

September 2002

NATIONAL GUARD

Effective Management
Processes Needed for
Wide-Area Network





NATIONAL GUARD

Effective Management Processes Needed for Wide-Area Network

Highlights of [GAO-02-959](#), a report to the Committees on Armed Services, U.S. Senate and House of Representatives.

Why GAO Did This Study

The Fiscal Year 2002 Defense Authorization Act required GAO to review GuardNet, the National Guard's wide-area network, which is used to support various Defense applications and was used to support homeland security activities after the terrorist attacks of September 11th. GAO was asked to determine the current and potential requirements for GuardNet and the effectiveness of the processes for managing the network's requirements, configuration, and security.

What GAO Recommends

GAO is making numerous recommendations aimed at (1) limiting network users' current exposure to risk; (2) understanding and evaluating the network's current requirements, configuration, and security posture; and (3) developing and implementing action plans to address current network weaknesses and risks. The Department of Defense generally agreed with our recommendations, stating that they were valued and timely.

What GAO Found

The National Guard does not fully know the current or potential requirements for GuardNet or how it is being used, because it has not fully documented requirements. Guard officials provided GAO with a list of applications that the network supports, but they would not attest to the list's completeness, and GuardNet users identified other applications.

The processes for managing GuardNet are not effective in three key areas:

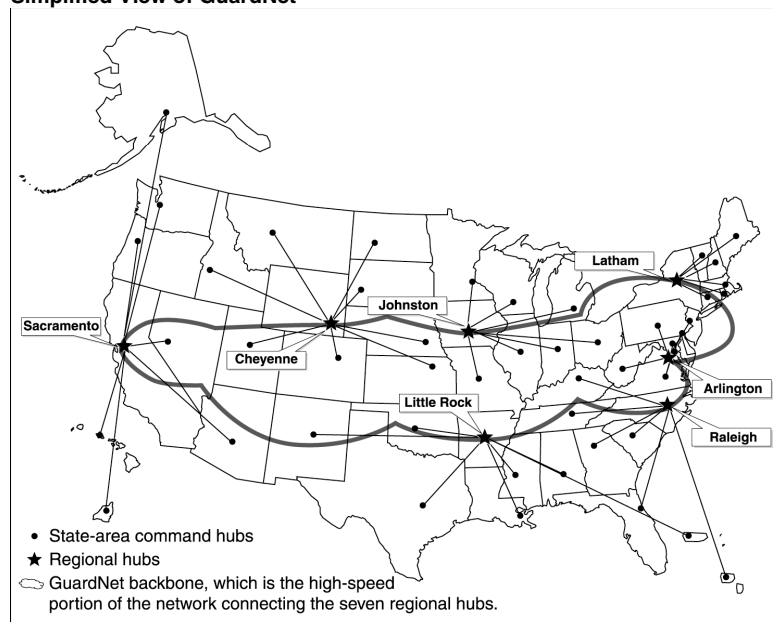
Requirements. For example, the Guard has not developed a requirements management plan or clearly established users' roles in developing and changing requirements.

Configuration. For example, the Guard has not documented the network's configuration and is not controlling changes to configuration components.

Security. For example, the Guard has not implemented needed security controls, such as firewalls, to protect GuardNet and does not monitor controls on an ongoing basis to ensure that implemented controls are working as intended.

According to Guard officials, establishing these management processes has not been a priority. Without these basic processes, the Guard cannot ensure that GuardNet will perform as intended and provide its users with reliable and secure services. GuardNet is thus a dubious option for further support of critical mission areas such as homeland security.

Simplified View of GuardNet



Source: National Guard.

Contents

Letter		1
	Results in Brief	2
	Background	4
	Current and Potential Requirements of GuardNet Are Not Fully Known	13
	NGB Does Not Have an Effective Process for Managing GuardNet Requirements	16
	NGB Does Not Have an Effective Process for Managing GuardNet's Configuration	18
	NGB Does Not Have an Effective Process for Managing GuardNet's Security	20
	Conclusions	25
	Recommendations for Executive Action	26
	Agency Comments and Our Evaluation	28

Appendixes

Appendix I: Objectives, Scope, and Methodology	30
Appendix II: Comments from the National Guard	33
Appendix III: GAO Contact and Staff Acknowledgments	37
GAO Contact	37
Staff Acknowledgments	37

Table	Table 1: Summary of GuardNet Management Responsibilities and Functions	12
-------	--	----

Figures	Figure 1: Federalized National Guard Organization/Command Structure	6
	Figure 2: Nonfederal National Guard Organization/Command Structure	7
	Figure 3: Simplified Diagram of GuardNet and Its Interconnections	9
	Figure 4: Simplified View of GuardNet	11

Abbreviations

AIS	Information Systems Division
CCB	Configuration Control Board
CIO	chief information officer
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CMMI	Capability Maturity Model Integration
DISA	Defense Information Systems Agency
DITSCAP	DOD Information Technology Security Certification and Accreditation Process
DLA	Defense Logistics Agency
DOD	Department of Defense
DODD	Department of Defense Directive
DTTP	Distributive Training Technology Project
EIA	Electronic Industries Alliance
IEEE	Institute of Electrical and Electronics Engineers
IT	information technology
NGB	National Guard Bureau
NIPRNet	Unclassified but sensitive Internet Protocol Router Network
OMB	Office of Management and Budget
SEI	Software Engineering Institute
VTC	video teleconferencing
WAN	wide-area network



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

September 24, 2002

The Honorable Carl Levin
Chairman
The Honorable John Warner
Ranking Minority Member
Committee on Armed Services
United States Senate

The Honorable Bob Stump
Chairman
The Honorable Ike Skelton
Ranking Minority Member
Committee on Armed Services
House of Representatives

Although established to support Web-based training for National Guard units in the states, the U.S. territories, and the District of Columbia, GuardNet,¹ which is the National Guard Bureau's (NGB) wide-area network, has recently been used to support homeland security activities. For example, when faced with overloaded public telecommunications systems and limited radio communications on September 11, 2001, both New York Army National Guard units and civilian emergency authorities relied on GuardNet to perform command and control functions. Since then, the Guard has used this network to coordinate airport security activities, inform the public about anthrax, and coordinate with first responders.² According to Guard and Department of Defense officials, additional homeland-security-related uses of GuardNet are currently being considered.

¹Over the years, the network has been called the Distance Learning Network, the Distributive Training Technology Project (DTTP) network, and GuardNet XXI. For the purposes of this report, the network is referred to as "GuardNet." DTTP is used when we refer specifically to the National Guard's distance learning program.

²"First responders" refers to emergency personnel, such as local police, firefighters, and medical professionals.

The Fiscal Year 2002 Defense Authorization Act requires the Comptroller General to review GuardNet, including its requirements and its interconnectivity with other networks.³ As agreed with your offices, our objectives were to determine (1) the network's current and potential requirements and (2) the effectiveness of NGB's processes for managing network requirements, configuration,⁴ and security. (See app. I for more details on our objectives, scope, and methodology.)

Results in Brief

NGB does not have basic requirements documentation for GuardNet and, as a result, does not fully know its current and potential requirements. Instead, NGB officials told us what they characterized as their understanding of the existing and potential uses of GuardNet, but not the associated requirements that GuardNet needed to fulfill to support network users. Further, while NGB officials stated that future uses of GuardNet could include support to the homeland security mission, including wireless communications, they had no further specifics. Without a basic understanding of current and potential network requirements, NGB lacks the requisite information for meeting network users' needs and making informed network investment decisions.

NGB's lack of understanding of GuardNet's requirements is attributable in part to the ineffectiveness of its processes for managing network requirements, configuration, and security. In each of these important areas, NGB has not adhered to the proven practices that successful public- and private-sector organizations employ in managing their systems, and it has not followed relevant Department of Defense (DOD) policies and guidance. For example, NGB does not have a requirements management plan, a requirements baseline against which changes are controlled, or a systematic way to capture and evaluate proposed changes. NGB also does not have a configuration management plan or documentation describing the network's current configuration and changes that have been made to the configuration. In addition, NGB has not periodically assessed network security risks and has not implemented appropriate security controls, such

³Fiscal Year 2002 Defense Authorization Act, Public Law 107-107, Section 363.

⁴"Network configuration" refers to the hardware and software items that comprise the network.

as operational firewalls,⁵ to address risks that it has identified. According to NGB officials, establishing effective management processes has not been a bureau priority. Without these basic process controls, NGB has inadequate assurance that GuardNet will perform as intended and provide its users with reliable and secure services. This raises questions about the network's near-term viability as a communication option for mission-critical applications, such as homeland security.

In light of the significance of known and potential uses of GuardNet, as well as the extent of NGB management weaknesses, we are recommending that the Secretary of Defense, through the Secretary of the Army, direct the NGB Chief to take a series of actions aimed at (1) limiting network users' current exposure to risk; (2) understanding and evaluating the network's current requirements, configuration, and security posture; and (3) developing and implementing specific plans to appropriately address current network weaknesses and risks.

In written comments on a draft of this report, DOD thanked us for our timely assessment and valued recommendations, and it stated that NGB has begun to address the deficiencies cited in our report and would use our recommendations as a tool in enhancing GuardNet service delivery.

