

GAO

Report to the Chairman,
Subcommittee on Defense,
Committee on Appropriations,
House of Representatives

August 1999

BATTLEFIELD AUTOMATION

Opportunities to Improve the Army's Information Protection Effort



G A O

Accountability * Integrity * Reliability



United States General Accounting Office
Washington, D.C. 20548

National Security and
International Affairs Division

B-280565

August 11, 1999

The Honorable Jerry Lewis
Chairman, Subcommittee on Defense
Committee on Appropriations
House of Representatives

Dear Mr. Chairman:

Over the next decade, the Army's modernization objectives include the integration of information technologies to acquire, exchange, and employ timely information throughout the battlespace. Information technology integration—or digitization—is to be implemented throughout the Army through the development, production, and fielding of over 100 individual systems. According to the President's fiscal year 2000 budget request, the Army's digitization efforts will cost \$20.8 billion between fiscal year 2000 and 2005. The Army expects this investment to result in increased survivability, lethality, and tempo of operations. However, it also recognizes that reliance on digitization could make its command and control systems more vulnerable to enemy activities such as jamming and computer network attacks and has developed a *Protection Plan for Army XXI Information Systems* that lays out a general strategy for implementing information protection into the design of the digitized battlefield.

This report is in response to a Subcommittee request to evaluate the Army's development and acquisition plans for command and control systems that will be part of future digitized battlefield units. Specifically, we evaluated the Army's protection plan to determine whether it ensures sufficient assessments to test and develop the defensibility of the digitized battlefield against command and control warfare attacks.

Results in Brief

The Army has carried out a number of assessments to test and develop the defensibility of digitized battlefield systems and forces, but its protection plan does not ensure sufficient vulnerability assessments. While the Army's plan provides a general strategy for implementing information protection into the design of the digitized forces, it does not constitute a detailed implementation plan, one that lays out

- the specific systems, networks, and infrastructures covered;

-
- their information protection requirements or needs;
 - the information protection knowledge and knowledge gaps for those systems; and
 - the tests or other events that will be used to fill specific knowledge gaps and address previously identified weaknesses.

Without such a detailed implementation plan, systems vulnerabilities that might otherwise be identified may not be exposed and fixed and the substantial investment made by the Army could be at risk. Additionally, without a plan that identifies specific needed events, adequate funding may not be made available for needed activities, and valuable test opportunities could be lost. Furthermore, systems could be developed and tested under requirements that are not aligned with the goals and needs of the Army's protection plan. For example, we found that a key digitization effort does not have a minimum requirement for development of the protection concept outlined in the Army's protection plan. As a result, systems could be developed without providing features needed to achieve that concept. We also found that the system that is the centerpiece of the Army's digitization efforts has a key performance requirement that is set for a non-jamming environment and is not conducive to judging whether sufficient protection has been achieved. While the Army has already undertaken a number of activities laid out in its protection plan, much remains to be done as its digitization efforts are to extend over the next decade and be implemented through the development, production, and fielding of over 100 individual systems.

This report contains recommendations to the Secretary of Defense regarding the management of the Army's digitization-related information protection activities.

Background

The Army plans to use vulnerability assessments, including red team activities, to help develop digitization systems and networks. Vulnerability assessments are conducted to determine potential and exploitable weaknesses; red teaming activities are a specialized type of vulnerability assessment in which a group acting as an opposing force conducts offensive actions to generate a reaction or expose a weakness on the friendly side.

The Army has defined 16 high-priority systems that, at a minimum, are to be fielded to accomplish its First Digitized Division. (The Army plans to field its First Digitized Division by December 2000 and its First Digitized Corps

by September 2004.) One of these 16 high-priority systems—the Force XXI Battle Command, Brigade and Below (FBCB2) system—is the centerpiece of the Army’s digitization efforts because of its potential to contribute significantly to achieving the Army’s digitization goals.¹ When fielded, FBCB2 is expected to provide enhanced situational awareness to the lowest tactical level—the individual soldier—and a seamless flow of command and control information across the battlespace.

FBCB2 will be composed of

- a computer that can display a variety of information, including a common picture of the battlefield overlaid with graphical depictions (known as icons) of friendly and enemy forces;
- software that automatically integrates Global Positioning System data, military intelligence data, combat identification data, and platform data (such as the status of fuel and ammunition); and
- interfaces to communications systems.

Battlefield data will be communicated to and received from users of FBCB2² through the Tactical Internet—a network of tactical radios³ for the transmission and receipt of data needed for battlefield situational awareness and command and control decisions. The FBCB2 system requires a functioning and protected Tactical Internet to accomplish its mission.

Because the FBCB2 system and Tactical Internet are two of the Army’s most important digitization efforts, establishing their ability to withstand attacks is critical. The Army’s near-term information protection efforts have been designed to capitalize on FBCB2 and Tactical Internet development and test events “culminating in a ‘no holds barred’ electronic and computer attack” during the FBCB2 system’s initial operational test and evaluation. This test can serve as a proof-of-concept event to determine whether the Army has achieved its intent of developing a level of

¹ Nearly all of the other high-priority Army digitization systems are dedicated to enhancing the Army Tactical Command and Control System.

² For further information on the FBCB2 program, please see [Battlefield Automation: Acquisition Issues Facing the Army Battle Command, Brigade and Below Program](#) (GAO/NSIAD-98-140, June 30, 1998).

