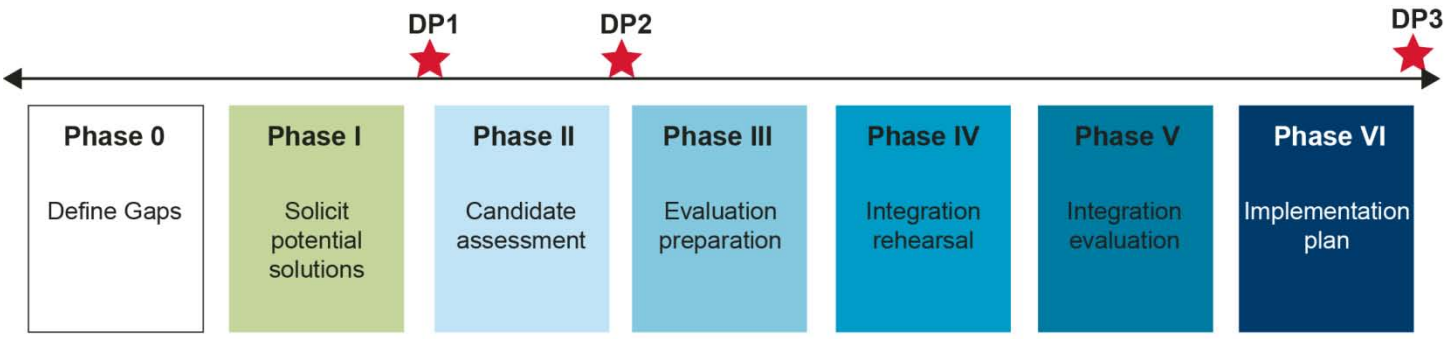
In response, the Army has fundamentally changed the way it develops, evaluates, tests, and delivers networked capability to its operating forces. The Army is shelving its inadequate, disjointed process in favor of an approach it calls capability set management.

Under capability set management, the Army evaluates the current operational environment and then designs a suite of systems and equipment, a "capability set," to answer the projected requirements of a 1-year period. Instead of developing an ultimate capability and buying enough to cover the entire force, the Army plans to buy only what is needed for units preparing to deploy. Every year, the Army will integrate the next capability set, which will reflect any changes or advances in technology realized since the last set was fielded. The Army is using this approach to manage network capabilities as a cohesive portfolio and synchronize all supporting activities. The Army numbers these sets to coincide with its upcoming training and fielding schedule to give units ample time to (1) integrate the new capabilities and (2) train with the systems before deploying to theater. For example, network capabilities being ready for fielding in 2013 are labeled capability set 13.

In support of capability sets, the Army has formulated an agile process that will rely heavily on industry to fill those networking capability gaps using nondevelopmental items or commercial-off-the-shelf options, meaning the Army will do less system development.[1] The Army's agile process involves seven phases and three decision points intended to identify proposed solutions that can be evaluated for feasibility to address an identified need and can be deployed to the field. This approach is also designed to help the Army cull out network system candidates that either may not be an appropriate solution or may not be technically ready for evaluation. Figure 1 illustrates the agile process. The Army believes this process will allow for both large- and small-scale industry involvement that could lead to increased competition and lower costs.

[1]The Army's agile capabilities life cycle process should not be confused with the Agile software development approach for Information Technology (IT) systems. Although they share similar practices, the Army's agile process is being used, at least initially, to identify and evaluate new networking capabilities for brigade combat teams.

Figure 1: The Agile Process



Decision Point 1 (DP 1) Viable candidate list
Decision Point 2 (DP 2) Candidates selected for evaluation
Decision Point 3 (DP 3) Solution implementation decision

Source: U.S. Army.

To implement this agile process, the Army sends out sources sought notices to attract proposed solutions to identified network capability gaps and evaluates each of the proposed solutions at decision points after key phases.[2] The Army initially screens proposals at Phase I to determine which systems will proceed further into the process. The Army screens systems again during a laboratory validation in Phase II. The Army notifies contractors as to whether their systems will be allowed to advance to the evaluation phase, where candidate systems are integrated with existing network capabilities and tested with a full Army brigade. If the system performs well at the evaluation, the Army decides whether or not to buy and field it.

Equipped with every vehicle platform currently in the Army inventory, the 2nd brigade, 1st armored division assigned to Brigade Modernization Command leads phases III to V of the process and is responsible for executing the Network Integration Evaluations (NIE), which are held semi-annually and typically last for approximately 6 weeks.[3] The NIEs are designed to replicate current real-world conditions and include systems

[2]The sources sought notice is a synopsis posted by a government agency seeking possible sources for a project. It is not a solicitation for work or a request for proposal.

[3]NIEs are sequentially numbered—NIE 13.1 and 13.2 are the two events to be held in fiscal year 2013.

already fielded to the operational theater. Soldiers, combat developers, training developers, materiel developers, and engineers participate in each event, providing feedback as the evaluation progresses. NIEs provide a venue for operational testing of formal acquisition programs and for demonstrating government and industry provided systems under evaluation in an operational environment. Army leaders use information from NIEs to inform decisions on what to send to the field. With this large-scale and centralized testing process, the Army intends to validate new technology as it becomes available; select the best candidates for quick insertion into operational units; and refine tactics, techniques, and procedures very quickly to eventually relieve or reduce the integration burden of new equipment on operational forces.

The standard operating procedure for the agile approach states that it is not a substitute for existing DOD acquisition policy. Rather, the agile process applies only to the testing, assessment, and evaluation during NIE events and does not address any subsequent development or procurement actions. Nevertheless, the standard operating procedures state that changes to DOD policy may be considered as the Army develops additional guidance for broader implementation of the agile process. Further, the Army believes this agile process addresses a portion of the information technology reform called for in Section 804 of the Fiscal Year 2010 National Defense Authorization Act, in which Congress directed DOD to formulate a new approach for acquiring information technology systems.[4] In the meantime, the Army expects to comply with procurement aspects of DOD acquisition policy when it decides to buy systems that proceed through the agile process.

Army Moving Ahead but Its Network Strategy Is Still Evolving

The Army has begun a number of initiatives intended to define a desired baseline network, enhance the ability of industry to develop networking systems, and streamline the acquisition of those systems. In particular, the Army is implementing a new overall network strategy and agile process, but details are still evolving. Through these initiatives, the Army has developed preliminary plans to address the areas of cost, technology maturity, security, and readiness. However, the ongoing implementation of the agile process makes it difficult to assess potential effectiveness of the Army's preliminary plans, and additional data to inform such an

[4]Pub. L. No. 111-84.

assessment will likely not be available until after the Army begins fielding new network capabilities. The Army has identified near-term funding needs for network investments and established a process for screening proposed networking capabilities before they are tested. The Army also recognized the need to protect the network and its content and is working with the National Security Agency and vendors to ensure systems are certified for integration into the network. The Army is also attempting to align network capability fielding with its relatively fixed schedule for deploying forces to ensure soldiers are trained with new equipment prior to deployment.

Army Executing Network Strategy and Implementing Agile Process

The Army is beginning to execute its network strategy and implement its agile process. However, the network strategy is still evolving, implementation has only recently started, and the Army has not yet executed one full cycle of the agile process. While the Army indicated that systems evaluated at the NIE in fiscal year 2012 and to be fielded in capability set 13 completed the entire agile process, some of those systems were not evaluated in the laboratory. A full cycle would include going through all phases of the process. The Army is using the agile process to quickly evaluate emerging networking capabilities. At this point, it is unclear what impact some of these actions will have on network modernization. The following examples detail steps the Army has taken to implement the new approach.

- Since 2011, the Army has solicited proposals from both industry sources and existing programs of record to address recognized capability gaps.[5] Industry participation in the agile process generally, and in the NIEs specifically, is critical to the success of the Army network modernization strategy. Under the agile process, the Army has decided to buy only one system from industry after having evaluated more than 100.[6] While the Army anticipates contracting, as appropriate, for solutions to fill capability gaps, industry is making a sizable investment to take part in an NIE, and it remains to be seen if

[5]A program of record is an acquisition effort that has either been recorded as such in the programming and budgeting process or one that has successfully achieved formal program initiation, which typically means it has entered the engineering and manufacturing development phase of the acquisition management process.