The department nevertheless disagreed with one aspect of one of our recommendations, which we have addressed through a wording clarification. It also disagreed with our recommendation for NGB to develop a plan for putting in place missing network security management process controls. While not challenging our finding that these process controls were missing, DOD stated that a plan for improving its current state of security management was not needed because NGB continually addresses security requirements but has been unable to fund them. We disagree that a plan is not needed. The improvement plan that we recommend provides for establishing the processes necessary to understand and prioritize security needs and ensure that they are effectively met. In addition, its implementation will not only place NGB in a better position for overcoming each of the security weaknesses discussed in the report, it will also help it justify its funding needs.

⁵Network firewalls are devices or systems that control the flow of traffic between networks with different security requirements. Organizations employ firewalls in an attempt to prevent unauthorized access to the respective systems and resources within the more sensitive areas.

Background

The National Guard consists of the National Guard Bureau (NGB)—which includes the Army National Guard and the Air National Guard—and the National Guard units, which are located in the 50 states, 3 U.S. territories,⁶ and the District of Columbia. The National Guard has played a critical role in a variety of crises in the recent past. For example, in 1999, the North Carolina National Guard unit assisted for more than 50 consecutive days during the aftermath of Hurricanes Floyd and Dennis. Also, within hours of the September 11, 2001, attacks on the World Trade Center and the Pentagon, 52 Air National Guard units were in the air over the United States, transporting medical supplies and personnel from emergency support organizations. By September 13th, nearly 3,800 members of the New York National Guard, and about 1,200 members of the Virginia, Maryland, and District of Columbia National Guard, were mobilized and on duty.

In executing its role in these crises, the Guard depends on a wide variety of assets, including a network, commonly referred to as GuardNet, which is to provide real-time, interactive, Web-based communications. According to NGB officials, GuardNet is a collection of 55 wide-area networks (WAN)⁷ that link 2,700 armories⁸ and other facilities, such as colleges and universities, around the country.

National Guard: Its Mission and Organization

The National Guard has both a federal and a state-level mission, making it unique among U.S. military organizations. Its federal mission is to (1) maintain well-trained and well-equipped units that are ready to be mobilized by the President of the United States during war or international peacekeeping efforts and (2) provide assistance during *national emergencies*, such as natural disasters or civil disturbances. In this role, the Guard is a supplemental reserve force for the Army and the Air Force. Its state-level mission, which is executed under the control of state and territory governors and, for the District of Columbia, the President, is to protect life and property and preserve peace, order, and public safety. This

⁶The three territories are Guam, Puerto Rico, and the U.S. Virgin Islands.

⁷A wide-area network is a network that provides data communications to a large number of independent users and spans a relatively large geographical area.

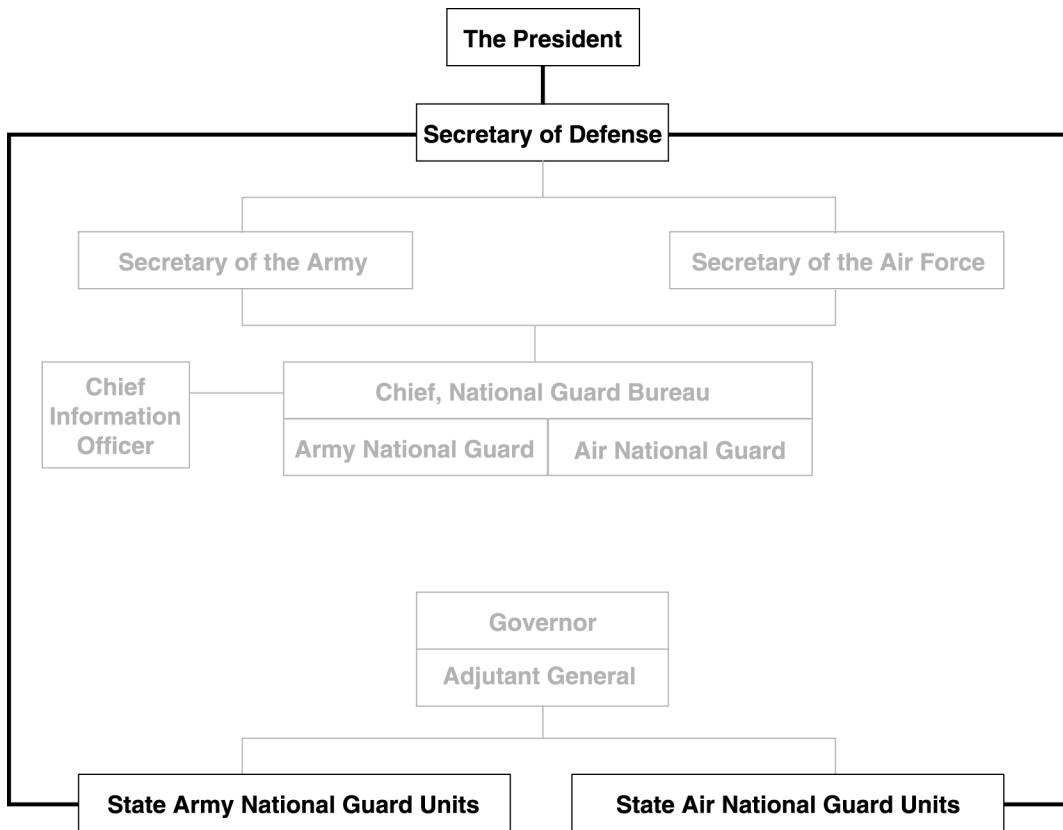
⁸Armories are buildings where one or more National Guard units may be housed and where training is conducted.

mission involves providing emergency relief support during *local* or *statewide emergencies*, such as riots, earthquakes, floods, or terrorist attacks.

The Army and Air National Guard units are located at 3,472 sites throughout the 50 states, 3 territories, and the District of Columbia. According to the Department of the Army, the Army National Guard is one of three force components of the department, with the other two being active duty Army forces and the Army Reserves. The Army National Guard comprises military and civilian personnel who serve their country on either a full- or part-time basis; it has about 350,000 soldiers in 1,832 units. Currently, about half of these are combat units. The Air National Guard is a reserve component of the Department of the Air Force, employing about 107,000 officers and airmen in 368 units. The Air National Guard supports the Air Force in its mission of providing air defense for the United States and provides airlift, combat communications, and aerial refueling support to the Air Force.

Structurally, NGB (the Army National Guard and the Air National Guard) is positioned between the state-level Guard units and the Departments of the Army and Air Force for communication purposes. During war or other national emergencies, the President can mobilize state-level Guard units as federal troops. When federalized, these units report to the Secretary of Defense (see fig. 1). Currently, about 9 percent of the Army National Guard's units and 24 percent of the Air National Guard's units are federalized.

Figure 1: Federalized National Guard Organization/Command Structure



Notes:

When deployed *within* the United States, National Guard units report to an active Army or Air Force component, which reports to the Secretary of the Army or Air Force, respectively, who reports to the Secretary of Defense.

When deployed *outside* of the United States, National Guard units report to the Secretary of Defense through their respective Theater Commanders-in-Chief, each of whom is responsible for combatant forces in one of seven geographical areas.

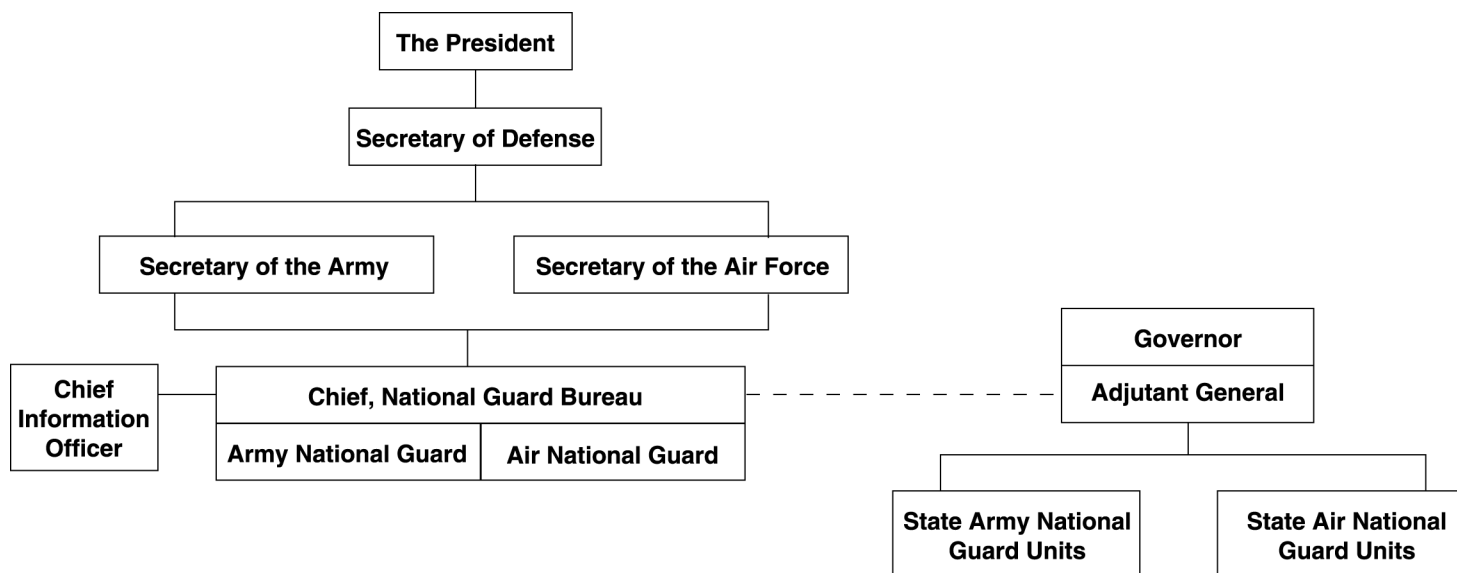
Source: NGB.