³ The Internet’s tactical radios are currently the Enhanced Position Location Reporting System (EPLRS) and Single Channel Ground and Airborne Radio System (SINCGARS).

information systems protection sufficient to allow its critical functions and operations to continue.

Information Protection Plan Is Not Sufficiently Detailed

The Army developed a plan to integrate information protection features and capabilities into its tactical systems, networks, and infrastructure. It has also carried out a number of assessment activities in keeping with that plan. However, while that plan lays out a general strategy for integrating information systems protection into the design of the digitized battlefield, it is not a detailed implementation plan. Without a detailed implementation plan, the Army is not as well positioned as it could be to ensure that important test opportunities are not lost, that needed information protection activities are adequately funded, and that digitization systems development and test requirements accurately reflect the Army's protection needs and goals.

The Army's Protection Plan

In September 1997 the Army Digitization Office published the Army's *Protection Plan for Army XXI Information Systems*.⁴ The plan states that the objective of information systems protection is to ensure that friendly command and control capabilities are available to the commander and staff. It then goes on to describe three types of command and control warfare threats that are of concern: physical attacks, electronic attacks, and computer attacks.

- Physical attacks involve destruction, damage, overrun, or capture of the physical components of "digitization." Overrunning and capture facilitate an adversary's ability to employ computer attacks on friendly forces.
- Electronic attacks (also referred to as electronic warfare) include attacks against communications links and "high energy" attacks. Attacks against communications links include (1) signal intercept to effect compromise of data, (2) radio emitter direction finding and geo-location to support signal analysis and attack, and (3) radio jamming, which is usually intended to corrupt data or deny service. High-energy attacks include those by electromagnetic pulse generators (which destroy or damage electronic components within an area by

⁴ Subsequently, responsibility for oversight and coordination of the efforts outlined in that plan transitioned from the Army Digitization Office to the Army's Director of Information Systems for Command, Control, Communications, and Computers (DISC4).

overloading them with energy) and directed energy weapons such as high-energy lasers (which direct large amounts of energy onto a specified target).

- Computer attacks are generally (1) aimed at software or data contained in either end-user or network computers; (2) intended to range from unauthorized but unobtrusive access to information and unauthorized modification of software or data to total destruction of software and data; and (3) the least well understood form of attack and may involve the most difficult countermeasures to successfully implement.

The protection plan notes that computer attacks can occur in peacetime and wartime and comments that the interconnected nature of the digitization networks may present the opportunity to create widespread service disruption. As a result, the Army plan concludes that computer attacks appear to pose the most serious potential threat to digitization.

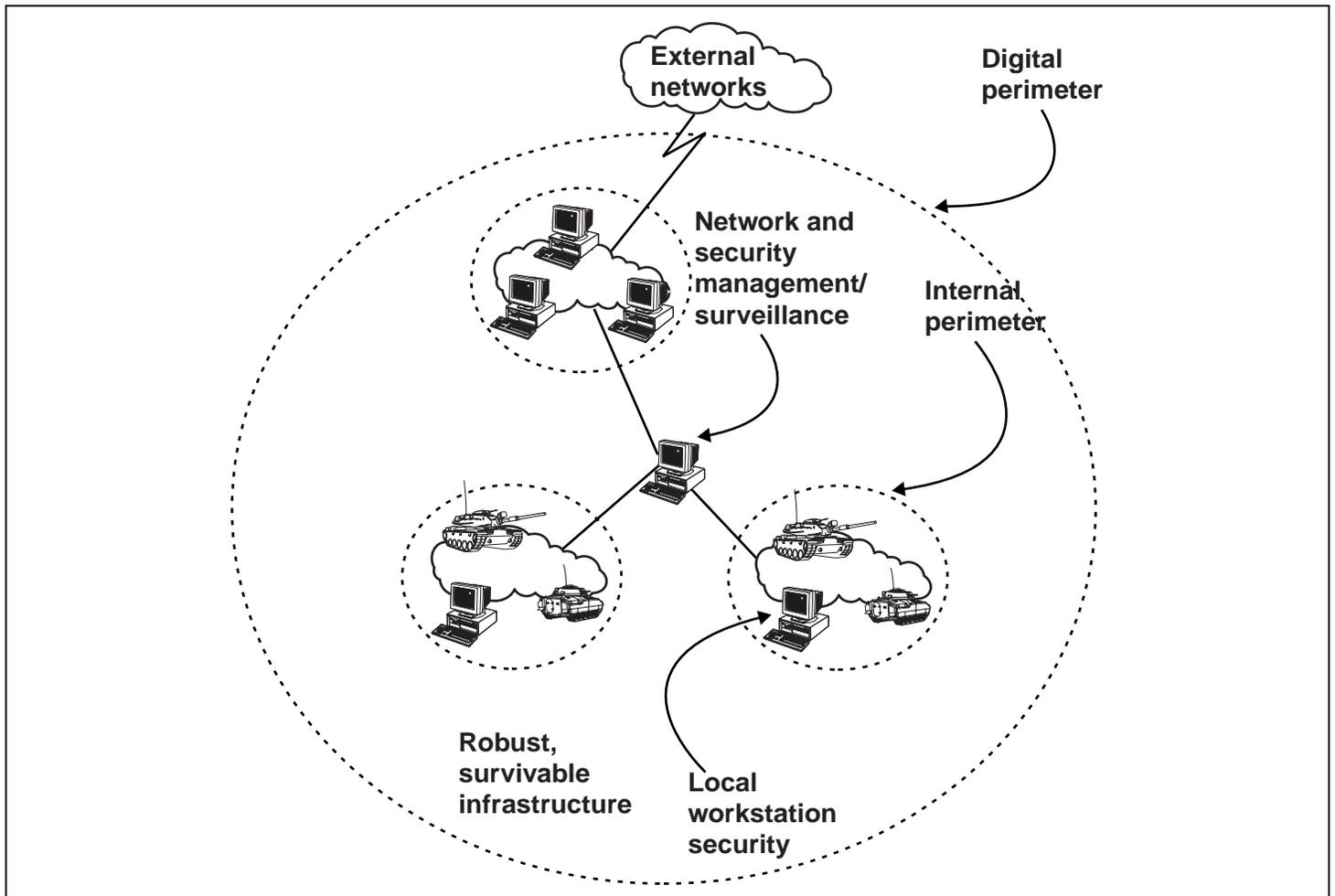
The Army's plan lays out an information protection strategy that reflects its belief that complete protection against all known and future vulnerabilities is not feasible. In line with that belief, the Army's intent is to field a digitized force with a level of protection that is "sufficient" to allow critical functions and operations to continue while under computer attack. To accomplish this level of protection, the Army has adopted a "defense in depth" protection concept consisting of electronically guarded perimeters and active information surveillance. The Army's "defense in depth", depicted in figure 1, is to include