[6]In October 2012, the Army issued a request for proposals for a vehicular-mounted, software-defined radio after having evaluated similar systems at prior NIEs.

industry will continue to participate in this strategy over the longer term while purchases to date have been minimal.

- The Army is learning lessons from the use of the agile process. For instance, the Army issued an initial sources sought notice for the second NIE in fiscal year 2012—NIE 12.2. Army officials stated that some of the gaps were too broad, which resulted in too many responses that were not targeted to the specific gap the Army was hoping to fill. Consequently, the Army issued a second, more targeted sources sought notice for NIE 12.2 that resulted in fewer submissions, yet they were better targeted to the specific gaps.

- After the fiscal year 2012 NIEs, the Army established a baseline network architecture, which is essentially the logical and structural design of the Army's network and includes capabilities such as on-the-move communications, battle command, and position location. This baseline architecture incorporates both programs of record and commercial technologies. This architecture provides the foundation upon which the Army will add future networking capabilities. The Army now has an expanded network design that will inform network investment decisions; enable the development of tactics, techniques, and procedures; and serve as the next baseline for future development efforts. Army and DOD planning documents include notional enhancements to the baseline architecture, which implement a number of design considerations that are intended to reduce capability gaps and mitigate risks while enhancing the capability of the brigade combat teams. The Army is utilizing its new agile process to evaluate systems that could fill identified capability gaps, enhance networking, and thus add to the network architecture over time.

- The Army has screened and evaluated government and industry proposals in various ways and recently implemented a laboratory screening process, from which it accepted and subsequently forwarded many candidate solutions for evaluation at an upcoming NIE. The Army has conducted four NIEs to date and is implementing lessons learned from those events to improve future evaluations. For instance, past NIEs included systems that were immature and simply not technically ready for the evaluation. The Army believes that its enhanced screening efforts will identify systems that are not technically ready for the events.

- The Army is already procuring many of the systems planned for its first capability set and additional procurements are pending. Based on testing and evaluations during prior NIEs, the Army determined the

content of capability set 13 and began procuring this equipment this past October. All but one of the capability set 13 systems was developed through a program of record. In many cases, funding had already been identified for these systems. In other cases, the Army had to find additional funding for some equipment through reprogramming. Soldiers at Fort Drum, New York and Fort Polk, Louisiana are receiving capability set 13 equipment and have begun training in preparation for deployment later this year. While a detailed description of capability set 14 systems is not yet available, they will likely include many systems from capability set 13, plus potentially other capabilities tested at recent NIEs.

Army Network Strategy Expected to Be Very Costly Over the Long Term

Because the Army's network modernization effort is a portfolio and not a single acquisition program, the Army has not been required to compile an estimate of the total costs to develop and field its tactical network across the entire Army force structure. However, those costs will be substantial—at an estimated $3 billion annually, this level of effort could total in excess of $60 billion over a 20-year period. For fiscal year 2013, the Army plans to invest about $3.8 billion in its network-enabled mission command portfolio—about $1 billion in research and development and $2.8 billion in procurement (see table 1).

Table 1: Fiscal Year 2013 Requested Funding for Network-Enabled Mission Command

Then-year dollars in millions			
Program	**Research and development**	**Procurement**	**Total**
Warfighter Information Network-Tactical Increment 2	2.8	785.9	**788.7**
Joint Tactical Radio System Manpack Radio		441.5	**441.5**
Warfighter Information Network-Tactical Increment 3	275.2	0	**275.2**
Single Army Logistics Enterprise	120.9	112.7	**233.6**
Brigade Combat Team Equipment Evaluation/NIE	214.3	0	**214.3**
Defense Satellite Communications	5.7	157.2	**162.9**
Joint Battle Command-Platform	20.8	141.4	**162.2**
Nett Warrior	46.8	103.3	**150.1**
Tactical Battle Command	68.3	52.9	**121.2**
Mid-tier Networking Vehicular Radio	12.6	86.2	**98.8**
Warfighter Information Network-Tactical Increment 1		98.3	**98.3**
Joint Tactical Radio System/Airborne, Maritime, Fixed Station Radio		74.0	**74.0**
Tactical Electric Power	13.6	59.5	**73.1**
Joint Tactical Radio System Rifleman Radio		40.7	**40.7**
Others	$175.5	$649.7	**825.2**
Mission Command Total	**956.5**	**2803.3**	**3759.8**

Source: U.S. Army.

Those investments are intended for communications transport, applications, and network services capabilities. Funding for communications transport equipment such as radios and Warfighter Information Network-Tactical makes up a significant portion of network funding.[7]

[7]We are currently assessing the Army's radio and waveform initiatives.

The Army estimates a need for this level of funding to continue indefinitely. In planning documents, the Army assumes that its spending within the mission command portfolio—at least out to the 2030s—will be about $3 billion annually for procurement plus about $0.5 billion to $1.0 billion for research and development.[8] That level of spending would fund the fielding of full capability sets to four brigade combat teams per year and basic network capabilities to other operational forces to ensure interoperability. The Army would continue to roll out capability sets to initially cover all operating forces through the late 2020s and additional upgraded capabilities are expected after that. In 2013, the expected level of funding is greater than that provided to all but one of the nine Army equipment portfolios.

As the Army prepared to buy and field the first network capability set in fiscal year 2013, it did not have funds to complete certain tasks. In June 2012, it requested a total of $139.4 million in reprogrammed funds from other accounts to cover unplanned costs, including vehicle modifications to enable network integration ($59.4 million); procurement of various radios and ancillary equipment ($51.3 million); and procurement of a variety of equipment for tactical operations centers ($28.7 million). Army officials have told us that funding for these costs in fiscal year 2014 and beyond will be accounted for in future Army budgets.

As the Army gets actual cost data on procuring and fielding improved network capabilities, it will be in a better position to estimate future costs.

[8]The mission command portfolio consists of three distinct capability areas: Transport, Applications, and Network Services. The Warfighter Information Network—Tactical and the Joint Tactical Radio Systems are the primary transport programs; Tactical Battle Command, Joint Battle Command—Platform and Global Command Support System—Army are the key application programs; and communications security with key management infrastructure and network management are the key network service programs. According to Army officials, the Army integrates these elements into a coherent network of sensors, soldiers, platforms, and command posts linked by a robust transport network.

Army Laboratory Expected to Validate Technologies in Relevant Environment, but Effectiveness Uncertain

Acquisition best practices and DOD policy both emphasize the need for the use of mature technologies in acquisition programs. Our prior work has found technology readiness levels to be a valuable decision-making tool because they can presage the likely consequences of incorporating a technology at a given level of maturity into a product's development.[9] To date, all the sources sought notices issued as part of the agile process have required proposed network solutions to have achieved technology readiness level 6, which means a high-fidelity prototype demonstrated in a relevant environment, in order to be considered for filling a capability gap. Appendix IV contains a complete listing and description of technology readiness levels. The Army has established a screening process to validate the contractors' assertions regarding technology maturity. Army officials believe this validation process will improve upon multiple critiques of previous NIE activities by soldiers and testers, including the burdensome number of systems being evaluated, perceived military utility of systems, and overall performance of the network architecture.

Army officials have multiple opportunities to reject a proposed capability based on technical maturity and other factors. Interested vendors are instructed to submit a detailed white-paper description of their proposed solutions and those solutions are evaluated on a variety of factors, including technical maturity, compatibility with the Army's network architecture, demonstration in a relevant environment, and ability to meet schedule and provide field support for testing. Successful candidate systems will then proceed to laboratory-based testing to determine, among other things, whether the system is mature enough to be fielded and supported, whether the system performs as intended, and whether it fits into the network architecture. Successful laboratory-based validation results in selected government and industry systems proceeding to the NIE.