When performing their state-level mission, Guard units within a state, territory, or the District of Columbia report to a state-level commanding officer known as the Adjutant General,⁹ who in turn reports to either a state

⁹For the District of Columbia, this commanding officer is referred to as the “Commanding General.”

or territorial governor or, for the District, the President (as commanders-in-chief). The Adjutant General coordinates with NGB's Army or Air National Guard, as appropriate, on such matters as staffing and unit readiness. The Army and Air National Guard in turn coordinate with the Secretaries of the Army and the Air Force, respectively. (See fig. 2 for the organizational/command structure of the Guard when it is performing its state-level mission.)

Figure 2: Nonfederal National Guard Organization/Command Structure



Source: NGB.

GuardNet: A Brief Description

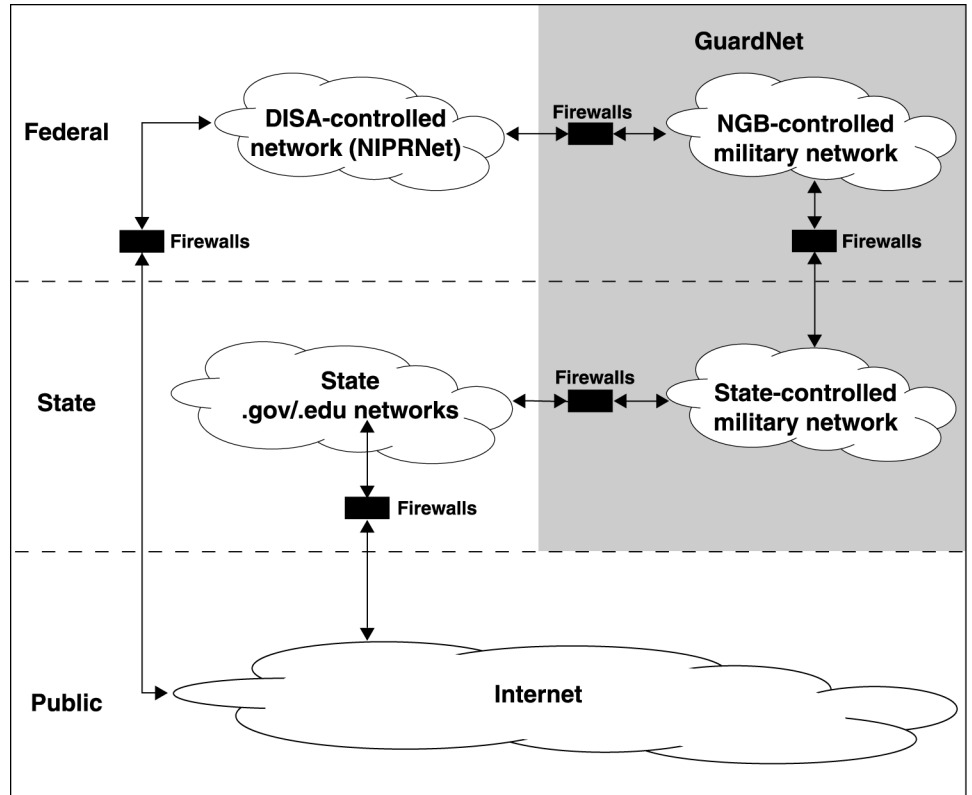
GuardNet is a WAN that bridges the military and civilian sectors, just as the National Guard itself does. GuardNet was created to support NGB's Distributive Training Technology Project (DTTP), a distance learning program established by Congress in 1995 to ensure enhanced military readiness and improve command, control, and communications for the Guard. According to NGB, GuardNet became operational in 1998.

GuardNet is a network of interconnected federal and state military networks (both wide-area and local-area) across the United States (see fig. 3). Through GuardNet, states, territories, and the District of Columbia can connect to a defense network operated by the Defense Information

Systems Agency (DISA),¹⁰ and through this network to the Internet. In addition, some states and territories have established connections to other state networks, such as local-area networks on university campuses, which also allow access to the Internet. According to NGB officials, firewalls exist at connections between the federally controlled and state-controlled portions of GuardNet, between the federally controlled portion of GuardNet and DISA's network, and between DISA's network and the Internet. In addition, these officials stated that while they were not certain about the presence of firewalls between the state-controlled portions of GuardNet and the state networks, approximately one-half of the states, on their own initiative, might have implemented these firewalls, since NGB has yet to do so.

¹⁰This DISA-controlled network is called the "Unclassified but sensitive Internet Protocol Router Network" (NIPRNet).

Figure 3: Simplified Diagram of GuardNet and Its Interconnections



Legend:

DISA = Defense Information Systems Agency

NIPRNet = Unclassified but sensitive Internet Protocol Router Network

Source: GAO on the basis of NGB information.

GuardNet comprises 7 regional hubs,¹¹ each of which connects to between 6 and 8 “state-area command” hubs within the 50 states, 3 territories, and the District of Columbia (see fig. 4). The seven regional hubs are located in Sacramento, California; Cheyenne, Wyoming; Johnston, Iowa; Latham, New York; Raleigh, North Carolina; Little Rock, Arkansas; and the Army National Guard Readiness Center in Arlington, Virginia. The backbone

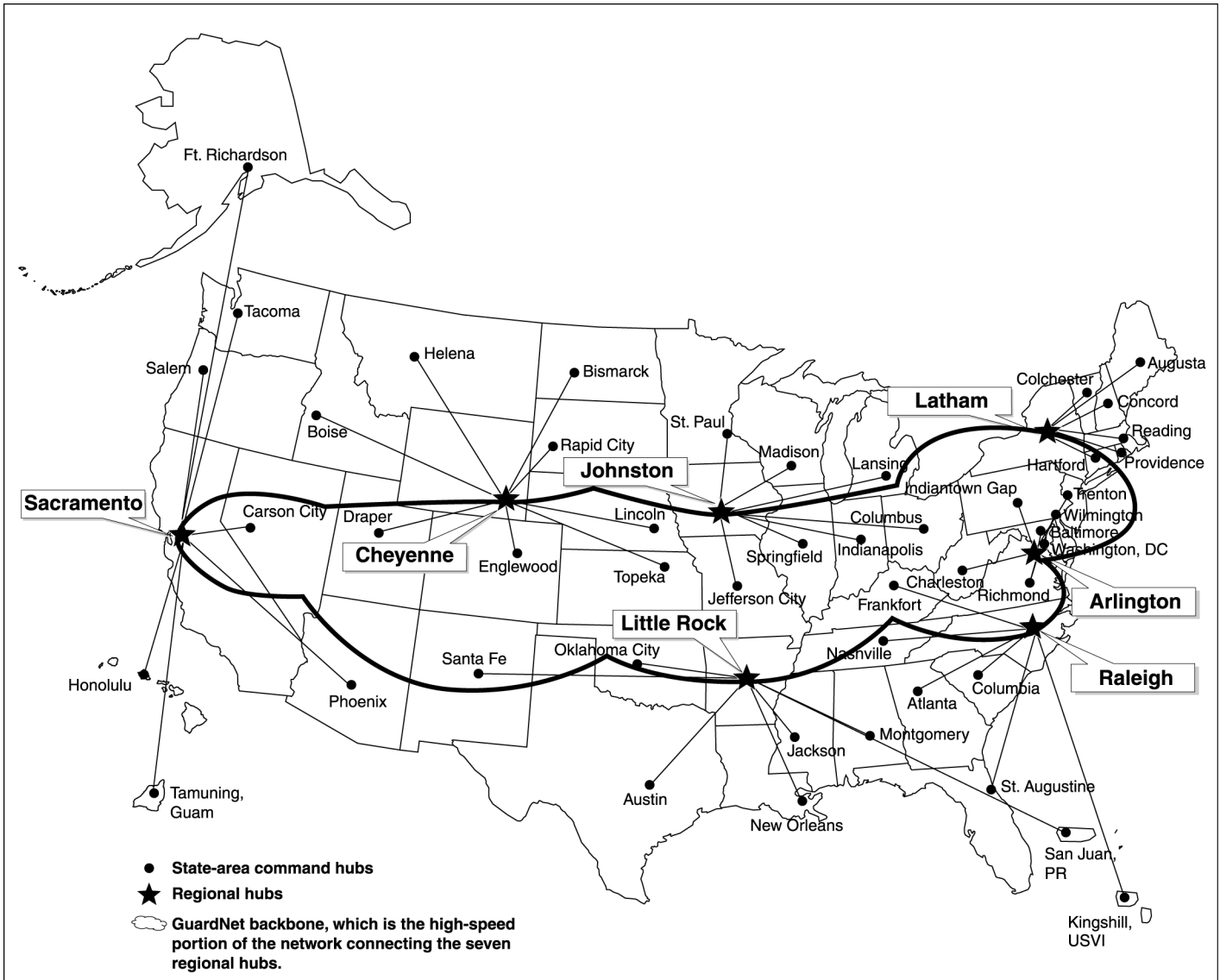
¹¹Hubs are common connection points for devices in a network. They accept signals from one point and redistribute them to other points in the network.

connections among the regional hubs are either OC-3 or T-3 lines,¹² both of which are dedicated telecommunications lines that support voice, video, and data transmissions. The connections between the regional hubs and the state-area command hubs are primarily T-1 lines.¹³ From the state-area command hubs, leased T-1 lines provide permanent telephone connections to the DTTP classrooms and local-area networks located at, for example, universities and Guard armories.