- an external digital perimeter composed of communications security, firewalls,⁵ security guards, and where necessary, physical isolation serving as a barrier to outside networks;
- similar internal perimeters between echelons and/or functional communities;
- a secure local workstation environment, consisting of individual access controls, configuration audit capability, command and control protect tools, and procedures;
- intrusion detection systems;
- extensions to network management capabilities to provide real-time network surveillance and reaction to network intrusions; and

⁵ Firewalls are hardware and software components that protect one set of systems resources (e.g., computers, networks) from attack by outside network users by blocking and checking all incoming network traffic. Firewalls permit authorized users to access and transmit privileged information and deny access to unauthorized users.

- a robust, survivable infrastructure designed to “contain” damage from attacks and to be readily repairable in the event of an attack.

Figure 1: Army’s “Defense in Depth” Protection Concept



Source: U.S. Army, Protection Plan for Army XXI Information Systems.

The Army’s plan lays out a strategy to translate this “defense in depth” protection concept into action by incorporating lessons learned through vulnerability assessment activities into the design and implementation of digitization systems, networks, and infrastructures. These assessment activities are to be conducted during experiments, training events, and development and test events to

-
- determine the level of protection achieved;
 - identify vulnerabilities; and
 - provide feedback to impact (1) architecture, design and development efforts and (2) tactics, techniques, and procedures development and training activities.

The Army's Assessment Activities

The protection plan describes three phases of vulnerability assessments. Phase I and phase II have been completed.

Phase I used computer attacks focused on probing the network for potential vulnerabilities, but did not involve active attacks. During the first phase, electronic attack vulnerability assessments were performed in laboratory and other controlled facilities against individual systems, including EPLRS and SINCGARS. These assessments were conducted as a part of the Task Force XXI Advanced Warfighting Experiment (AWE). Table I.1 in appendix I lists the phase I Task Force XXI AWE RedTeam tasks, their objectives, and where and when they were conducted.

In one example of the Army's phase I activities, the Army's Electronic Proving Ground performed position navigation vulnerability experiments using an early version of FBCB2 software and the Tactical Internet. In a simulated Global Positioning System jamming environment, the Electronic Proving Ground found that the FBCB2 software fluctuated between displaying and reporting inaccurate Global Positioning System and accurate EPLRS position navigation data. The jamming resulted in not only a fluctuating display of inaccurate and accurate positions for the unit's own location, but also the transmission of both inaccurate and accurate position reporting through the Tactical Internet to other units on the network. As a result of this work, the Electronic Proving Ground concluded that the early version of FBCB2 software tested had a major software design problem. The Electronic Proving Ground recommended that this finding be considered by the system developer.

Phase II involved computer attacks focused on intrusions from both outside and inside the network to detect exploitable vulnerabilities. The attackers were allowed to leave "markers"⁶ but were not authorized to cause any physical impact or to disconnect computers from the network. Electronic attacks were simulated or conducted surgically. Table I.2 in

⁶ The "markers" left were computer files indicating that unauthorized access had been achieved.

appendix I lists the September 1997 Army protection plan's list of phase II Division XXI AWE Red Team tasks, their objectives, and where and when they were to be conducted.

One example of red team activities in the Division XXI AWE that is reported to have occurred during phase II was an examination of the impact of jamming the Army's Mobile Subscriber Equipment.⁷ The Army reported that it used progressive jamming against the Mobile Subscriber Equipment of the 3rd Brigade Tactical Operations Center and learned that

- as expected, the Mobile Subscriber Equipment rerouted traffic around jammed frequencies with no initial impact on situational awareness;
- jamming both of the operations center's main data pipes at artificially high levels caused severe slowing of rerouted data traffic; and
- jamming two frequencies with high power for a sustained time would make the perpetrator vulnerable to detection and counterattack by friendly air or artillery.

As a result, the Army concluded that jamming the Mobile Subscriber Equipment would not be a high payoff opportunity for the enemy. Overall, the Army reported that the red teaming efforts conducted during the Division XXI AWE provided valuable insights into strategies for protection of information technologies on the battlefield and reinforced the need for a "defense in depth" approach.