NIE 13.1, which the Army conducted in the fall of 2012, was the first NIE for which all systems have been subjected to the entirety of the agile process, including the various laboratory exercises. Army officials believe the rigor they have built into the agile process will filter out many systems that are not quite ready for the NIEs, thus reducing the soldier burden and

[9]Technology readiness levels are measures pioneered by the National Aeronautics and Space Administration and adopted by DOD to determine whether technologies were sufficiently mature to be incorporated into a weapon system.

improving the scores for individual systems and the overall network. However, the real success of this approach can only be determined by NIE results—particularly whether systems perform as advertised, how well they integrate with the network, and the level of military utility determined by soldiers and operational testers. The Army received preliminary results from NIE 13.1 in December 2012.

Army Plans to Address Information Assurance and Security Issues during Network Integration Evaluations

The Army defines information assurance as the protection of systems and information in storage, processing, or transit from unauthorized access or modification; denial of service to unauthorized users; or the provision of service to authorized users. It also includes those measures necessary to detect, document, and counter such threats, as well as measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

The Army collaborates with the National Security Agency to ensure that information assurance issues are addressed early in the NIE process. Vendors understand that they need to secure certification from the National Security Agency, and the Army has a customer service advocate to help in this regard. To implement the certification process, vendors complete a product summary questionnaire, detailed proposal, and security evaluation, which eventually lead to a security certification from the National Security Agency. Vendors must also get certification from DOD for communications-security-related equipment.[10] For over-the-air transmissions of communications-security-related items, the NIE requires the National Security Agency to issue an over-the-air or interim-approval-to-operate that sets the parameters of how and where the testing can be performed on the system. After the NIE, programs of record will work with the National Security Agency to make sure any devices that have not completed National Security Agency certification complete the tasks before systems are fielded.

One of the specific objectives for NIE 12.2 was to assess and evaluate network vulnerabilities. According to Director, Operational Test and

[10]DOD requires “information systems” to receive DOD Information Assurance Certification and Accreditation Process certification with a Designated Accrediting Authority signature accepting risks, if any.

Evaluation officials, the Army continues to improve threat operations during NIEs. NIE 12.2 was the first NIE in which threat information operations—for example, when a mock opposition force uses electronic warfare tactics such as jamming and network intrusion to try and disrupt Army network operations—were fully integrated into the threat commander's allowable tactics. Director, Operational Test and Evaluation officials also noted that an aggressive, adaptive threat that is intent on winning the battle is an essential component of good operational testing and that the Army should continue to ensure that future NIEs contain a robust threat force to include threat information warfare capabilities.

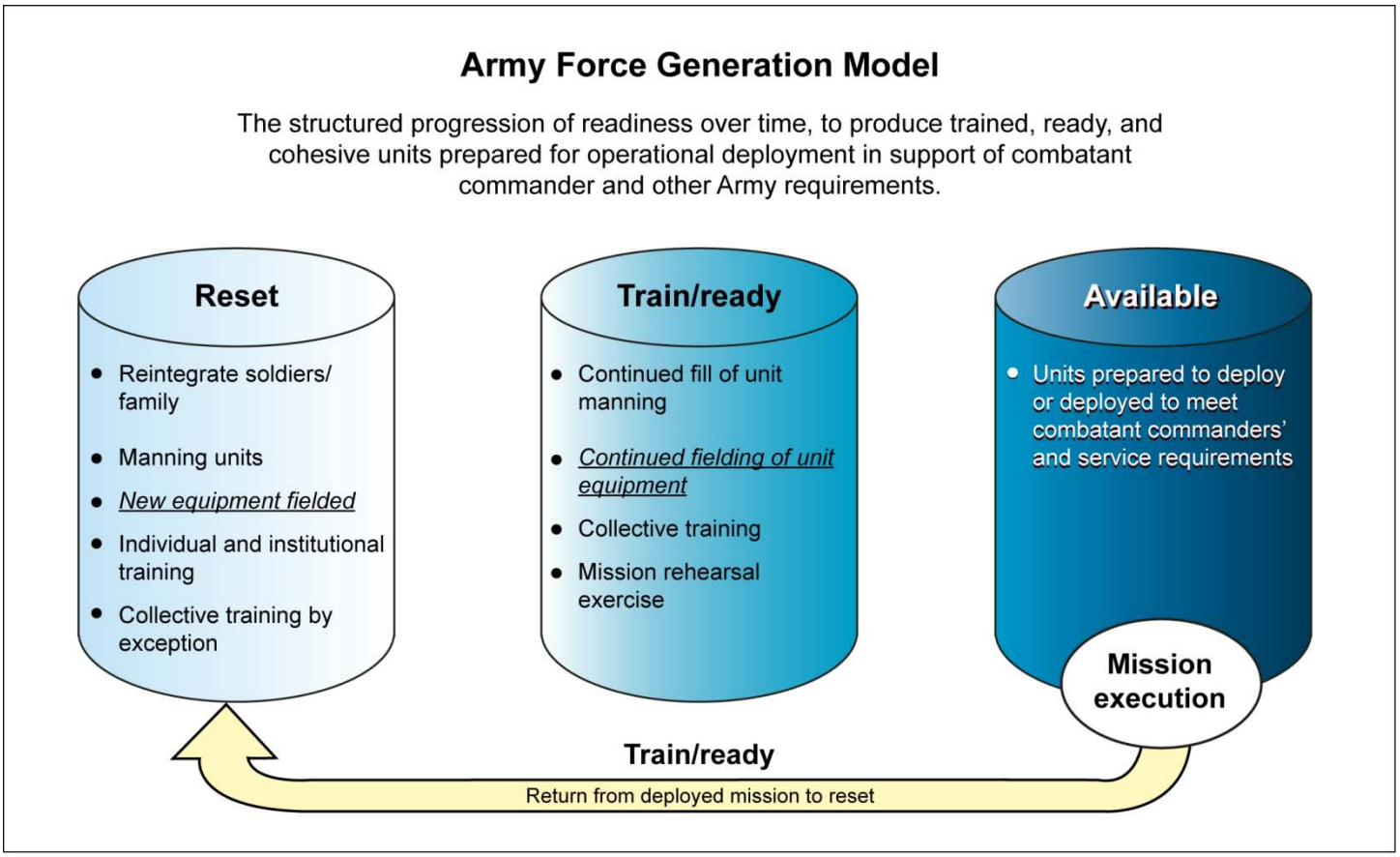
Army Plans to Synchronize Integration of New Technology with Deployment of Forces

To achieve its tactical network objectives, the Army is changing the way it delivers capability to its operating forces. Previous Army efforts to develop and field network technologies were seldom coordinated. Program funding, developmental timelines, and testing for network-related programs were rarely, if ever, aligned. Network capabilities were fielded piecemeal and frequently for only one element of the operational force, such as at the company, battalion, or brigade level versus an entire brigade combat team. In the past, the Army has sent network systems to operational units already in theater, leaving soldiers to figure out how to use them, resulting in frustrated soldiers and ineffectively utilized systems—all of which had negative effects on unit readiness.

The Army is shelving this approach in favor of capability set management, where it treats tactical network capability as a cohesive portfolio. After evaluating its current operational environment, identifying capability gaps, and designing a suite of systems and equipment to address these gaps, the Army will procure any elements of the set not already in the Army inventory and distribute them throughout a combat formation, from the brigade command post, to the commander on-the-move, to the dismounted soldier. Capability set management also diverges from the past practice of conducting limited user tests of individual systems. The Army plans to test the entire capability set to assess its collective functionality and interoperability, each component's individual performance and compliance with architectural standards, and whether the set works with technology already in use and can accommodate the rapid pace of emerging technologies.

The Army plans to integrate fielding of the capability set with the Army's Force Generation process that prepares forces for deployment through three force pools: Reset, Train/Ready, and Available (See figure 2).

Figure 2: Army Force Generation Model



Source: U.S. Army.