¹²OC-3 and T-3 are used to designate a telecommunications line that can transmit voice and data information at the rate of approximately 155 million bits per second and 45 million bits per second, respectively, in each direction.

¹³T-1 is used to designate a telecommunications line that transmits voice and data information at the rate of approximately 1.5 million bits per second in each direction.

Figure 4: Simplified View of GuardNet



Source: NGB.

According to NGB, the Army National Guard provides the funding for GuardNet. However, GuardNet management is a shared responsibility between NGB at the federal level and directors of information

management¹⁴ at the state level. The Air National Guard does not have any management responsibilities for GuardNet. These respective roles and responsibilities are described in table 1.

Table 1: Summary of GuardNet Management Responsibilities and Functions

Entity	Responsibility/Function
Federal level	
NGB Chief Information Officer (CIO)	Serves as the senior information technology (IT) advisor to the NGB Chief.
NGB CIO Executive Council	Provides a forum to improve NGB's IT management practices.
NGB Information Systems Division (NGB-AIS) ^a	Operates and maintains GuardNet.
AIS Configuration Control Board	Reviews and approves network change requests for GuardNet.
Army National Guard Systems Engineering Integration Group	Reviews and provides technical guidance to the NGB-AIS Configuration Control Board on change requests.
IT Requirements Control Board	Reviews and approves IT requirements with estimated life-cycle costs over \$100,000.
External Connection Review Board	Reviews requests for external connections to GuardNet.
State level	
Information Management Council	Communicates state-level concerns regarding pending network changes.
Director of Information Management/Deputy Chief of Staff for Information Management	Operates and maintains state-controlled portion of GuardNet, including managing network changes and security.

^aAccording to NGB officials, AIS refers to the Information Systems Division.

Source: NGB.

¹⁴States, territories, and the District of Columbia have either a Director of Information Management, a Deputy Chief of Staff for Information Management, or both. These individuals have similar responsibilities.

Current and Potential Requirements of GuardNet Are Not Fully Known

Industry best practices¹⁵ and DOD guidance¹⁶ recognize the importance of clearly and formally defining system requirements. For example, DOD guidance requires the development of (1) a mission needs statement, which defines current and future high-level operational capabilities that a system must provide to meet mission needs, and (2) an operational requirements document, which translates these high-level capabilities into detailed and unambiguous functional (what the system is to do), performance (how well it is to do it), and interface (how it is to interact with other systems) requirements. Without this basic requirements documentation, system owners are not in a position to deliver systems that meet users' needs, evaluate system performance, or make informed decisions about system changes.

NGB has neither a mission needs statement nor an operational requirements document for GuardNet. According to officials of NGB's Information Systems (AIS) Division, while a comprehensive and authoritative set of requirements for GuardNet does not exist, the bureau has a "fairly good" informal understanding of how the network is currently being used. However, we did not find evidence that such an understanding exists. For example, although the officials initially attributed their understanding of the network's use to memorandums of agreement between NGB and the states, territories, and the District of Columbia, they subsequently stated that the memorandums do not currently exist, but they should in the near future. In addition, while they provided us with a list of 130 DOD and bureau applications that GuardNet supports, they did not know whether this list was complete, and other sources of information suggest that the list is not complete. For example, NGB's fiscal year 2003 funding request states that the network supports 135 applications.

¹⁵See, for example, Institute of Electrical and Electronics Engineers (IEEE), *Standard for Application and Management of the Systems Engineering Process* (IEEE Standard 1220-1998, Jan. 22, 1999); and the Software Engineering Institute (SEI), *Capability Maturity Model Integration* (CMMI), Version 1.1 (March 2002).

¹⁶Chairman of the Joint Chiefs of Staff Instruction: *Requirements Generation System* (CJCSI-3170.01b, Apr. 15, 2001).

In the absence of basic requirements documentation, we reviewed NGB expenditure and budget documents relating to the operation and maintenance of the network in an attempt to trace funding back to requirements. However, these budget documents related funding needs to very generic requirements, such as “security” or “network maintenance,” and according to NGB-AIS officials, the funding levels were not based on specific requirements but rather on prior year funding levels. Since fiscal year 1997, NGB estimates that its cumulative spending on GuardNet is between \$172 million and \$451 million.¹⁷

In addition, because NGB-AIS officials do not compare actual performance to performance expectations (i.e., requirements), we could not determine GuardNet requirements by reviewing such performance analyses. The bureau provided the results of an ongoing study commissioned by NGB’s Chief Information Officer (CIO) to identify future network requirements in support of homeland security command, control, and communications activities.¹⁸ However, the results to date do not yet identify GuardNet requirements. Instead, these results raised states’ concerns about network security and reliability and interoperability with other networks, all of which the states currently deemed inadequate.¹⁹ According to a Guard official for Iowa, the state uses its own network, instead of GuardNet, for video conferencing (VTC) because it is more reliable and faster.

Because of states’ concerns about GuardNet’s capabilities, we attempted to interview Virginia and Iowa state officials using GuardNet’s VTC facilities. To accomplish this, we requested that these interviews be conducted at a site that was used for VTC purposes by the Army National Guard and others following the September 11th terrorist attacks, specifically asking that GuardNet be used to establish both the voice and video connection. We experienced difficulties in getting this connection and using the VTC capabilities at this facility. For example, in connecting with Virginia officials, it took four attempts to establish the initial video connection, which lasted about 15 minutes before communications were lost

¹⁷Data on the bureau’s spending on GuardNet for fiscal years 1995 and 1996 were not available.

¹⁸*C3 Requirements Definition: Using DTTP and GuardNet XXI in Support of the National Guard C3 Mission*, requirements document-report to the CIO, NGB. (Feb. 14, 2002).

¹⁹The states that participated in this study were California, Iowa, Louisiana, New Jersey, New York, Oklahoma, Pennsylvania, Texas, Virginia, and Washington.

altogether; a voice connection was never established. As a result, we communicated with Virginia officials using a telephone. In the case of Iowa, a connection was established; however, the quality of both the video and voice connections was poor. For example, the screen froze several times during the meeting and, at times, it was difficult to hear the Iowa officials. After receiving a draft of this report for comment, the Acting Director of NGB's Information Systems Division informed us that the public switched network was used to connect us with the states, not GuardNet. To verify this, we requested copies of error logs that document problems associated with the network's usage. However, NGB did not provide us the logs. Further, the NGB official who established our connection with Virginia and Iowa told us that we had used GuardNet, as did a Virginia official. Two other Virginia officials, however, stated that we had not used GuardNet.

In addition to the list that NGB provided of 130 DOD and bureau applications that GuardNet supports, NGB-AIS officials stated that the network has been used recently to support activities related to homeland security. For example, after last year's terrorist attacks, NGB officials used GuardNet to communicate with states, territories, and the District of Columbia on the use of National Guard units to coordinate airport security activities. They also used GuardNet to inform the public about anthrax and coordinate with first responders. In addition, these officials stated that NGB's recently established Homeland Security Program Office is considering GuardNet for future homeland security support. Further, the Information Technology Advisor of DOD's Homeland Security Task Force told us that GuardNet is being considered for homeland security mission support, and although a final decision has not been made, it may be the best choice of network support because it already exists. In addition, NGB and several states are currently conducting a pilot project, referred to as the Domestic Emergency Response Information System, to evaluate GuardNet's capabilities to support wireless communications between NGB and first responders in the event of a national emergency. At the same time, the Office of the Assistant Secretary of Defense for Reserve Affairs is defining requirements for a Nationwide Distributed Fiber Optic Network to support the National Guard's distance learning program. According to NGB's CIO, this network has no link to GuardNet and will not replace GuardNet.

NGB's lack of understanding about current and potential GuardNet requirements is attributable in part to limitations in its process for managing requirements (which is discussed in the next section of this report), as well as what NGB-AIS officials stated was a lack of management

attention and priority given to creating and maintaining formal requirements documentation. NGB's CIO agreed that this is a problem and that an assessment of GuardNet's requirements is needed. Without clearly understood and defined requirements, NGB is not able to effectively manage the network and thus runs the serious risk that network users are not receiving the level of support they need now, and will need in the future, to effectively perform their respective missions.