The Army is currently involved in phase III of the vulnerability assessments outlined in its protection plan for Army XXI information systems. The assessments conducted in this phase are to be progressively more robust, more broadly based attacks intended to apply stress to digitization systems, networks, and infrastructure. Ultimately, this phase is to culminate in a "no holds barred" command and control attack on its digitization systems. The Army, however, has not yet defined the scope and nature of the attacks that are to occur during that event.

The Army's protection plan calls for its phase III activities to capitalize on the FBCB2 system's development and acquisition program test and evaluation events. While the primary focus of its efforts are to be test and

⁷ The Army's Mobile Subscriber Equipment provides secure voice telephone and data transmission to corps and below forces. All of its equipment is classified secret and all personnel operating on the network must have a secret security clearance.

evaluation events associated with FBCB2 and the Tactical Internet, the Army also plans to take advantage of other events to assess its information systems protection posture, including events associated with the Army Global Command and Control System, the Integrated Combat Service Support System, and the Warfighter Information Network. To date, however, the Army has not detailed the planned use of non-FBCB2 related development and test events. Table I.3 in appendix I lists the Army protection plan's phase III vulnerability assessment tasks with objectives, events, and responsible organizations.

The Army has already carried out some phase III activities. For example, information protection activities occurred as a part of both the FBCB2 Field Test 1 and the FBCB2 Limited User Test. As a part of the Field Test 1 held during May and June 1998,⁸ the Army subjected the FBCB2 and Tactical Internet to 2 nights of barrage jamming. Additionally, during the last 3 days of the field test, the Army's Program Manager for Information Warfare with the Army's Communications and Electronics Command conducted a Command and Control Protection Advanced Technology Demonstration that consisted of localized jamming and information warfare attacks. During the August 1998 FBCB2 Limited User Test, the Army also carried out some "red team" tasks⁹—mapping¹⁰ the Tactical Internet to gain an understanding of its architecture and possible weaknesses and analyzing digitized forces' susceptibility to signals intelligence efforts.

While the Army has already undertaken a number of activities laid out in its protection plan, much remains to be done as the Army's digitization efforts are to extend over the next decade and be implemented through the development, production, and fielding of over 100 individual systems. For

⁸ The FBCB2 Field Test 1 consisted of 61 FBCB2 systems spread across the Electronic Proving Ground's east range. Fourteen of the systems were on mobile platforms. Among its other limitations, the test did not involve as heavy a command and control message load as had been planned.

⁹ Many of the Army's "red team" tasks are other forms of vulnerability assessments, not "red teaming" as has been defined. For example, in discussing the FBCB2 Limited User Test information protection efforts, the Army official overseeing those efforts stated that it would be more accurate to call them "blue team" activities (i.e., friendly force efforts) because the individuals carrying them out were working to identify vulnerabilities and point them out to the "friendly" forces, not to exploit them.

¹⁰ Mapping involves sending out "requests for service" to try to determine the structure of the network; i.e., who can be identified as being on the Internet. Enemies would use mapping to try to define the structure of friendly networks and identify possible points of exploitation. Friendly forces would use mapping of their own networks to try to determine if unauthorized equipment or connections (which can serve as "back doors" for unauthorized access) are hooked up to the network.

example, the Army's report on its Field Test 1 information protection activities stated that FBCB2 and the Tactical Internet must undergo more extensive electronic and information warfare testing during upcoming FBCB2 test events, including Field Test 2, Force Development Test and Experimentation, and its Initial Operational Test and Evaluation. The report also stated that systematic electronic and information warfare test and evaluation of the other First Digitized Division systems and networks must be initiated and completed prior to fielding.

Detailed Implementation Plan Not Developed

While the Army has developed a general strategy for integrating information systems protection and has conducted a number of assessment activities, it lacks the specificity that would be contained in a detailed implementation plan. The Army's protection plan does not

- define the more than 100 systems that are a part of its overall digitization efforts;
- detail their specific information protection requirements, what is known or unknown about their individual vulnerabilities, or the specific test or other events to be used to fill identified knowledge gaps and ensure satisfactory resolution of previously identified weaknesses;
- define specific information protection aspects or issues to be tested during specific tests and events or who is responsible for carrying out and funding those specific activities; and
- identify the cost of specific protection plan activities or the parties responsible for funding those activities.

A detailed implementation plan that provides this information could help the Army identify test opportunities, address funding issues, and ensure that requirements are aligned with the goals and needs of its protection plans.

Identification of Test Opportunities and Funding Issues

Because its protection plan lacks sufficient implementation information, the Army could lose valuable testing opportunities. For example, during our review, we found that guidelines (in draft form as a security annex to the *Army Digitization Master Plan* of January 1999) that would charge involved parties with specific tasks contained no more information than the Army's overall protection plan itself. Specifically, the September 1997 Protection Plan and the security annex both state that follow-on assessments will be included in their next updates and that those assessment plans will address test and evaluation events such as the Maneuver Control System's Initial Operational Test and Evaluation, the

M1A2 (Abrams Tank) System Enhancement Program Initial Operational Test and Evaluation, the M2A3 (Bradley Fighting Vehicle) Initial Operational Test and Evaluation, and other events as appropriate. In June 1998 the Maneuver Control System¹¹ (MCS) Block III software underwent an initial operational test and evaluation, but that test was not used for protection plan activities. The opportunity to use this test for protection plan activities was lost because the Army's protection plan lacked sufficient implementation information including specific identification of activities to be carried out during that MCS test and because no such details were subsequently developed.