Through capability set management, the Army will align program funding and timelines so that operational units—brigade combat teams and other operating units—receive an integrated network capability set prior to or during the train/ready phase of the Army's Force Generation cycle.[11] The Army expects to buy and integrate the elements of capability set 13 with the existing Army network and later field it to eight brigade combat teams and other operating units. Capability sets will go only to those units in the Army's Force Generation queue available for deployment and will be

[11]For example, two of the units scheduled to receive capability set 2013 are brigades from the 10th Mountain Division located at Fort Drum, New York and Fort Polk, Louisiana.

fielded during the train/ready phase so that operational units are prepared when they land in theater. Additionally, rather than committing to purchasing any given system or capability in quantities sufficient to outfit the entire force at once, the Army will procure only what is needed by units entering the deployment pool.

The NIE conducted from late May to early June of 2012 included the systems for capability set 13, which is composed of vehicles, network components, and associated equipment and software that are intended to deliver an integrated voice and data capability throughout the Brigade Combat Team. This capability set, illustrated in table 2, will field a foundational network baseline, which is based on the integration of available satellite-based communications and land radios, upon which future capability sets will build.

Table 2: Capability Set 13 Systems

Satellite based
Warfighter Information Network-Tactical Increment 2
Tactical Communication Node
Point of Presence
Soldier Network Extension
Highband Network Radio
Tactical Communication Node
Vehicle Wireless Package
Software
Blue Force Tracker 2/Joint Capability Release software
Multiple Mission Command system improvements through software upgrades
Tactical radios
Handheld, Manpack, Small Form Fit Manpack radio
PRC 117G radio
Dismounted Soldier Radio (152A or Rifleman Radio)
Soldier Radio Waveform Appliqué radio
Soldier networking
Nett Warrior
Other
Company Command Post Capability
Tactical Operations Center Kit
Command Post of the Future/Tactical Battle Command
Tactical Ground Reporting

Source: U.S. Army.

Fielding for capability set 13 started at the beginning of fiscal year 2013, to align with the Army's deployment cycle. This equipment will provide a baseline network solution until the Army's intended networking radio hardware and waveforms are ready for fielding.[12] The Army's deployment cycle is schedule driven in that the operating units are expected to arrive at their destination in a ready and trained status at predetermined times. However, the technical maturity and integration of network capabilities may not always occur as expected. In the future, the challenge for the

[12]A waveform is the representation of a signal that includes the frequency, modulation, type, message format, and/or transmission system.

Army will be to ensure that the network equipment to be sent to operating units has been thoroughly demonstrated and integrated in advance, that fielding decisions are not made solely to accommodate the deployment schedule, and that the process is delivering mature and militarily useful capabilities.

Army's Network Modernization Strategy and Agile Process Face Other Risks and Challenges

The Army's network strategy and agile process face several other risks and challenges as implementation continues. For instance, the Army is still weighing different funding approaches and contracting strategies to enable rapid production of capabilities. The Army is challenged with (1) the inability of some current force vehicles to accommodate new networking capabilities, (2) encouraging both industry and existing programs to implement new computing technologies and standards that will shape future development efforts, and (3) continuing other initiatives aimed at improving efficiency and effectiveness of the network. The network strategy also presents oversight challenges in that the Army has not yet (1) fully defined performance metrics that would allow decision makers to gauge progress in the portfolio and make informed investment decisions and (2) created a consolidated reporting and budgeting framework for the network portfolio.

Army Considering a Variety of Options For Funding and Procuring New Network Capabilities

As part of the agile process, Army officials are testing and evaluating systems presented at the NIEs for forthcoming capability sets at a rapid pace. They are also striving to identify funding methods and contracting strategies that allow rapid procurement and fielding of these systems, yet are consistent with established acquisition regulations. The processes for procuring systems that are already part of a program of record are understood. Those programs go through various acquisition steps that include developing a requirement, developing and procuring systems to meet the requirement, and identifying funds to procure those systems through the traditional budgeting process. However, the processes for buying systems that are not already established programs is less clear due to the fact that items to be bought are not yet known and it can take 2 years to complete the budget cycle.

The Army has identified a number of possible funding scenarios for systems under evaluation that are chosen for procurement after an NIE. One option would be to reprogram unobligated funds from other programs. Another option available is to procure initial quantities of chosen systems from a $25 million procurement fund the Army worked into the fiscal year 2013 budget, and obtain follow-on procurements

through the traditional budgeting process. However, the Army seems to realize that the reprogramming option may not be available in all cases and that the $25 million procurement fund may not be sufficient. According to Army officials, a third option would be to allow continued development of the proposed capability to proceed in conjunction with similar efforts to develop new technologies under DOD's science and technology line of effort. In any event, the Army may face challenges given the long lead time for getting items in the budget (up to 2 years), and items the Army wants to buy may not be known at the time the budget is prepared.

Finally, the Army is looking at various contracting strategies available under existing acquisition regulations to enable it to rapidly procure a capability. If the capability originated from a program of record, procurement would proceed according to the program's acquisition strategy. However, if the capability is not linked to a program of record or if multiple contractors could provide a comparable system, the Army will most likely look to competitively procure the capability, which could be time consuming. If the capability in question is available under a General Services Administration schedule, the Army could proceed to order off the schedule. However, the Army noted that acquiring such a capability without adequate evaluation and testing adds risk that it will not work properly in a combat environment.

The Army is still formulating plans for funding and procuring networking equipment in capability sets planned for combat brigades in fiscal years 2014 and beyond. Planning documents we reviewed reflect uncertainty about the source of future funding over the next 2 years, noting that funding strategies could require reprogramming above thresholds allowable at the DOD's discretion, which would require congressional approval. For fiscal years 2016 and beyond, capability sets could be included in the fiscal years 2015-2019 planning budget and future budget submittals.

Army Addressing Size, Weight, Power, and Cooling Challenges of Heavy Forces

A number of the Army's current fleet of combat and tactical vehicles—the Abrams, Bradley, and Paladin—have reached or exceeded their size, weight, power, and cooling limit. The Army is managing upgrades to these vehicles based on technical advances, cost benefit analyses, and alignment with vehicle modernization opportunities. These vehicles will receive moderate capability improvements, or interim solutions, until modernized vehicles are available to receive full network capabilities. Operational needs and changes to combat vehicle modernization plans

have led the Army to focus on initially fielding its new network capabilities to infantry and Stryker brigades.[13]

The integration and fielding of network capabilities to the heavy brigades cannot occur until the heavy combat vehicles are network-ready. The Abrams and Bradley upgrades are expected to begin production in fiscal year 2017 and the Paladin upgrade program started developmental testing in May 2011 with its first production delivery scheduled for June 2015. According to the Army, the Stryker, particularly the Double V-Hull variant, has proven protection and size, weight, and power capacities to accept some of the capability set 13 network-related equipment. Under the capability set management process, the Army will complete some initial Stryker Brigade Combat Team network modernization two years faster than originally planned. The Army is also developing a new ground combat vehicle and a joint light tactical vehicle. The challenge for the Army will be to align new network technologies with the upgraded and newly procured vehicles in a cost effective and efficient manner.

Army Focusing on Having Industry and Programs of Record Implement Common Operating Environment

A key component of the Army's tactical network development strategy is to establish technical standards to guide the computing environment. The Army has defined and begun to implement a set of computing technologies and standards to which the network, all applications, and all network systems must comply. The Army believes this Common Operating Environment (COE) will reduce development time, lower costs, improve interoperability, and ease system maintenance. The value of having a COE is that industry will know in advance the standards to which it must build solutions, cutting acquisition timelines and, possibly, cost. The COE is expected to reduce the complexities of configuration, support, and training, making integration of new capabilities with existing technology much easier and faster.

The COE, which includes the current network architecture, is intended to reduce duplication and redundancy. For example, rather than asking for proposals to provide a new network capability that complies with various standards and interfaces, the Army would specify that the new capability should assume that certain capabilities already reside within the network.

[13]A brigade combat team is the U.S. Army's basic deployable unit of maneuver. A Stryker Brigade Combat Team is a mechanized infantry force structured around the lightweight armored Stryker vehicle.