NGB Does Not Have an Effective Process for Managing GuardNet Requirements

Industry best practices²⁰ and DOD guidance²¹ recognize the importance of having an effective process for managing system requirements. Such a process ensures that a clear and unambiguous understanding exists between the system's users, acquirers, and developers about what the system is to do (functionality), how well it is to do it (performance), and how it is to interact with other systems (interfaces); this process also ensures that this understanding is sustained throughout the system's life. Without an effective requirements management process, the chances of a system effectively supporting mission needs and providing mission value commensurate with costs are appreciably reduced.

An effective requirements management process includes, among other things, (1) adhering to a documented requirements management plan; (2) involving system users in developing and changing requirements; (3) establishing a comprehensive set of requirements that serves as the authoritative baseline against which approved changes are made; and (4) controlling changes to the baseline by systematically capturing proposed changes and centrally evaluating and approving changes on the basis of cost, schedule, and risk.

²⁰See, for example, IEEE Standard 1200-1998; SEI CMMI, Version 1.1; Electronic Industries Alliance: National Consensus Standard for Configuration Management (EIA-649, August 1998); and IEEE/EIA, *Industry Implementation of International Standard ISO/IEC 12207:1995: Standard for Information Technology-Software Life Cycle Processes* (March 1998).

²¹Department of Defense, *Military Handbook 61A(SE): Configuration Management Guidance* (Feb. 7, 2001).

NGB's approach to managing GuardNet requirements does not satisfy any of these four tenets and, as a result, is not effective. First, the bureau does not have a requirements management plan for the network and does not have plans to develop one. Second, it does not have a clear understanding with network users of their respective roles in managing requirements. Specifically, NGB officials told us that 85 organizations²² participate in GuardNet requirements management activities. However, officials that NGB directed us to, and that represent 7²³ of these 85 organizations, did not corroborate this statement. For example, 3 stated that they did not know whether they participated in requirements management and 3 stated that they did not participate, even though they have concerns about network capabilities, such as bandwidth.²⁴ Moreover, the chairman of the Administration and Support Group of the Information Management Council, which represents the 50 states, the 3 territories, and the District of Columbia, stated that while the council's constituencies use GuardNet to varying degrees for VTC and distributed training, they do not participate in requirements definition and management beyond sometimes raising concerns about NGB-proposed changes to GuardNet.

Third, NGB does not have a comprehensive and authoritative set of requirements that serves as the baseline against which changes are made (see prior section of this report for more information about current GuardNet requirements). Fourth, NGB does not have a systematic way to control changes to GuardNet requirements, such as steps to capture proposed changes and evaluate them on the basis of cost, schedule, and risk. According to NGB-AIS officials, requirements are received in a "piecemeal" fashion, and as long as the originating organization has approved the requirements and funding is available, NGB attempts to implement them. Further, they stated that it is not possible to fully assess the impact of requirements on the network because they have neither a comprehensive and authoritative set of requirements, as noted above, nor a complete accounting of the network's current configuration (which is discussed in the next section of this report).

²²These organizations include (1) functional areas within NGB (e.g., personnel and logistics); (2) other DOD components, such as DISA, the Defense Logistics Agency (DLA), and Forces Command; and (3) the 50 states, 3 territories, and the District of Columbia.

²³The 7 organizations were NGB's Logistics Division, DISA, DLA, Forces Command, Missouri, Iowa, and Virginia.

²⁴NGB officials could not identify an official at the seventh organization for us to contact.

According to NGB officials, formally managing GuardNet requirements has not been an area of management attention or a priority. As a result, NGB does not know what its network is being used for, what its users' needs are, or whether GuardNet is satisfying these needs. This means that NGB could be investing its resources on network capabilities that do not provide the greatest mission value to its users.

NGB Does Not Have an Effective Process for Managing GuardNet's Configuration

Industry best practices²⁵ and DOD guidance²⁶ recognize the importance of configuration management when developing and maintaining a system or network. Through configuration management, the composition of a system is formally defined and tracked to ensure that an unauthorized change is not introduced. Configuration management is a key means for ensuring that additions, deletions, or other changes to a system do not compromise the system's ability to perform as intended.

An effective configuration management process consists of four primary elements, each of which should be described in a configuration management plan and implemented according to the plan. The four are:

- *Configuration identification*: Procedures for identifying, documenting, and assigning unique identifiers (e.g., serial number and name) to a system's hardware and software component parts and subparts, generally referred to as configuration items.
- *Configuration control*: Procedures for evaluating and deciding whether to approve changes to a system's baseline configuration, generally accomplished through configuration control boards, which evaluate proposed changes on the basis of costs, benefits, and risks and decide whether to permit a change.
- *Configuration status accounting*: Procedures for documenting and reporting on the status of configuration items as a system evolves. Documentation, such as historical change lists and original designs or drawings, are generated and kept in a library, thereby allowing organizations to continuously know the state of a system's configuration

²⁵See, for example, IEEE Standard 1200-1998, and SEI CMMI, Version 1.1.

²⁶Military Handbook 61A(SE).

and be in a position to make informed decisions about changing the configuration.

- *Configuration auditing*: Procedures for determining alignment between the actual system and the documentation describing it, thereby ensuring that the documentation used to support the configuration control board's decisionmaking is complete and correct. Configuration audits, both functional and physical, are performed when a significant system change is introduced, and help to ensure that only authorized changes are being made.

For GuardNet, NGB does not have a configuration management plan or documentation describing the network's current configuration, such as topology maps and interface control documents. Moreover, NGB is not performing any of these four elements of the configuration management process.²⁷ For example, the bureau has not identified network configuration items, and it does not have documentation on the network's original or current baseline or on network changes that have been made over its life. In addition, the bureau has not accounted for and reported on the status of the network, and it has not audited the network's configuration.

Further, while NGB established a configuration control board in June 2001 and chartered it to evaluate and decide whether to approve proposed network changes, this board is not an effective body because it lacks a configuration management plan and an authoritative understanding of the network's current configuration. In addition, board officials told us that changes are made to the network without the board's knowledge and that funding availability is the board's sole criterion in deciding whether to implement a change request.

According to bureau officials, knowing the network's configuration and having a process for managing it have not been bureau priorities, and thus adequate management attention and resources have not been devoted to doing either. Bureau officials acknowledge that this needs to change, and they told us that they plan to correct their configuration management weaknesses. To this end, configuration control board officials told us that the board's charter is being revised and that a configuration management

²⁷An October 2001 Texas Army National Guard study of GuardNet also reported that NGB-AIS needed to establish a configuration management process.

plan and description of the network's current configuration are being developed. Further, the Army has recently required states and territories to actively participate in network configuration management of common user component devices.²⁸ However, these officials had not set milestones for completing these ongoing tasks, and GuardNet officials in the three states included in our review (Virginia, Missouri, and Iowa) told us that they were not aware of this participation requirement and had not committed resources to fulfilling it.

The absence of effective network configuration management is a serious risk that further jeopardizes GuardNet's ability to support current and potential requirements. Unless this situation is promptly remedied, users of the network do not have adequate assurance that the network will perform as intended and to the level needed to support their respective mission areas.

NGB Does Not Have an Effective Process for Managing GuardNet's Security

An effective security management program is essential to ensuring the confidentiality, integrity, and availability of IT assets. Our research on best practices for IT security management shows that leading organizations manage this vital area centrally through a continuous cycle of risk management.²⁹ The key tasks in this cycle include (1) identifying and assessing security risks as the basis for determining security needs and requirements; (2) establishing and implementing policies and controls that meet security needs and requirements; (3) conducting tests and evaluations to ensure that policies and controls have been implemented and are functioning as intended, and that on the basis of these tests and evaluations, certifying and accrediting³⁰ mission-critical systems as secure; and (4) establishing a central, enterprisewide security management function.

²⁸Department of the Army, Army Regulation 25-1: *Army Information Management* (May 31, 2002).

²⁹U.S. General Accounting Office, *Information Security Management: Learning From Leading Organizations*, GAO/AIMD-98-68 (Washington, D.C.: May 1998).

³⁰Certification is the technical and nontechnical evaluation that is conducted to verify that IT systems comply with security requirements. Accreditation is the formal declaration that the appropriate safeguards have been properly implemented and that the residual risk is acceptable.

NGB has not adequately satisfied any of these four tenets of effective IT security management because, according to NGB officials, it has not treated this area as a mission priority and devoted sufficient management attention and resources to it. As a result, the bureau does not know, for example, how vulnerable GuardNet is to attack or when it is under attack. This means that users of the network, and the critical missions they perform, are likely being exposed to undue risk.

NGB Has Not Adequately Assessed GuardNet Security Risks and Has Not Developed a Security Plan

Our research on leading organizations,³¹ as well as DOD and Army policy,³² recognizes that identifying and assessing IT security risks is an essential step in determining the controls needed and the resources that should be invested in these controls. Federal and DOD guidance advocate performing these risk assessments at least once every 3 years or when a significant change in the system has occurred. Among other things, these assessments should address the risks introduced through connections to other networks and the mission impacts should network security be compromised. Federal and DOD guidance also advocate developing security plans to define the steps to be taken and controls to be implemented to mitigate the risks identified.³³ These security plans should be updated regularly to reflect both significant changes to the system and new and emerging threats posed by technological advances.