The Army's protection plan is based on an assumption that sufficient resources will be made available to implement a prudent amount of information systems protection in the first digitized division and beyond. As mentioned, however, the plan provides no funding details. Development of a detailed implementation plan could help the Army avoid funding shortfalls. For example, last year the Army's Test and Evaluation Management Agency put in a funding request for unfunded requirements of over \$6 million in fiscal year 1999 and \$7 million in each of fiscal years 2000 through 2006 for the Army's Survivability/Lethality Analysis Directorate (SLAD) to perform information warfare vulnerability assessments of digitized battlefield systems and related activities. The Army was unable to locate funds for those activities and included them on a list of unfunded requirements sent to Congress. Congress subsequently increased the SLAD's fiscal year 1999 budget for vulnerability assessments by \$4 million. These funding issues have not disappeared, however, as the unfunded requirement for fiscal year 2000 SLAD-led, information warfare vulnerability assessments and related activities has grown to \$10.2 million.

Ensuring Requirements Are Aligned With Plan's Goals and Needs

A detailed implementation plan could help the Army ensure that digitized battlefield systems have requirements that are aligned with its protection plan's goals and needs. Two key components of the Army's digitization efforts—the FBCB2 system and the Tactical Internet—have requirements that are not in line with the goals and needs of the Army's *Protection Plan for Army XXI Information Systems*. Specifically, the *Capstone*

¹¹ The MCS program is intended to develop and field a computer system that provides automated critical battlefield assistance to maneuver commanders and their battle staff at the corps-to-battalion level. MCS—a key component of the Army Tactical Command and Control System—is 1 of 16 systems considered to be critical elements within the Army's digitization effort because of the expected contribution they will make to achieve the required capabilities of the digitized battlefield.

*Requirements Document for the Tactical Internet*¹² sets an objective, not threshold, requirement for the “defense in depth” protection concept envisioned in the Army’s protection plan. The capstone requirements document states that a “threshold” value is the minimum acceptable value necessary to satisfy an operational need and that an “objective” value is the desired performance above that threshold.¹³

To be able to judge whether sufficient protection has been achieved, systems’ performance criteria need to be set and systems need to be judged for performance in the hostile environment in which they may need to operate. The capstone requirements document appropriately sets criteria for performance in a tactical environment that includes radio jamming, but the program most clearly tied to the Tactical Internet—FBCB2—has criteria set for performance in a non-jamming environment. Specifically, a key FBCB2 performance requirement, Information Exchange, has not been set to demonstrate attainment of a minimal level of performance in a jamming environment—a type of threat that the Army protection plan seeks to address.

The FBCB2 operational requirements document states that the requirement for Information Exchange, listed as a Key Performance Parameter¹⁴ for the system, is to provide a capability for the timely and reliable exchange of information between a sender and recipient. The document lists four categories of messages by type and assigns speed of service requirements for the transmission of those messages based on their type. For example, as a threshold value, 90 percent of category one messages sent—defined as Alerts and Warnings—are to be successfully received within 6 seconds.

¹² User requirements may be documented as capstone requirements, which are common systems’ requirements (such as overarching inter-operability requirements or standards) that apply to a family of systems.

¹³ Army Regulation 71-9 states that the “minimum acceptable value (threshold) requirements will be truly essential and minimum needs for successful operations and not desires or artificial contract or acquisition values.”

¹⁴ A key performance parameter is that capability or characteristic so significant that failure to meet the threshold can be cause for the concept or system selection to be reevaluated or the program to be reassessed or terminated.

It also includes, however, an assumption of no jamming for the defined “Information Exchange” requirements.¹⁵

Conclusions

The Army’s digitization efforts hold the promise of providing its fighting forces with operational improvements. However, they will also provide potential enemies new avenues of attack and greater opportunities to exploit existing vulnerabilities. Although, the Army has developed a general strategy for implementing systems protection into the design of the digitized battlefield, its plan lacks sufficient detail. Given the substantial digitization work that remains to be done (the integration of information technologies into over 100 systems), we believe a detailed implementation plan is needed to help ensure that the Army (a) fields a digitized force that can carry out its critical functions and operations and (b) is cognizant of any residual vulnerabilities—a factor that could prove important in recognizing enemy information system attacks. Furthermore, we believe such a plan could help ensure that sufficient funding, oversight, and effort are applied to developing the needed information protection. To be effective, the implementation plan should be a “living” document that will extend beyond the First Digitized Division and First Digitized Corps—a plan that is continually updated as circumstances dictate. We believe that the absence of such a plan places the substantial investment the Army is making in digitization at greater risk.

In addition to developing a detailed implementation plan, we believe the Army has further opportunities to enhance its information protection effort. The Army’s successful implementation of its “defense in depth” concept will depend, in part, on how well that concept is reflected in requirements placed on individual systems. In our opinion, the threshold Tactical Internet information protection requirement should be aligned to the Army protection plan concept, that is, Tactical Internet related systems should be required to support the development of the “defense in depth” called for in the Army protection plan. Also, to help ensure that the digitized forces that are fielded provide sufficient protection allowing critical functions and operations to continue, the Army needs to set minimum performance criteria for systems’ performance in such an environment, including setting minimum performance for FBCB2 in a jamming environment. We believe that setting such performance standards

¹⁵ The FBCB2 operational requirements document is not entirely clear, and the assumption of a no jamming environment may apply to other key performance parameters also.

will help ensure that systems that cannot carry out critical functions and operations when under attack are not fielded.