One of the key issues stemming from this initiative is how and when to get current programs of record, which number in the hundreds, to fully implement the COE. The initial implementation of this convergence has already begun and the Army's goal is to ensure full implementation by all programs in 5 years. The Army has already acknowledged some challenges it will face in getting current programs of record to fully implement the COE, including

- Securing funding—COE convergence is an unfunded requirement at present;
- Managing up front and transition costs, which are expected to be high;
- Aligning implementation to lessen potential for disruption to schedule and cost of Army acquisition programs;
- Aligning requirements and acquisition processes; and
- Revising current testing methodologies to help facilitate the desired pace of technological change.

Technical standardization is necessary to speed development and fielding of new capabilities. The COE provides industry the parameters within which Army technology (hardware and applications) must fit. The Army also mandated a single mode for transmission of information, regardless of format; text, voice, video, signal, or other type of data. That mode of transmission—which is called "everything over Internet protocol"—brings the Army in line with commercial-sector norms and expands the possibility of using commercial-off-the-shelf, or near-commercial-off-the-shelf solutions, especially for hardware, such as radios. Pre-existing standards and nonproprietary Internet protocol and waveforms will enable industry to develop products more quickly than previously possible. In addition, technology built to common standards will make the testing process simpler, and integration with existing systems and software, including those of U.S. allies, much easier and faster. However, a drawback to the "everything over Internet protocol" policy is that such a policy makes Army networks more vulnerable to widely-proliferating, Internet-based attacks.

If implemented properly, COE could facilitate improved efficiency for the Army's network development effort including lower costs, lower risks, and improved performance. However, COE implementation also represents a

potential bottleneck or chokepoint if the challenges discussed above are not addressed in an effective and timely manner by the Army.

Army Is Pursuing Other Network Initiatives to Improve Efficiency and Effectiveness

Over the next several years, to improve efficiency and effectiveness, the Army plans to pursue a number of network improvement initiatives such as consolidating several separate sensor networks; consolidating a number of network planning, monitoring, and other tools; moving toward a single set of network tools; and improving the efficiency of command posts because commanders need a converged voice, data, imagery, and video transport system capability that is reliable and secure in a cyber and electronic warfare environment. The Army has also started an initiative to identify and manage the costs—including operating and support costs—of the Army tactical network. Each of these initiatives could be challenging in that it is expected to impact multiple components of the emerging network at the same time that the Army is proceeding with integration and fielding.

- The Army has identified benefits of taking several existing but separate sensor networks and consolidating their capabilities for improved efficiency and effectiveness. These networks have separate operation centers and employ many different satellites. As a result, according to the Army, there is inefficient network utilization and limited operational utility. The goal is to consolidate to far fewer operational centers and to employ fewer satellites. Among other benefits, the consolidation is expected to provide more responsiveness, agility, and quality of service. This initiative will begin soon and initial parts of the consolidation will be demonstrated in NIE 13.2.

- The Army has identified a need to consolidate various network planning, monitoring, and other tools for better efficiency and effectiveness. Currently, network operations tools such as network planning, monitoring, and loading devices reside in many individual network systems and each are used independently. The consolidation initiative will move toward the use of a single set of network tools that can deal with issues throughout the network. According to the Army, the potential benefits include more network visibility and reduced cost and complexity. As the Army identifies opportunities to use common tools, officials will adjust the network architecture. The Army plans to evaluate the converged tools at forthcoming NIEs.

- Another Army initiative involves the integration of existing and new elements of command posts, which are made up of many different systems and subsystems. Currently, most of the command post elements are not integrated, resulting in inefficiencies for the network as a whole. This initiative is to incrementally integrate the current command post systems and other systems demonstrated at NIEs. As a part of that demonstration, the command post architecture will be examined closely and standardization implemented wherever possible. The Army will also develop new command post operational procedures as well as training materials and processes. As it moves forward, the Army plans to evaluate the updated command posts at the NIEs.

- The initiative, called Resourcing the Portfolio, is to identify and manage the costs of the Army network enterprise in various ways. During the recent capability portfolio review, the Army looked at the operating and support requirements and funding for the various mission command systems and found that the projected annual costs would be far beyond the current expected funding levels. Those additional costs, coupled with the expected costs of future NIEs, capability set fielding, and the other new initiatives would have to be appropriately addressed in the fiscal years 2014-2018 budget planning deliberations. At the same time, the Army wants to find ways to reduce the operating and support costs of the various systems that are already in the current network as well as those expected to be introduced in coming years.

Information and Insights from NIEs and Consolidated Budgeting Could Benefit DOD and Congressional Oversight

In February 2011, USD(AT&L) designated the Army Tactical Network as a special interest portfolio consisting of a set of acquisitions. As part of this special designation, the USD(AT&L) directed the Army to provide a comprehensive network acquisition strategy to ensure the alignment, adaptation, and synchronization of acquisition efforts, including network integration and testing. The USD(AT&L) directed the Overarching Integrated Product Team Chair for Network to provide periodic portfolio reviews. According to USD(AT&L) officials, the Chair for Network conducted an initial review in 2011 of the Army's proposed network architecture and its strategy for acquiring, integrating, and fielding the network. In that review and subsequent collaboration with the Army, the USD(AT&L) officials and staff have (1) provided extensive technical input on the soundness of individual network components and whether they are in synch with the rest of the capability set and the existing network as a whole, and (2) reviewed the acquisition schedules of all the network programs of record within the capability set to ensure that they are

properly aligned. Also, USD(AT&L) officials and staff have provided input as part of acquisition milestone reviews for major programs that are a part of the Army network.

DOD has also issued guidance for the measurement of outcomes from IT investment portfolios, which would include the network portfolio. DOD's directive, issued in 2005, calls for responsible authorities to "measure[ ] actual contributions of the portfolio against established outcome-based performance measures to determine improved capability as well as to support adjustments to the mix of portfolio investments, as necessary." [14] The Army and DOD consider the fielding of capability set 13 as the initial output from the Army's network modernization portfolio but have yet to fully define outcome-based performance measures to evaluate the actual contributions of the capability set. The Army and USD(AT&L) officials point to a set of design considerations that drove the definition of capability set 13 as appropriate sources for outcome-based performance measures. Those design considerations include (1) robust network connectivity from the command post down to the soldier; (2) access to unclassified, classified, and coalition networks; and (3) planning, configuration, and monitoring of the network.

Subsequently, the expectation is that capability set 13 and the entire Army network will be evaluated at future NIEs. Optimally, based on those evaluations, the Army and USD(AT&L) would have the necessary information to determine how capability set 13—as fielded in operational units—has actually affected (1) overall network performance, (2) identified capability gaps, and (3) essential network capabilities. That could provide a basis to determine if any adjustments need to be made to future capability sets. However, it is not yet clear whether and how the NIE can provide the necessary data and insights on the performance of the network as a whole. To date, the NIEs have been focused primarily on the operational testing of selected major acquisition programs and the operational evaluation of emerging network capabilities. While USD(AT&L); Army; and Director, Operational Test and Evaluation officials offer that the NIEs present a good opportunity to evaluate the overall performance of the network, they concede that they have not designed the NIEs to fully focus on that task.

[14]Department of Defense Directive 8115.01, Information Technology Portfolio Management (Oct. 10, 2005).

Although the Army is managing its network modernization initiatives as a portfolio, the individual programs and initiatives are spread out over a variety of research and development and procurement accounts. Budget justification and other planning materials for these individual programs and initiatives focus mostly on planned activities to move the individual system along in the development effort and little on how that system may relate to the network as a whole. For the fiscal year 2013 request, the network portfolio was made up of over 50 research and development and procurement budget elements. At present, these materials do not provide insight into the budgets and activities for the tactical network capability sets as a whole, which could stymie oversight of the Army network development and fielding by congressional committees. A consolidated reporting and budgeting framework for all of the programs that are part of the tactical network portfolio could yield more consistency and clarity in the justifications for Army network initiatives as well as facilitate oversight of the strategy's affordability.

Conclusions

Given less-than-successful past efforts to modernize its information network, the Army is making a good faith effort to take a more realistic, lower-risk strategy to getting the capability it desires. Specifically, leveraging private sector innovation to quickly and incrementally deliver technology has advantages over the Army trying to define and develop an ultimate long-term solution. Yet, this strategy is only in its initial stages and there are a number of implementation challenges that lie ahead. Looking ahead, although the Army network strategy is more modest from a technology standpoint, it is still a huge transformational effort that will affect all aspects of Army operations. The size and scope of the Army's modernization investment deserves high-level oversight attention by both the Army and DOD. Effective oversight can reduce risk and improve outcomes.