According to NGB-AIS officials, no risk assessment of GuardNet was performed between 1995 and 2000. In February 2001, a risk assessment of the Army National Guard Readiness Center's local-area network, which connects to GuardNet, was prepared, and in October 2001, a draft risk assessment was developed for GuardNet. However, neither risk assessment

³¹[GAO/AIMD-98-68](#).

³²DOD Instruction 5200.40: *DOD Information Technology Security Certification and Accreditation Process* (DITSCAP), (Dec. 30, 1997); DOD Directive (DODD): *Security Requirements for Automated Information Systems* (DODD 5200.28, Mar. 21, 1988); Department of the Army, *Army Regulation 380-19: Information Systems Security* (Feb. 27, 1998); and *Army Regulation 25-1*.

³³Office of Management and Budget (OMB), *Management of Federal Information Resources*, OMB Circular A-130, Appendix III (Nov. 30, 2000). Additional guidance on effective risk assessment is available in the National Institute of Standards and Technology publications and in the U.S. General Accounting Office, *Information Security Risk Assessment: Practices of Leading Organizations*, [GAO/AIMD-00-33](#) (Washington, D.C.: November 1999). See also, DODD 5200.28 and *Army Regulation 380-19*.

is consistent with the above criteria. The February 2001 assessment was for a single local-area network, not GuardNet. Further, the October 2001 draft assessment has not been approved, and it did not identify all threats (e.g., GuardNet's interconnectivity with other entities' networks and the associated risks, such as the lack of operational firewalls), and it did not provide an estimate of the potential losses or damage if network security was breached. Nevertheless, this assessment still identified potential network vulnerabilities that could be exploited, such as unauthorized access to information and the theft or destruction of system software and files.

NGB also has not developed a network security plan. Although NGB-AIS officials stated that they were in the process of developing this plan as part of NGB's ongoing efforts to certify and accredit GuardNet, they could not provide us with any documentation to support this statement. Moreover, NGB still does not have an approved risk assessment upon which to base the security plan.

According to NGB officials, because GuardNet security management has not been a bureau priority, adequate management attention and resources have not been devoted to assessing network risks and planning for how to address these risks. As a result, NGB is not in a position to ensure that its investments in GuardNet include the proper mix of cost-effective countermeasures for addressing network vulnerabilities.

NGB Has Not Implemented Basic Network Security Controls

Our research on IT security practices employed by leading organizations also shows that risk-based and cost-effective security policies and related procedural and technology controls, such as firewalls, are the means for protecting a system from compromise, subversion, and tampering.³⁴ To this end, DOD, the Army, and NGB have established security policies that can provide for an effective security program if the needed controls are implemented. The key is for NGB to comply with applicable DOD and Army policies, such as DOD's certification and accreditation policy³⁵ and the Army's information security policy,³⁶ as well as its own policies and

³⁴GAO/AIMD-98-68.

³⁵DOD Instruction 5200.40.

³⁶Army Regulation 380-19.

guidance on various topics, such as intrusion detection systems, external requests for network connections, firewalls, and information assurance vulnerability alerts.³⁷

Despite these security policies and guidance, NGB has yet to implement the security controls needed to satisfy them. For example, Army policy requires that firewalls be implemented to prevent outside users from directly accessing nonpublic information.³⁸ According to NGB officials, the bureau has implemented 54 firewalls to protect the federally controlled portion of GuardNet, and 38 of the 54 firewalls needed to protect the state-controlled portion are operational; the bureau plans to complete this effort in September 2002. In the interim, NGB officials confirmed that individuals with access to states' systems could use these unprotected connections as pathways to access Army National Guard systems. In addition, NGB has yet to certify and accredit GuardNet as required by DOD policy.

According to NGB-AIS officials, adequate management attention and resources have not been devoted to implementing needed security controls. Until these controls are implemented, both GuardNet and other organizations whose networks are connected to it will remain vulnerable to attack, and the execution of their respective missions will be in jeopardy.

NGB Is Not Adequately Monitoring Security Policies and Controls

IT security management best practices³⁹ and Army policy⁴⁰ also recognize the need to continuously monitor controls through tests and evaluations, commonly referred to as vulnerability assessments, to ensure that controls have been appropriately implemented and are operating as intended. This type of oversight is critical because it enables management to identify and correct problems in a timely fashion.

³⁷See for example, NGB's Internal Vulnerability Assessment Policy for GuardNet, November 2000; NGB's Intrusion Detection System Policy for GuardNet XXI, November 2000; NGB's External Connection Policy for GuardNet XXI, November 2000; NGB's Firewall Baseline Security Configuration Policy for GuardNet XXI, November 2000; and NGB's Information Assurance Vulnerability Alert Policy for GuardNet XXI, November 2000.

³⁸Army Regulation 380-19.

³⁹[GAO/AIMD-98-68](#).

⁴⁰Army Regulation 380-19.

NGB is not performing critical monitoring activities to ensure that implemented controls are operating as intended. According to NGB-AIS officials, only one vulnerability assessment related to GuardNet has ever been conducted, and it covered two local-area networks connected to GuardNet. This assessment showed significant weaknesses, such as poor password administration (e.g., system administrator and user accounts that do not require passwords and commonly known default passwords that have never been changed), a lack of security training awareness, and poorly configured operating system functions that allow intruders to bypass security controls and overwrite existing files or create new ones. Further, NGB security officials, who are responsible for ensuring that the recommendations resulting from the vulnerability assessment are implemented, stated that they are not doing so; rather, they are relying on the operations personnel to evaluate and appropriately implement needed security controls, and the security officials do not know whether the recommendations have been implemented.

NGB officials also told us that while they have placed 54 intrusion detection devices⁴¹ on GuardNet as a security control, these devices are not continuously monitored. Specifically, NGB-AIS has one contract employee who is responsible for maintaining the devices and monitoring the device's logs to identify attacks on GuardNet. However, this individual is on duty only during East Coast business hours. As a result, no one is actively detecting attacks during a portion of several states' normal business hours. This means that a properly timed intrusion would likely go undetected. Exacerbating this, according to NGB officials, is that at any given time, about 10 percent of the 54 devices are not functional.⁴²

According to NGB officials, monitoring whether security controls have been implemented according to policies has not been a priority, and thus adequate resources have not been allocated to it. As a result, GuardNet is unnecessarily vulnerable to undetected attack, and network users and their missions are being jeopardized.

⁴¹Intrusion detection devices are software or hardware systems that monitor network traffic and help identify cyberthreats.

⁴²The bureau does not compile statistical data on the failure rate of these devices.

NGB's Central Organization for Managing Security Is Not Fulfilling Its Responsibilities

Our research shows that centralized management is the foundation of an effective information security management program because it allows the requisite security knowledge and expertise to be assimilated and applied on an enterprisewide basis and the other segments of the risk management cycle to be addressed in an integrated fashion.⁴³ Central management is especially important for managing the increased risks associated with a highly connected computing environment, such as GuardNet, where security weaknesses in one organization's network can compromise the security of other organization's IT assets.

NGB has established a central management function that is responsible for many of the tenets of effective security management, such as assessing network risks on a periodic basis, developing security plans to address the risks identified, implementing needed security controls, and independently ensuring that implemented controls are operating as intended. However, as previously discussed, NGB's security management function is not effectively discharging its assigned responsibilities.

NGB officials told us that key security management duties have not been performed because network security has not been designated a bureau priority and thus has not received adequate management attention and resources, including staff. Without satisfying these central security management responsibilities, the bureau will be unable to assure itself and other organizations that appropriate steps have been taken to effectively protect GuardNet and will not know the extent of network vulnerabilities.

Conclusions

GuardNet has played an important role in critical mission areas, including homeland security, and consideration is being given to expanding this role, thus making the network's ability to support a range of mission-critical applications in a reliable and secure manner of paramount importance. However, GuardNet is not ready to meet this challenge because NGB does not fully know the network's requirements and is not effectively managing the network. More specifically, important controls in the three interrelated areas of network requirements, configuration, and security management are absent, precluding NGB from fully knowing such things as what the true makeup of the network is, how and by whom it is being used, how it is performing, what risks it faces, and what security features are needed. This

⁴³[GAO/AIMD-98-68](#).

absence of controls is due to insufficient NGB management attention and resources being devoted to these three areas. Without giving swift and immediate management attention and priority to limiting network users' current exposure to risk; understanding and evaluating the network's current requirements, configuration, and security posture; and developing and implementing plans of action to appropriately address current network management weaknesses and risks, the mission effectiveness of not only the bureau, but also all organizations that either use or are connected to the network, is at risk.