Recommendations

We recommend that the Secretary of Defense direct the Secretary of the Army to:

- Develop a detailed implementation plan for the Army's protection efforts for Army XXI information systems to include information such as a system by system breakout of tested and untested (known and unknown) areas of vulnerabilities; the specific test events to be used to look for systems vulnerabilities or to confirm fixes to previously identified, significant vulnerabilities; and responsible performing and funding parties.
- Require the Tactical Internet to have threshold information protection requirements consistent with the Army's "defense in depth" protection concept.
- Set performance requirements for and test FBCB2 in a jamming environment.

Agency Comments

DOD generally concurred with the recommendations contained in a draft of this report. DOD concurred with our first recommendation stating that the Army has already initiated an effort to develop a detailed implementation plan for its information protection activities. Regarding our second recommendation on tactical internet security, DOD generally concurred and stated that the Army will review requirements documents for all First Digitized Division systems to determine whether their security requirements are consistent with the Army's "defense in depth" concept. DOD generally concurred with our third recommendation, stating that the Army will revise performance requirements for FBCB2 to reflect performance in a jamming environment and will test in that environment. We believe that the actions outlined in DOD's response should enhance the Army's information protection efforts.

DOD's comments are reprinted in their entirety in appendix II.

Scope and Methodology

To evaluate the Army's protection plans to determine whether they ensure sufficient assessments to test and develop the defensibility of the digitized battlefield, we reviewed the Army's overall protection plans by analyzing

key Army information protection related documents (including the Army's *Protection Plan for Army XXI Information Systems* and its draft security annex for the *Army Digitization Master Plan*) and considering them in the context of the Army's larger digitization efforts. In evaluating the Army's near-term plans to develop and test its "defense in depth" protection concept, we reviewed its plans to use FBCB2 and Tactical Internet development and test events and examined key development and test documents for those efforts to determine whether their approach was in line with the Army's protection plan. We obtained briefings from and discussed issues with parties directly involved in the development and oversight of Army information protection efforts, program managers for high-priority digitization systems, and testers.

In the course of our work, we were briefed by and interviewed officials responsible for management and oversight of the Army's digitization-related information protection efforts; program managers for high-priority digitization systems; officials responsible for planning, carrying out, and overseeing system vulnerability assessments; and other Army and DOD representatives. We examined DOD and Army information protection documents, system requirements, test plans, and other program documents. We performed our work primarily with officials from the Army Office of the Director of Information Systems for Command, Control, Communications, and Computers. We also gathered data from the Army Communications-Electronics Command, Fort Monmouth, New Jersey; the Office of the Director, Operational Test and Evaluation, Alexandria, Virginia; the Army Training and Doctrine Command, Fort Monroe and Fort Eustis, Virginia; the Army Operational Test and Evaluation Command, Alexandria, Virginia; the Army National Training Center, Fort Irwin, California; the Army's Electronic Proving Ground, Fort Huachuca, Arizona; the Army Survivability/Lethality Directorate, Aberdeen Proving Grounds, Maryland; the Defense Information Systems Agency, Falls Church, Virginia; the Army Land Information Warfare Activity, Fort Belvoir, Virginia; and the 4th Infantry Division and 3rd Corps, Fort Hood, Texas.

We performed our review from July 1998 to July 1999 in accordance with generally accepted government auditing standards.

We are sending copies of this report to Representative John P. Murtha, Ranking Minority Member of the Subcommittee; Representative C.W. Bill Young, Chairman, and Representative David R. Obey, Ranking Minority Member, House Committee on Appropriations; and other interested

congressional committees. We are also sending copies of this report to the Honorable William S. Cohen, Secretary of Defense, and the Honorable Louis Caldera, Secretary of the Army. Copies will also be made available to others upon request.

Please contact me at (202) 512-4841 if you or your staff have any questions concerning this report. Key contributors to this assignment were Charles F. Rey, Bruce H. Thomas, and Gregory K. Harmon.

Sincerely yours,

A handwritten signature in black ink that reads "Allen Li". The signature is written in a cursive style with a large initial "A" and a stylized "L".

Allen Li
Associate Director
Defense Acquisitions Issues

Contents

| | | |
|---|--|----|
| Letter | | 1 |
| Appendix I Red Team Tasks | | 20 |
| Appendix II Comments From the Department of Defense | | 24 |
| Tables | Table I.1: Phase I (Task Force XXI) Red Team Tasks | 20 |
| | Table I.2: Phase II Division XXI AWE Red Team Tasks | 21 |
| | Table I.3: Planned Phase III Vulnerability Assessments During FBCB2 Test Events | 22 |
| Figures | Figure 1: Army's "Defense in Depth" Protection Concept | 6 |

Abbreviations

| | |
|----------|--|
| DOD | Department of Defense |
| FBCB2 | Force XXI Battle Command, Brigade and Below |
| EPLRS | Enhanced Position Location and Reporting System |
| SINCGARS | Single Channel Ground and Airborne Radio System |
| DISC4 | Director of Information Systems for Command, Control, Communications, and Computers |
| AWE | Advanced Warfighting Experiment |
| MCS | Maneuver Control System |
| SLAD | Survivability /Lethality Analysis Directorate |