Regarding implementation, DOD and the Army collaborated extensively on the technical design of capability set 13 and the Army has proceeded with the procurement and fielding of those capabilities. To facilitate oversight of the latter phase, it is important for the Army and DOD to assess the actual contributions of the initial capability set to be fielded in fiscal year 2013 and use the results to inform future investments. Establishing outcome-based performance measures will allow the Army and DOD to assess progress of network development and fielding and be in a position to determine the cost-effectiveness of their investments in capability set 13. It will also be important for the Army to assess the cost effectiveness of individual initiatives before and during implementation.

The Army and DOD are expecting a lot from future NIEs in terms of providing information and insights on the capability sets and the Army network as a whole; however, these officials have yet to put a plan in place to make this a reality. Finally, as the NIE process begins to provide the needed information and insights, DOD oversight would be enhanced by an Office of the Secretary of Defense-level review of the actual effectiveness and suitability of capability set 13. Such a review should consider how capability set 13 actually affected overall network performance, capability gaps, and essential network capabilities. This level of review would be part of the intended periodic reviews and be more targeted than the initial review conducted in 2011 and could help to ensure that available resources are managed effectively.

It is important for the Army to take the steps necessary to ensure that the technologies it procures are fully mature and ready for integration and fielding; immature technology delivered faster still puts the Army at risk for less than optimum results. Considering nondevelopmental items or commercial-off-the-shelf options has the potential benefit of substantially lower development time and cost. However, those options may not be available to address all of the capability gaps, and some development investments may be needed over time. Also, given the realities of the federal budgeting process and the time commitments associated with full and open competition, it may not be possible to procure all emerging technologies immediately. However, if the Army can find a way to procure and field new technologies within 2 to 3 years, that is still considerably better than a typical development effort that in the past has taken a decade or longer. Industry participation may be a lynchpin to the continued availability of cutting edge network capabilities, but to date, Army procurement of new network technologies from other than programs of record has been very limited. The Army/industry relationship will have to be carefully monitored and nurtured—that should be a priority for both DOD and the Army.

Regarding oversight, the Army's network investment is a dispersed portfolio of efforts funded in a number of places in the budget. While network modernization is not defined as a major acquisition program, it is a substantial level-of-effort investment that will encompass on the order of $3 billion a year indefinitely. The magnitude and duration of the financial commitment command attention regarding the affordability of the strategy. Increased congressional and DOD oversight of the Army network portfolio would benefit from an integrated budget encompassing the Army tactical network elements.

Recommendations

In order to enhance oversight of Army network initiatives by the Army, DOD, and Congress, we recommend that the Secretary of Defense direct the Secretary of the Army to

- define an appropriate set of quantifiable outcome-based performance measures to evaluate the actual contributions of capability set 13 and future components under the network portfolio, and
- develop and implement a plan for future NIEs to provide the necessary information and insights to determine if those performance measures have been met.

As additional information is provided, we recommend that the Secretary of Defense identify an oversight body to

- determine how capability set 13—as fielded in operational units—has actually impacted overall network performance, capability gaps, and essential network capabilities and make recommendations for adjustments, as may be necessary, and
- determine how well the Army is rapidly fielding mature and militarily useful network capabilities to its operating forces and maintaining robust industry participation in the process.

To facilitate congressional oversight of the overall affordability of this important Army initiative, we also recommend that the Secretary of Defense direct the Secretary of the Army to consolidate tactical network budget elements and justifications into a single area of the Army budget submittal.

Agency Comments and Our Evaluation

DOD provided written comments on a draft of this report. Of the five recommendations, DOD concurred with two and partially concurred with the three other recommendations. DOD's comments appear in appendix V. DOD also provided technical comments, which we have incorporated as appropriate in the report.

DOD concurred with our recommendations that the Army (1) define an appropriate set of quantifiable outcome-based performance measures to evaluate the actual contributions of capability set 13 and future components under the network portfolio and (2) develop and implement a plan for future Network Integration Evaluations (NIEs) to provide the necessary information and insights to determine if those performance

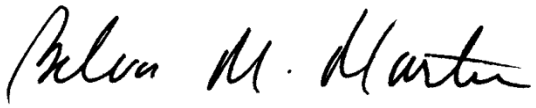
measures have been met. However, DOD noted that the complexity of NIEs will change in the future and that those changes will result in outcome-based performance measures changing accordingly. DOD also noted that the Army, as well as other military departments and several major components, are working collaboratively to define the architecture and standards for a Joint Information Environment, which will help focus DOD engineering efforts on five specific operational capabilities, including network normalization and single security architecture. DOD further noted that it is defining metrics and associated minimum values for each capability and that the Army's network modernization strategy and NIEs will need to conform to the Joint Information Environment architecture and standards. The development of Joint Information Environment architecture and standards will be noteworthy to the extent that they enhance oversight, reduce risk, and improve outcomes. Regarding our recommendation to develop a plan to use future NIEs to provide information and insights into how well performance metrics have been met, DOD noted that NIEs are not static events and that plans will evolve over time. We recognize the dynamic nature of the NIEs and agree adjustments to the plan will be necessary and we will monitor the Army's progress in developing and implementing its plan in our continuing review of the Army's tactical network strategy.

DOD partially concurred with our two recommendations regarding an oversight role for the Overarching Integrated Product Team Chair for Network to determine (1) how capability set 13 has actually impacted overall network performance, capability gaps, and essential network capabilities; and (2) how well the Army is rapidly fielding mature and military useful network capabilities to its operating forces and maintaining robust industry participation in the process. While noting that the specific integrated product team we referenced no longer exists, DOD agreed that an Office of the Secretary of Defense-level oversight body needs to be identified and chartered to review the Army system-of-systems NIEs. Such a body would provide oversight of the NIEs and inform the acquisition and budget processes. In response to DOD comments, we have modified our recommendation to reflect the need for an Office of the Secretary of Defense-level oversight body instead of the Overarching Product Team Chair for Network that no longer exists. DOD also agreed to work with the Army to maintain industry support and participation in the agile process. Because the Army is moving out to field capabilities, we believe that the oversight body needs to be established expeditiously in order to evaluate in near real time the results of NIE 13.1 and the initial fielding of capability set 13.

Finally, DOD partially concurred with our recommendation that the Secretary of Defense direct the Secretary of the Army to consolidate network budget elements and justifications into a single area of the Army budget. DOD stated that this recommendation was too broad and unclear, noting that the complete Army Network Portfolio is broader than the tactical segment addressed in our report. We agreed to clarify and narrow the recommendation to consolidate "tactical" network budget elements and justifications into a single area of the Army budget. DOD notes that the Army has already consolidated many elements of the network in its Mission Command portfolio and is developing a structure to align all network assets. The purpose of the recommendation is to facilitate congressional oversight; therefore, we support actions by the Army to increase clarity and visibility to improve congressional oversight of the Army's tactical and other network initiatives.

We are sending copies of this report to the appropriate congressional committees, the Secretary of Defense, the Secretary of the Army, and other interested parties. In addition, the report is available at no charge on the GAO website at http://www.gao.gov.

If you or your staff have any questions about this report, please contact Belva M. Martin at (202) 512-4841 or martinb@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix VI.



Belva M. Martin
Director, Acquisition and Sourcing Management

Appendix I: Scope and Methodology

Our objectives were to (1) examine the extent to which the Army's agile process addresses cost, technology maturity, security, and readiness; and (2) identify other risks and challenges facing implementation of the Army's agile process and networking in general.