Recommendations for Executive Action

To strengthen NGB's management of GuardNet and reduce the risks associated with federal, state, and local governments relying on it to perform mission-critical functions, we recommend that the Secretary of Defense direct the Secretary of the Army to ensure that GuardNet management is given the priority attention and resources commensurate with the criticality and importance of the network's current and potential uses. To this end, we recommend that the Secretary, through the Secretary of the Army, direct the NGB Chief to immediately

- develop a complete and comprehensive inventory of network user organizations;
- fully disclose to these users all known network management weaknesses and security vulnerabilities;
- advise these users to take appropriate steps to ensure that their respective needs for reliable and secure network services are met; and
- fully disclose, in a controlled manner, all known network management weaknesses and security vulnerabilities to all known potential network users, particularly potential homeland security-related users at the federal, state, and local government levels.

Next, we recommend that the Secretary of the Army direct the NGB Chief to ensure that near-term changes to the network are limited to those needed to address already identified performance and security problems. During this period of limited network change, we further recommend that the Chief develop an authoritative and comprehensive baseline understanding of GuardNet's requirements, configuration, and security posture.

Next, we recommend that the Secretary of the Army direct the NGB Chief to correct each network management process weakness discussed in this report. More specifically, we recommend that the NGB Chief develop management process improvement plans for requirements management, configuration management, and security management. We further recommend that each of these plans, at a minimum, specify measurable goals and objectives, assign roles and responsibilities, involve network users, and identify work tasks, implementation schedules, and resource needs. In addition, we recommend that

- the requirements management improvement plan provide for establishing a process that includes (1) developing a requirements management plan, (2) involving network users in developing and changing requirements, (3) developing requirements management baseline documentation, such as a mission needs statement and an operational requirements document, and (4) establishing controls for assessing and approving proposed changes to the baseline;
- the configuration management improvement plan provide for establishing a process that includes (1) identifying and documenting the network's components/subcomponents (hardware and software), (2) creating a baseline configuration (development, test, and production environments) of these component parts, (3) controlling changes to these configuration baselines through a formal change process that allows only the NGB-AIS Configuration Control Board to approve changes to GuardNet, (4) ensuring that network documentation remains current to enable accurate reporting of changes as the network evolves, and (5) periodically auditing to ensure that the documentation is complete and accurate; and
- the security management improvement plan provide for establishing a process that includes (1) assessing risks to determine security needs, (2) implementing needed controls in accordance with applicable policy and guidance, (3) monitoring existing controls to ensure that they are operating as intended, and (4) ensuring that the network is certified and accredited in accordance with DOD policy.

Last, we recommend that, until these recommendations are fully implemented, the NGB Chief report to the Secretary of the Army and advise the Director of the White House's Office of Homeland Security, on a quarterly basis, on NGB's progress in implementing each of these

recommendations and the associated reliability and security risks faced by GuardNet users in the interim.

Agency Comments and Our Evaluation

In DOD's written comments on a draft of this report signed by the Acting Chief of NGB (see app. II), the department agreed with our conclusion that GuardNet is not ready to reliably and securely support the homeland security mission, and it endorsed the network management processes that we described as needed. In addition, the department characterized our report as timely and our recommendations as valued, and stated that it would use these recommendations to enhance network services.

However, DOD did not agree with one component of our recommendation aimed at disclosing to GuardNet users, current and future, all known network management weaknesses and security vulnerabilities so that these organizations could take appropriate steps. In particular, the department did not agree with the need to first establish an inventory of network users, stating that it would serve no meaningful purpose to NGB because user lists are maintained by the organization that provides local-area network access. We understand DOD's point and, in fact, these user organizations are precisely the users we are referring to in our recommendation. Therefore, we have modified our recommendation to refer to "users" as "user organizations" to alleviate any misunderstanding.

Also, DOD did not agree with our recommendation to develop a security management improvement plan for establishing an effective security management process, stating that NGB already addresses GuardNet security requirements with appropriate representatives, attributing current security deficiencies to funding inadequacies. We disagree with DOD because its comments neither provide sufficient basis for the position it takes nor refute the facts presented in the report that are the basis for our recommendation. As we state in the report, NGB has not established an effective security management process for the network. For example, NGB has not performed a risk assessment to understand security needs, implemented needed controls, or certified and accredited GuardNet, each of which is a critical element of an effective security management process. Accordingly, we recommended that NGB develop a security management improvement plan that provides for putting these missing process elements in place. Without this plan, which should include a provision for adequate resources, NGB's efforts to address its security management weaknesses are unlikely to be successful.

Last, the Acting Director of the NGB's Information Systems Division provided other clarifying comments on our experience in using GuardNet to video teleconference with Army National Guard officials in Virginia, which we have incorporated as appropriate in the report.

We are sending copies of this report to interested congressional committees. We are also sending copies to the Director, Office of Management and Budget; the Attorney General of the United States; the Director of the White House's Office of Homeland Security; the Secretary of Defense; the Secretary of the Army; and the Chief of the National Guard Bureau. We will also make copies available to others upon request. The report will be available at no charge on the GAO Web site at <http://www.gao.gov>.

If you have any questions regarding this report, please contact me at (202) 512-3439 or by E-mail at hiter@gao.gov. Key contributors to this report are listed in appendix III.



Randolph C. Hite
Director, Information Technology
Architecture and Systems Issues

Objectives, Scope, and Methodology

The objectives of our review were to determine (1) the current and potential requirements of the National Guard Bureau's (NGB) GuardNet and (2) the effectiveness of the processes for managing current and potential network requirements, the network's configuration, and network security.

To determine current and potential requirements of the network, we reviewed industry best practices and Department of Defense (DOD) guidance,⁴⁴ as well as draft network diagrams and performance reports, minutes from the Information Systems (AIS) Division Configuration Control Board (CCB) meetings, system change requests, and expenditure and budget documents. We also requested requirements inventories, documents, and specifications, as well as a current list of network applications, which we discovered do not exist for GuardNet. We obtained and reviewed the results of a study commissioned by NGB's Chief Information Officer (CIO) that primarily focused on the Distributive Training Technology Project, but also covered GuardNet performance concerns.⁴⁵ In addition, we interviewed officials from NGB's AIS Division, the chairman of the Information Management Council's Administration and Support Group (which represents the interests of the 50 states, 3 territories, and the District of Columbia), and the directors of information management for 3 states (Virginia, Iowa, and Missouri)⁴⁶ to identify network requirements and discuss network use, including the possibility of a future homeland security mission. We also interviewed NGB's CIO and officials from its Homeland Security Program Office, as well as the Information Technology Advisor for DOD's Homeland Security Task Force, to inquire whether a decision had been made regarding the network's future use in support of a homeland security mission.

⁴⁴Institute of Electrical and Electronics Engineers (IEEE), *Standard for Application and Management of the Systems Engineering Process* (IEEE Standard 1220-1998, Jan. 22, 1999); the Software Engineering Institute (SEI), *Capability Maturity Model Integration (CMMI)*, Version 1.1, (March 2002); and Chairman of the Joint Chiefs of Staff Instruction: *Requirements Generation System* (CJCSI-3170.01b, Apr. 15, 2001).

⁴⁵*C3 Requirements Definition: Using DTTP and GuardNet XXI in Support of the National Guard C3 Mission*, requirements document-report to the CIO, NGB (Feb. 14, 2002).

⁴⁶We selected these 3 states because (1) Virginia does not have a state network and, therefore, relies solely on GuardNet to access DOD and NGB applications and the Internet, and (2) Iowa and Missouri were recommended by NGB as examples of states that are using GuardNet.

To determine the effectiveness of NGB's process for managing current and potential network requirements, we reviewed industry best practices and DOD guidance on establishing such a process and evaluated NGB's efforts using these criteria.⁴⁷ We also reviewed management reports, funding proposals, documentation on network expenditures, CCB meeting minutes, and system change requests. We interviewed officials from NGB's CIO organization, AIS Division, the CCB, and the Distributive Training Technology Project program office, including the CIO and the Acting Chief of the AIS Division. We selected seven organizations including three states identified by NGB as participants in the requirements management process—Defense Logistics Agency, Defense Information Systems Agency, Forces Command, NGB's Logistics Division, Virginia, Iowa, and Missouri—and the Information Management Council's Administration and Support Group chairman to determine their respective roles in this process. We interviewed officials from the organizations for which NGB provided a point of contact.

To determine the effectiveness of NGB's process for managing the network's configuration, we reviewed industry best practices and DOD policy and guidance on establishing such a process and evaluated NGB's efforts using these criteria.⁴⁸ We reviewed draft network diagrams, minutes of AIS CCB meetings, system change requests, and the current CCB charter. We also inquired about the status of NGB's efforts to revise the CCB charter and develop a configuration management plan and network topology for GuardNet. In addition, we interviewed NGB-AIS and CCB officials on configuration management processes and practices, as well as the directors of information management for Virginia, Iowa, and Missouri on their respective roles in this process.

To determine the effectiveness of NGB's network security management process, we reviewed industry best practices and DOD policy and guidance

⁴⁷IEEE Standard 1200-1998; SEI CMMI, Version 1.1; and Department of Defense, *Military Handbook 61A(SE): Configuration Management Guidance* (Feb. 7, 2001).