Contents

Red Team Tasks

Table I.1: Phase I (Task Force XXI) Red Team Tasks

| Red Team task | Objective | Location | Dates |
|---|--|--|------------------------|
| • Position/navigation vulnerability assessment | To determine the impact of loss of Global Positioning System signal on the Task Force information network | Fort Huachuca, AZ Fort Huachuca, AZ | Apr. 1996 Dec. 1996 |
| • Hacker/virus vulnerability assessment | To determine the vulnerability of the Task Force information network to hacker, virus, and other non-traditional threats | Fort Hood, TX Fort Irwin, CA | Dec. 1996 Mar. 1997 |
| • Operations security evaluation | To determine new/increased operational security vulnerabilities due to digitization of the battlefield | Fort Hood, TX Fort Irwin, CA | Dec. 96 Mar. 97 |
| • Signal intelligence/ measurement and signatures intelligence characterization | To determine unique pattern and signatures of the digitized force | Fort Hood, TX Fort Irwin, CA | Dec. 1996 Mar. 1997 |
| • Security policy evaluation | To assess the needs for revised and/or additional security policy due to digitization | Fort Hood, TX Ft. Irwin, CA | Dec. 1996 Mar. 1997 |
| • Tactical Internet components vulnerability assessment | To determine unique vulnerabilities of the individual systems comprising the Tactical Internet (e.g., SINGARS and EPLRS) | Fort Monmouth, NJ Fort Monmouth, NJ | June 1996 Nov. 1996 |

Source: U. S. Army, Protection Plan for Army XXI Information Systems.

**Appendix I
Red Team Tasks**

Table I.2: Phase II Division XXI AWE Red Team Tasks

| Red Team task | Objective | Location | Dates |
|--|---|-------------------------------------|-------------------------|
| • Electronic warfare | To determine the impact of loss of selected communication links on the Division XXI AWE experimentation information network | Simulation Exercise II Fort Hood | Sept. 1997 Nov. 1997 |
| • Operations security evaluation | To determine new/increased operational security vulnerabilities due to digitization of the battlefield | Fort Hood | Nov. 1997 |
| • Computer attack vulnerability assessments | To detect exploitable vulnerabilities of attacks from both outside and inside the Division XXI AWE information network | Simulation Exercise II Fort Hood | Sept. 1997 Nov. 1997 |
| • Capture/exploitation of the mobile subscriber equipment node | To determine vulnerabilities to the Mobile Subscriber Equipment network resulting from capture of Small Extension Node | Fort Hood | Nov. 1997 |
| • Measurement and signatures intelligence characterization | To determine unique patterns and signatures of the digitized force | Fort Hood | Nov. 1997 |

Source: U. S. Army, Protection Plan for Army XXI Information Systems.

**Appendix I
Red Team Tasks**

Table I.3: Planned Phase III Vulnerability Assessments During FBCB2 Test Events

| Red Team task | Objective | Event | Responsible organization |
|---|--|---|--|
| System assessments | To assess performance of individual systems to electronic warfare and command and control attack and characterize their signatures | | |
| • Electronic attack | To assess vulnerabilities of new communication systems to jamming | Laboratory assessments of Near Term Digital Radio, High Capacity Trunk Radio, and others as required | PM TRCS/CECOM |
| • Computer attack | To assess vulnerability of Army Tactical Command and Control System component systems to command and control attack | Vulnerability assessments of FBCB2, Maneuver Control System, other command and control systems | <ul style="list-style-type: none"> • PM Applique • PM ATCCS • Other PMs • SLAD |
| Technical Network assessment | To assess the vulnerabilities of the network to attack and characterization in a controlled environment | | |
| • Electronic attack | To assess vulnerability of battalion- and brigade-level communication systems/networks to jamming | <ul style="list-style-type: none"> • Field Test I • Field Test II | EPG |
| • Computer attack | To assess vulnerability of information and Command and Control systems to attack | <ul style="list-style-type: none"> • Laboratory and testbed assessments • Field Test I • Field Test II | PM IW/SLAD |
| • Characterization | To assess the ability to identify friendly nodes through unique signatures | Laboratories | CECOM/SLAD/INSCOM/EPG |
| Operational network assessment | To assess the vulnerabilities of the network to attack and characterization in an operational environment | | |
| • Electronic warfare attack | To assess vulnerability of battalion- and brigade-level communication systems/networks to near-peer live electronic warfare attack | IOT&E | OPTEC/SLAD/PM IW |
| • Command and control attack | To assess vulnerability of information and Command and Control systems to live attack culminating in a full-up near-peer computer attack during IOTE | <ul style="list-style-type: none"> • Limited User Test • FDT&E • IOT&E | OPTEC/LIWA/PM IW/SLAD |
| • Characterization | To assess the ability to identify friendly nodes through unique signatures in an operational setting | Limited User Test | CECOM/INSCOM |
| • Operations security/computer security | To assess operational and computer security procedures and training | <ul style="list-style-type: none"> • Limited User Test • FDT&E • IOT&E | INSCOM |

Appendix I
Red Team Tasks

Legend:

| | |
|--------|---|
| ATCCS | Army Tactical Command and Control System |
| CECOM | Communications and Electronics Command |
| EPG | Electronic Proving Ground |
| FDT&E | Force Development Test and Experimentation |
| INSCOM | Intelligence and Security Command |
| IOT&E | Initial Operational Test and Evaluation |
| IW | Information Warfare |
| OPTEC | Operational Test and Evaluation Command |
| PM | Program Manager, Product Manager, Project Manager |
| LIWA | Land Information Warfare Activity |
| SLAD | Survivability/Lethality Analysis Directorate |
| TRCS | Tactical Radio Communications Systems |

Source: U. S. Army, Protection Plan for Army XXI Information Systems.