To examine the extent to which the Army's agile process addresses cost, technology maturity, security, and readiness, we interviewed officials from the Army's System of Systems Integration Directorate; the Army Training and Doctrine Command; the Army's Program Executive Office for Command, Control, Communications—Tactical; the Army's Program Executive Office for Intelligence, Electronic Warfare and Sensors; Communications—Electronics Research, Development, and Engineering Center; Army G-8; and the Army Test and Evaluation Command. We also interviewed officials from the Deputy Assistant Secretary of Defense for Developmental Test and Evaluation; the Director, Operational Test and Evaluation; and the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics. We analyzed the Army's emerging agile process and evaluated it against acquisition best practices, and we toured lab facilities to understand how the Army is validating and selecting technologies for network evaluations. We reviewed Army programmatic documentation to understand cost projections for testing and procuring network equipment under the new approach and we analyzed current and prior budget documentation in order to evaluate how the Army would resource this approach. We also analyzed the Army's emerging plans for ensuring networking hardware receives proper security certifications and reviewed the Army's assessments of recent testing for information assurance and network protection. Finally, we reviewed the Army's agile process to identify the fielding strategy for equipping units with emerging networking capabilities.

To identify other risks and challenges, we compared the Army's agile process and overall networking strategy against established policies for managing a portfolio of capabilities. We reviewed Army decisions to defer network improvements to certain legacy platforms due to acknowledged size, weight, and power limitations. We attended test events and an industry day and spoke with contractor officials about their experiences with the agile process. We also interviewed Army officials to identify other networking challenges the Army is addressing concurrent with implementation of the agile process.

We discussed the issues presented in this report with officials from the Army and the Secretary of Defense and made several changes as a result.

We conducted this performance audit from February 2012 to January 2013 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Army Mission Command Essential Capabilities

Essential network capability	Description
Robust Network Transport Capability	A converged voice, data, imagery, and video transport layer consisting of line-of-sight and beyond line-of-sight means that are reliable, protected, layered, secure, and defended in a cyberspace and electronic warfare environment.
Execute Tactical Network Operations	Efficient and dynamic allocation of transport resources to maximize mission command application and service performance in all conditions and through all phases of operations.
Standard and Sharable Geospatial Foundation	Enable all elements of the force to operate on the same map and support real-time coordination and collaboration.
Display/Share Relevant Tactical Information	Enable the receipt and dissemination of essential information from dismounted soldier to all higher echelon command posts.
Enable Collaboration	Sharing of ideas and situational awareness within the tactical, operational, and/or strategic community of interest.
Create, Communicate, and Rehearse Orders	Collaboratively create, change, distribute and rehearse mission orders (voice, written, and graphical) between command posts, platforms, dismounted leaders, and soldiers.
Command and Control on-the-Move	Maintain situational awareness and communications while away from the command post and moving on the ground or in the air.
Execute Running Estimate	Continuously gather, track, and fuse logistic and intelligence and operational information to support tactical decision making and continuous assessments.
Joint, Interagency, Intergovernmental, and Multinational Interoperability	Coordinate and collaborate with authenticated partners to exchange relevant intelligence and operational information
Training Support	Support live-virtual-constructive-gaming training environments and enhance mission rehearsals

Source: U.S. Army.

Appendix III: Highest Priority Army Network Capability Gaps and Descriptions

Capability Gap	Description
Fusing Operations and Intelligence at the Tactical Edge	Commanders and leaders engaged at the tactical edge have very little capability to combine local information/intelligence, position location information, processed sensor data and intelligence, and higher-level environmental information together to define contextual significance/implications and inform understanding, decisions, and actions.
Executing Command and Control On-the-Move	Commanders and leaders engaged in full spectrum operations require the capability to access, filter, share, display, and collaborate on fused operations and intelligence information, while operating away from their command post, in air or ground platforms, and while dismounted at the tactical edge.
Building a Common Operating Picture	Commanders and leaders…have limited capability to access, select, integrate, display and share relevant information (geospatially rectified and time stamped) from multiple sources.
Connecting Joint, Interagency, Intergovernmental, and Multinational (JIIM) Partners	Commanders and leaders engaged in full spectrum operations have limited capability to digitally integrate JIIM partners during planning and execution.
Tailoring Network Transport	Commanders and leaders lack the capability to dynamically adapt network architecture and resources to match network transport capability with the commander's priorities in support of full spectrum operations

Source: U.S. Army.

Appendix IV: Technology Readiness Levels

Technology Readiness Levels (TRL) are measures pioneered by the National Aeronautics and Space Administration (NASA) and adopted by the Department of Defense (DOD) to determine whether technologies were sufficiently mature to be incorporated into a weapon system. Our prior work has found TRLs to be a valuable decision-making tool because they can presage the likely consequences of incorporating a technology at a given level of maturity into a product development. The maturity level of a technology can range from paper studies (TRL 1), to prototypes that can be tested in a realistic environment (TRL 7), to an actual system that has proven itself in mission operations (TRL 9). According to DOD acquisition policy, a technology should have been demonstrated in a relevant environment or, preferably, in an operational environment (TRL 7) to be considered mature enough to use for product development. Best practices of leading commercial firms and successful DOD programs have shown that critical technologies should be mature to at least a TRL 7 before the start of product development.

Table 3: Technology Readiness Levels

Technology readiness level	Description	Hardware and software	Demonstration environment
1. Basic principles observed and reported.	Lowest level of technology readiness. Scientific research begins to be translated into applied research and development. Examples might include paper studies of a technology's basic properties.	None (paper studies and analysis).	None.
2. Technology concept and/or application formulated.	Invention begins. Once basic principles are observed, practical applications can be invented. The application is speculative and there is no proof or detailed analysis to support the assumption. Examples are still limited to paper studies.	None (paper studies and analysis).	None.
3. Analytical and experimental critical function and/or characteristic proof of concept.	Active research and development is initiated. This includes analytical studies and laboratory studies to physically validate analytical predictions of separate elements of the technology. Examples include components that are not yet integrated or representative.	Analytical studies and demonstration of non-scale individual components (pieces of subsystem).	Lab.
4. Component and/or breadboard. Validation in laboratory environment.	Basic technological components are integrated to establish that the pieces will work together. This is relatively "low fidelity" compared to the eventual system. Examples include integration of "ad hoc" hardware in a laboratory.	Low-fidelity breadboard. Integration of non-scale components to show pieces will work together. Not fully functional or form or fit but representative of technically feasible approach suitable for flight articles.	Lab.

Technology readiness level	Description	Hardware and software	Demonstration environment
5. Component and/or breadboard validation in relevant environment.	Fidelity of breadboard technology increases significantly. The basic technological components are integrated with reasonably realistic supporting elements so that the technology can be tested in a simulated environment. Examples include “high fidelity” laboratory Integration of components.	High-fidelity breadboard. Functionally equivalent but not necessarily form and/or fit (size, weight, materials, etc.). Should be approaching appropriate scale. May include integration of several components with reasonably realistic support elements/subsystems to demonstrate functionality.	Lab demonstrating functionality but not form and fit. May include flight demonstrating breadboard in surrogate aircraft. Technology ready for detailed design studies.
6. System/subsystem model or prototype demonstration in a relevant environment.	Representative model or prototype system, which is well beyond the breadboard tested for TRL 5, is tested in a relevant environment. Represents a major step up in a technology’s demonstrated readiness. Examples include testing a prototype in a high-fidelity laboratory environment or in simulated operational environment.	Prototype—Should be very close to form, fit, and function. Probably includes the integration of many new components and realistic supporting elements/subsystems if needed to demonstrate full functionality of the subsystem.	High-fidelity lab demonstration or limited/restricted flight demonstration for a relevant environment. Integration of technology is well defined.
7. System prototype demonstration in an operational environment.	Prototype near or at planned operational system. Represents a major step up from TRL 6, requiring the demonstration of an actual system prototype in an operational environment, such as in an aircraft, vehicle, or space. Examples include testing the prototype in a test bed aircraft.	Prototype. Should be form, fit, and function integrated with other key supporting elements/subsystems to demonstrate full functionality of subsystem.	Flight demonstration in representative operational environment such as flying test bed or demonstrator aircraft. Technology is well substantiated with test data.
8. Actual system completed and “flight qualified” through test and demonstration.	Technology has been proven to work in its final form and under expected conditions. In almost all cases, this TRL represents the end of true system development. Examples include developmental test and evaluation of the system in its intended weapon system to determine if it meets design specifications.	Flight-qualified hardware.	Developmental test and evaluation in the actual system application.