⁴⁸IEEE Standard 1200-1998; SEI CMMI, Version 1.1; Military Handbook 61A(SE); and Department of the Army, Army Regulation 25-1: *Army Information Management* (May 31, 2002).

and evaluated NGB's efforts using these criteria.⁴⁹ We reviewed security test results, risk analyses, and associated mitigation plans and progress reports. We also reviewed a certification and accreditation package for a local-area network and the October 2001 vulnerability assessment test report⁵⁰ for two local-area networks. We interviewed NGB-AIS security officials, including the Computer Emergency Response Team and state officials from Virginia, Iowa, and Missouri, about their security management programs.

We conducted our work at the Army National Guard Readiness Center, National Guard headquarters, and the Pentagon in Arlington, Virginia, and at the Advanced Distributive Learning Co-Laboratory in Alexandria, Virginia, from March 2002 through September 2002 in accordance with generally accepted government auditing standards.

⁴⁹See for example, U.S. General Accounting Office, *Information Security Management: Learning From Leading Organizations*, GAO/AIMD-98-68 (Washington, D.C.: May 1998); Office of Management and Budget (OMB), *Management of Federal Information Resources*, OMB Circular A-130, Appendix III (Nov. 30, 2000); DOD Directive (DODD): *Security Requirements for Automated Information Systems* (DODD 5200.28, Mar. 21, 1988), and Department of the Army, Army Regulation 380-19: *Information Systems Security* (Feb. 27, 1998).

⁵⁰Texas Army National Guard Information Operations Vulnerability Assessment Team 1, *National Guard Bureau: Vulnerability Assessment Findings Report* (Readiness Center, Arlington, Va.: Nov. 1, 2001).

Comments from the National Guard



DEPARTMENTS OF THE ARMY AND THE AIR FORCE
NATIONAL GUARD BUREAU
1411 JEFFERSON DAVIS HIGHWAY
ARLINGTON, VA 22202-3231

12 September 2002

Mr. Joel C. Willemssen
Managing Director, Information Technology Issues
United States General Accounting Office
Washington, DC 20548

Dear Mr. Willemssen:

Thank you for your thorough review and detailed comments concerning the National Guard's wide area network, GuardNet. Enclosed is the response to the tentative findings and recommendations contained in the draft report.

The National Guard Bureau is committed to providing the highest level of information technology support possible to our soldiers, our units, the 54 States, territories and District of Columbia, and the various communities of interest that rely on GuardNet to support both their State and Federal missions. The Army National Guard is committed to operating and maintaining GuardNet in a manner that is consistent with Department of Defense and Department of the Army policy. I generally concur with the recommendations in the GAO report and look forward to using its recommendations as a tool to enhance the service provided to the various users of GuardNet.

Although not covered in the report, GuardNet has experienced enormous operational successes in meeting the congressional mandate for information technology (IT) support for administration, mobilization, and training (distance learning) of the National Guard. In addition to this essential congressional priority, we learned in the 9-11 crisis that GuardNet can provide command and control for local emergencies and natural disasters. We concur with GAO's conclusions that GuardNet is not ready to assume this role as a full IT partner for the Homeland Security mission. However, once that requirement is officially established and funding provided for the necessary enhancements to GuardNet, I am confident that GuardNet can participate with others in providing critical command and control support to the Homeland Security mission.

The National Guard Bureau is aware and endorses the processes for managing GuardNet requirements, security, and configuration described in the GAO report. In many cases NGB had previously identified these requirements and initiated tasks to document and establish these processes. The processes and other deficiencies identified do have management's attention and are extremely important to our program. Operational exigencies and a dynamic environment have consumed many of the energies and resources available to the GuardNet function. With adequate funding,

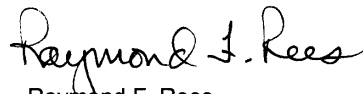
Appendix II
Comments from the National Guard

these essential administrative and operational (security) deficiencies can be corrected and GuardNet with modest enhancements can become a national resource available to the States for the Homeland Security mission.

I would hope that this GAO report will stimulate support for fully funding the GuardNet IT structure and the improvements that will allow it to function as an integral part of the Homeland Security IT solution. The National Guard Bureau is already addressing the deficiencies identified in the GAO report and looking forward to reporting our progress in completing the corrective action. Our solutions will include controls to prevent recurrence.

Again, thank you for your timely assessment and valued recommendations concerning the Army National Guard's wide area network.

Sincerely,



Raymond F. Rees
Major General, U.S. Army
Acting Chief, National Guard Bureau

Enclosure

Recommendations and Comments
United States General Accounting Office Draft Report (GAO-02-959)
National Guard Effective Management Processes Needed for Wide-Area Network

Recommendation 1: We recommend that the Secretary, through the Secretary of the Army, direct the NGB Chief to immediately: (1) develop a complete and comprehensive inventory of network users; (2) fully disclose to these users all known network management weaknesses and security vulnerabilities; (3) advise these users to take appropriate steps to ensure that their respective needs for reliable and secure network services are met; and (4) fully disclose, in a controlled manner, all known network management weaknesses and security vulnerabilities to all known potential network users, particularly potential homeland security-related users at the federal, state, and local government levels.

Comments: Non-concur with the recommendation to develop a comprehensive inventory of network users. This recommendation would serve no meaningful purpose at the National Guard Bureau level. User-lists and their associated network authorizations are maintained by the organization that provides local area network access. In the next 45 days NGB will develop documentation that identifies the network's capabilities and limitations to be provided to prospective network users. This documentation will be placed under configuration control to ensure it evolves as the network evolves.

Recommendation 2: We recommend that the Secretary of the Army direct the NGB Chief to ensure that near-term changes to the network are limited to those needed to address already identified performance and security problems. During this period of limited network change, we further recommend that the Chief develop an authoritative and comprehensive baseline understanding of GuardNet's requirements, configuration, and security posture.

Comments: Concur. NGB has taken steps to ensure that network configuration changes are limited to those that are deemed to be operational necessities. NGB believes the steps taken to limit wide area network changes meets the intent of this recommendation.

Recommendation 3: We recommend that the NGB Chief develop management process improvement plans for requirements management, configuration management, and security management. We further recommend that each of these plans, at a minimum, specify measurable goals and objectives, assign roles and responsibilities, involve network users, and identify work tasks, implementation schedules, and resource needs. In addition, we recommend that:

- (1) the requirements management improvement plan provide for establishing a process that includes (a) developing a requirements management plan, (b) involving network users in developing and changing requirements, (c) developing requirements management baseline documentation, such as a mission needs statement and an operational requirements document, and (d) establishing controls for assessing and approving proposed changes to the baseline;

Enclosure

- (2) the configuration management improvement plan provide for establishing a process that includes (a) identifying and documenting the network's components/ subcomponents (hardware and software); (b) creating a baseline configuration (development, test, and production environments) of these component parts; (c) controlling changes to these configuration baselines through a formal change process that allows only the NGB AIS configuration control board to approve changes to GuardNet; (d) ensuring that network documentation remains current to enable accurate reporting of changes as the network evolves; and (e) periodically auditing to ensure that the documentation is complete and accurate; and
- (3) the security management improvement plan provide for establishing a process that includes (a) assessing risks to determine security needs, (b) implementing needed controls in accordance with applicable policy and guidance, (c) monitoring existing controls to ensure that they are operating as intended, and (d) ensuring that the network is certified and accredited in accordance with DOD policy.

Comments:

- (1) Requirements Management: Concur with the intent of this recommendation. NGB will work more closely with functional representatives to better define network requirements changes as part of implementing its configuration management improvement plan.
- (2) Configuration Management: Concur. NGB has taken action to allocate additional resources in FY03 to enhance its configuration management activities.
- (3) Security Management: Non-concur with the recommendation to create and implement a separate security management improvement plan. NGB recognizes the importance of information security and continually addresses information security requirements with representatives of HQDA and appropriate functional representatives. In the past NGB has been unable to adequately resource its information security requirements. However, we anticipate the allocation of additional resources in FY03 enabling the NGB to address information security in a more holistic manner.

Recommendation 4: We recommend that, until these recommendations are fully implemented, the NGB Chief report to the Secretary of the Army and advise the Director of the White House's Office of Homeland Security, on a quarterly basis, on NGB's progress in implementing each of these recommendations and the associated reliability and security risks faced by GuardNet users in the interim.

Comments: Concur. NGB will provide quarterly updates on the implementation of the recommendations contained in the GAO report.

GAO Contact and Staff Acknowledgments

GAO Contact

Cynthia Jackson, (202) 512-5086

**Staff
Acknowledgments**

In addition to the individual named above, key contributors to this report were Justin Booth, Joanne Fiorino, Sophia Harrison, Anjalique Lawrence, and William Wadsworth.

GAO's Mission

The General Accounting Office, the investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to www.gao.gov and select "Subscribe to daily E-mail alert for newly released products" under the GAO Reports heading.

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are \$2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. General Accounting Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
 TDD: (202) 512-2537
 Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Public Affairs

Jeff Nelligan, managing director, NelliganJ@gao.gov (202) 512-4800
U.S. General Accounting Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

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

**Presorted Standard
Postage & Fees Paid
GAO
Permit No. GI00**

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

Address Service Requested