Comments From the Department of Defense



OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

July 22, 1999

Mr. Allen Li
Associate Director, Defense Acquisition Issues
National Security and International Affairs Division
U.S. General Accounting Office
Washington, D.C. 20548

Dear Mr. Li:

This is the Department of Defense (DoD) response to the General Accounting Office (GAO) draft report, "BATTLEFIELD AUTOMATION: Opportunities to Improve the Army's Information Protection Effort," dated June 18, 1999 (GAO Code 707347/OSD Case 1847).

The Department generally concurs with the report and its recommendations. DoD strongly supports increased efforts in protection of our critical battlefield information and command and control systems. DoD concurs that the Army's Information Protection Plan should be more detailed and that its critical information systems should be operationally tested in a hostile information warfare environment.

The Army has already taken action to address several of the issues presented in this draft report. They have recently initiated a revision to the 1997 Protection Plan for Army XXI Information systems that will encompass planned vulnerability assessments, red teaming events, and specific test events. The plan will focus on security evaluations of the network architecture, individual systems, and system of systems.

The Army is also reviewing their Operational Requirements Documents (ORD) to determine whether information warfare security requirements are documented and consistent with their stated "defense in depth" strategy. Finally, the Army is addressing the identified concerns in regard to testing information systems in an electronically "hostile environment" and is adjusting system evaluations appropriately.

The Department appreciates the opportunity to comment on the GAO draft report. Detailed comments on the report's recommendations are enclosed.

Sincerely,



Arthur L. Money
Senior Civilian Official

Attachment



GAO DRAFT REPORT DATED JUNE 18, 1999
(GAO CODE 707347) OSD CASE 1847

**“BATTLEFIELD AUTOMATION: OPPORTUNITIES TO IMPROVE THE
ARMY’S INFORMATION PROTECTION EFFORT”**

**DEPARTMENT OF THE DEFENSE COMMENTS
TO THE GAO RECOMMENDATIONS**

RECOMMENDATION 1: Develop a detailed implementation plan for the Army’s protection efforts for Army XXI information system to include information such as a system by system breakout of tested and untested (known and unknown) areas of vulnerabilities; the specific test events to be used to look for system vulnerabilities or to confirm fixes to previously identified, significant vulnerabilities; and responsible performing and funding parties. (p.15 draft report)

Now on p. 14.

DoD RESPONSE: Concur. The Department agrees that the Army needs to revise their information protection plan. The Army has already initiated efforts in this regard. The next revision of the Protection Plan for Army XXI Information Systems is planned to be completed NLT January 2000.. This update will encompass vulnerability assessments, red teaming events, and operational unit information operation assessments of the key events leading up to the fielding of the digitized force. The plan will focus on security evaluations of the network backbone architecture, individual systems, and system of systems. The end product for these security evaluations will include a system assessment test report consisting of a prioritized list of vulnerabilities, recommended solutions for material (SW/HW) fixes or mitigating procedures, and the development of a rectification plan for implementation based on the validated threat. A comprehensive review of previously tested individual system and system of system vulnerabilities will be conducted and action will be taken to verify system fixes.

Now on p. 14.

RECOMMENDATION 2: Require the Tactical Internet to have threshold information protection requirements consistent with the Army’s “defense in depth” protection concept. (p. 15 draft report)

DOD RESPONSE: Generally concur. The Army is conducting reviews of Operational Requirements Documents (ORD) for all FDD (First Digitized Division) systems, to include the Tactical Internet (TI) Capstone Requirements Document (CRD), to determine whether security requirements are documented and consistent with the “defense in depth concept” as stated in the aforementioned Army Protection Plan. The Army will revise the TI CRD as necessary. Additional reviews of Army security regulations will be conducted to ensure that the appropriate security standards are met during the certification and accreditation process of Army information systems and weapons platforms.

Now on p. 14.

RECOMMENDATION 3: Set performance requirements for and test FBCB2 in a jamming environment. (p. 15 draft report)

DOD RESPONSE: Generally concur. The Army will revise performance requirements for FBCB2 to reflect performance in a jamming environment. The Army will conduct additional FBCB2 system tests in a jamming environment in accordance with the revised performance requirements. These planned test events will be documented in the aforementioned revised Army Protection Plan.

Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are \$2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary, VISA and MasterCard credit cards are accepted, also.

Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:

**U.S. General Accounting Office
P.O. Box 37050
Washington, DC 20013**

or visit:

**Room 1100
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC**

**Orders may also be placed by calling (202) 512-6000
or by using fax number (202) 512-6061, or TDD (202) 512-2537.**

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

For information on how to access GAO reports on the INTERNET, send an e-mail message with "info" in the body to:

info@www.gao.gov

or visit GAO's World Wide Web Home Page at:

<http://www.gao.gov>

**United States
General Accounting Office
Washington, D.C. 20548-0001**

**Official Business
Penalty for Private Use \$300**

Address Correction Requested

| |
|---|
| <p>Bulk Rate Postage & Fees Paid GAO Permit No. GI00</p> |
|---|