Technology readiness level	Description	Hardware and software	Demonstration environment
9. Actual system “flight proven” through successful mission operations.	Actual application of the technology in its final form and under mission conditions, such as those encountered in operational test and evaluation. In almost all cases, this is the end of the last “bug fixing” aspects of true system development. Examples include using the system under operational mission conditions.	Actual system in final form.	Operational test and evaluation in operational mission conditions.

Source: GAO analysis of National Aeronautics and Space Administration data.

Appendix V: Comments from the Department of Defense

CHIEF INFORMATION OFFICER

DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

21 DEC 2012

Ms. Belva M. Martin
Director, Acquisition and Sourcing Management
US Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Ms. Martin,

This is the DoD response to the Government Accountability Office (GAO) Draft Report, GAO-13-179, "ARMY NETWORKS: Size and Scope of Modernization Investment Merit Increased Oversight," dated November 28, 2012 (GAO Code: 121030).

The DoD has reviewed the findings of the GAO and the draft report. We appreciate the efforts of the GAO staff to present objective viewpoints regarding Army Networks. We submit the enclosed comments to the GAO for consideration.

The point of contact for GAO Code GAO-13-179 (GAO Code: 121030 is the undersigned. I can be reached at 703-695-3901 or via email at randall.conway@osd.mil.

Sincerely,

Robert E. Wheeler
Major General, USAF
Deputy Chief Information Officer for
C4 & Information Infrastructure Capabilities

Enclosure as stated

GAO DRAFT REPORT DATED NOVEMBER 28, 2012
GAO-13-179 (GAO CODE 121030)

"ARMY NETWORKS: SIZE AND SCOPE OF MODERNIZATION INVESTMENT MERIT INCREASED OVERSIGHT"

DEPARTMENT OF DEFENSE COMMENTS TO THE GAO RECOMMENDATIONS

RECOMMENDATION 1: In order to enhance oversight of Army Network initiatives by the Army, DoD, and the Congress, GAO recommends that the Secretary of Defense direct the Secretary of the Army to define an appropriate set of quantifiable outcome-based performance measures to evaluate the actual contributions of capability set 2013 and future components under the network portfolio.

DoD RESPONSE:
Concur with the GAO recommendation with the caveat that the complexity of the NIE will change in the future; therefore, outcome-based performance measures will change accordingly. Each NIE is expected to cover a specific number of gaps in the network portfolio in order to be effective as the needed capabilities will change over time. Additionally, the Department of the Army, the other Military Departments and several of the major Components, are working collaboratively to define the architecture and standards for a Joint Information Environment (JIE). The JIE will help focus DoD engineering efforts on five specific operational capabilities: (1) Core Data Centers, (2) Enterprise Operations Centers, (3) Enterprise Directory Services, (4) Network Normalization, and (5) Single Security Architecture. Through Network Normalization, a current capability gap is being filled by providing standardized networks to increase mission effectiveness, improve cybersecurity, and deliver efficiencies. For each capability, metrics, and associated minimum values, are being defined. The Army's network modernization strategy and Network Integration Evaluations (NIE) will need to conform to the JIE architecture and standards for Network Normalization and Single Security Architecture.

RECOMMENDATION 2: In order to enhance oversight of Army Network initiatives by the Army, DoD, and the Congress, GAO recommends that the Secretary of Defense direct the Secretary of the Army to develop and implement a

plan for future NIEs to provide the necessary information and insights to determine if those performance measures have been met.

DoD RESPONSE:
Concur with the GAO recommendation with the caveat that NIEs are not static events and will address different capability gaps in the network portfolio over time. Since plans are developed two NIE cycles out to track identified capability gaps, a plan to develop and implement a plan for future NIEs to provide the necessary information and insights to determine if those performance measures have been met will be addressed over time.

RECOMMENDATION 3: As additional information is provided, GAO recommends that the Secretary of Defense task the Overarching Integrated Product Team Chair for Network to determine how capability set 2013 - as fielded in operational units – has actually impacted overall network performance, capability gaps, and essential network capabilities and make recommendations for adjustments, as may be necessary.

DoD RESPONSE:
Partially-Concur with the GAO recommendation. There is currently no OIPT Chair for system of system oversight. OIPTs are system /platform focused and do not address end to end capabilities. OSD agrees an OSD level oversight body needs to be identified and charted to review the progress of the Army system of system NIEs which will provide oversight of the NIEs and inform the acquisition and budget processes. Additionally, the NIE was designed to quantify Systems Under Evaluation (SUEs) by observation and robust electronic data collection and analysis against the baseline network. This construct has provided quantifiable and objective data to inform decision makers regarding adjustments/fielding to the Capability Sets. Additionally, the OSD response to recommendation one above provides information regarding the Joint Information Environment will provide a construct to evaluate NIE progress. The February 2011 USD AT&L designation of the "Army Tactical Network" as a special interest portfolio refers ONLY to the February 3, 2011 "Early-Infantry Brigade Combat Team Acquisition Decision Memorandum" signed by Mr. Carter. The Overarching Integrated Product Team (OIPT) Chair for Networks referred only to the specific network components of the E-IBCT fielding effort, which has since been cancelled, and the OIPT no longer exists. The Army has governance and oversight mechanisms in place to determine CS13 performance and potential future enhancements through the Agile Process (Department of the Army, Standard Operating Procedure, Agile Capabilities Life Cycle Process, 7 August 2012, Final v.1) and Capability Set Management Board.

RECOMMENDATION 4: As additional information is provided, GAO recommends that the Secretary of Defense task the Overarching Integrated Product Team Chair for Network to determine how well the Army is rapidly fielding mature and militarily useful network capabilities to its operating forces and maintaining robust industry participation in the process.

DoD RESPONSE:
Partially-Concur with the GAO recommendation.

As stated in Recommendation 3, there is no designated Overarching Integrated Product Team (OIPT) Chair for Networks. The Army has governance and oversight mechanisms in place to monitor Capability Set performance and potential future enhancements through the Agile Capabilities Life Cycle Process (Department of the Army, Standard Operating Procedure, Agile Capabilities Life Cycle Process, 7 August 2012, Final v.1) and Capability Set Management Board.

As indicated above an OSD level oversight body will be identified and chartered to review the progress of the Army system of system NIEs which will provide oversight of the NIEs and inform the acquisition and budget processes.

DoD will work with the Army on efforts in support of the Army to maintain industry support and participation in the Agile Capabilities Life Cycle Process.

RECOMMENDATION 5: To facilitate congressional oversight of the overall affordability of this important Army initiative, GAO also recommends that the Secretary of Defense direct the Secretary of the Army to consolidate network budget elements and justifications into a single area of the Army budget.

DoD RESPONSE:
Partially concur with the GAO recommendation.

Per teleconference with GAO on 4 December 2012, the recommendation to consolidate network budget elements is too broad and unclear. The Army recommendation to which GAO agreed is to clarify language to refer only to the tactical network. If the tactical network is defined on table 1 of the GAO report (page 7), then the Army has already consolidated many elements of the network in one portfolio (Mission Command division, HQDA G-8 Force Development). Table 1 includes EQUIPPING PEG Programs of Record and initiatives (e.g. NIE) and does not address tactical network PoRs within HDGA G-8 not managed by G-8 FDC.

The complete Army Network portfolio is broader than the tactical segment specifically addressed in this GAO report as it includes the Generating Force

Enterprise activities. The Army is developing a structure to align all network assets that currently span across the warfighting, business and enterprise information environment mission areas, but this was not included in the scope of the report.

Appendix VI: GAO Contact and Staff Acknowledgments

GAO Contact

Belva M. Martin, (202) 512-4841 or martinb@gao.gov

Staff Acknowledgments

In addition to the contact named above, William R. Graveline, Assistant Director; William C. Allbritton; Marcus C. Ferguson; Kristine Hassinger; Sean Seales; Robert S. Swierczek; and Paul Williams made key contributions to this report.