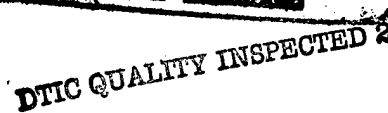
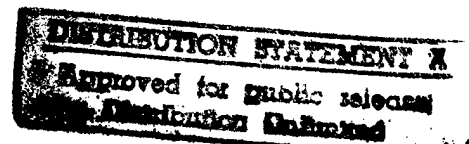


April 1998

COMBATING TERRORISM

Threat and Risk Assessments Can Help Prioritize and Target Program Investments



19980424 068



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

National Security and
International Affairs Division

B-279003

April 9, 1998

The Honorable Ike Skelton
Ranking Minority Member
Committee on National Security
House of Representatives

The Honorable J. Dennis Hastert
Chairman, Subcommittee on National
Security, International Affairs, and
Criminal Justice
Committee on Government Reform and
Oversight
House of Representatives

The Defense Against Weapons of Mass Destruction Act of 1996 established the Nunn-Lugar-Domenici (NLD) domestic preparedness program.¹ The program is intended to enhance federal, state, and local emergency response capabilities to deal with a domestic terrorist incident involving weapons of mass destruction (WMD).² Congress established the NLD program in response to a perceived significant and growing threat of WMD terrorism directed against American cities and shortfalls in U.S. cities' WMD emergency response capabilities. With its \$30.5 million budget for fiscal year 1997, program initiatives planned or underway include develop and execute a curriculum for training emergency response personnel in 120 cities selected for the NLD program; provide NLD cities some training equipment (generally \$300,000 worth of equipment per city), much of which has operational capabilities;³ and create a database on chemical and biological agents. The first 27 cities that were selected for the NLD program are in the process of receiving training.⁴

As requested, we are reviewing the implementation of the NLD program. Our review includes an assessment of the program's status and progress,

¹The Defense Against Weapons of Mass Destruction Act was contained in the National Defense Authorization Act for Fiscal Year 1997 (title XIV of P.L. 104-201, Sept. 23, 1996) and is commonly referred to by its sponsors' names, Senators Nunn, Lugar, and Domenici.

²In the National Defense Authorization Act for Fiscal Year 1997 (section 1403), WMD are defined as any weapon or device that is intended, or has the capability, to cause death or serious bodily injury to a significant number of people through the release of toxic or poisonous chemicals or their precursors, a disease organism, or radiation or radioactivity.

³The Department of Health and Human Services and the Federal Bureau of Investigation have separately funded programs to purchase equipment for U.S. cities' emergency response personnel.

⁴At the time of our review, 11 cities had received emergency response training.

the criteria and methodology used to select cities that receive assistance, the approach used to determine the capabilities and needs of participating cities, and the potential cost of equipping a city to respond to a terrorist incident involving a WMD. As part of that effort, we explored how some public and private sector organizations establish requirements and prioritize and allocate resources to safeguard assets against a variety of threats, including terrorism. Specifically, we (1) examined threat and risk assessment approaches used by several public and private sector organizations to deal with terrorist and other security risks and obtained detailed information on a private company's risk-assessment process, (2) determined whether 11 of the first 27 cities selected for NLD training and assistance used threat and risk assessments to establish requirements for dealing with WMD terrorist incidents, and (3) assessed the challenges of using formal threat and risk assessments to help define requirements and prioritize and target NLD program resources. This report discusses an opportunity to enhance decisions on how to allocate NLD and other similar federally funded program resources. We will report later on the rest of the work.

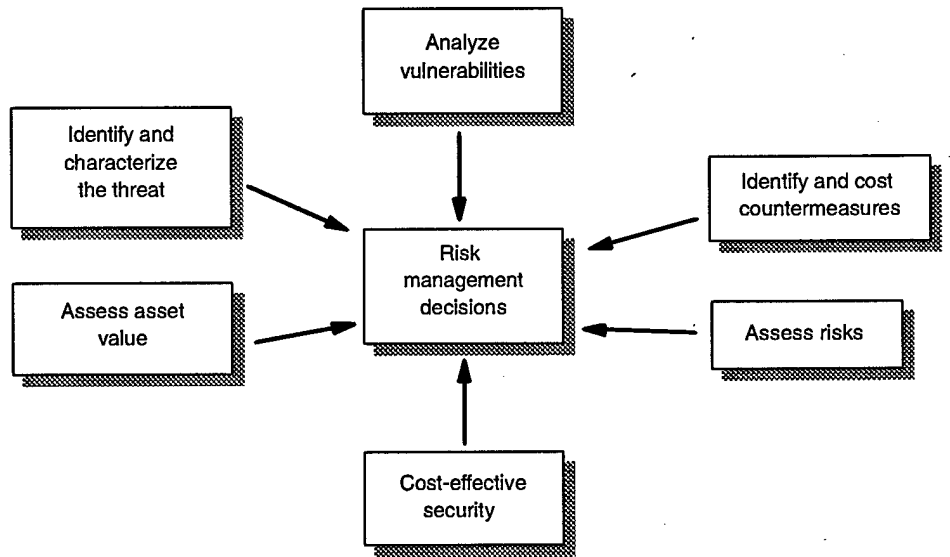
Background

The Department of Defense (DOD) is lead federal agency for implementing the NLD program. In that role, DOD works in cooperation with the Federal Bureau of Investigation (FBI), the Department of Energy (DOE), the Environmental Protection Agency, the Department of Health and Human Services, and the Federal Emergency Management Agency. Before providing cities training and other assistance, a federal interagency group comprising representatives from these six agencies formulated and distributed information and questions to help NLD cities assess their training and equipment needs. Some of the cities have begun to buy equipment for dealing with chemical and biological terrorist incidents with federal and their own funds. NLD program officials have reported that local emergency response personnel do not have the equipment and supplies necessary to protect themselves and victims in a WMD incident, and that most cities would be unable to afford them without federal assistance. Further, in its October 1997 report, the President's Commission on Critical Infrastructure Protection⁵ recommended that NLD funding be doubled in fiscal year 1999 to, among other things, provide cities with equipment to detect and identify WMD.

⁵The Commission, a government-private sector body established in 1996, was to develop a national strategy to protect the nation's critical infrastructures (e.g., banking and finance, telecommunications, and electric power system) from physical and computer-based threats.

Threat and risk assessments are widely recognized as valid decision support tools to establish and prioritize security program requirements. A threat analysis, the first step in determining risk, identifies and evaluates each threat on the basis of various factors, such as its capability and intent to attack an asset, the likelihood of a successful attack, and its lethality. Risk management is the deliberate process of understanding “risk”—the likelihood that a threat will harm an asset with some severity of consequences—and deciding on and implementing actions to reduce it. Risk management principles acknowledge that (1) while risk generally cannot be eliminated, it can be reduced by enhancing protection from validated and credible threats; (2) although many threats are possible, some are more likely to occur than others; and (3) all assets are not equally critical. Figure 1 shows factors considered in making risk management decisions.

Figure 1: Factors Considered in Making Risk Management Decisions



Source: A multinational oil company.

Generally, the risk-assessment process is a deliberate, analytical approach to identify which threats can exploit which vulnerabilities in an

organization's specific assets. These variables are ranked according to predetermined criteria, such as the probability of a threat targeting a specific asset or the impact of a vulnerability being exploited by a specific threat. The risk-assessment results in a prioritized list of risks (i.e., threat-asset-vulnerability combinations) that can be used to select safeguards to reduce vulnerabilities and create a certain level of protection.

Results in Brief

We identified several public and private sector organizations that use threat and risk assessments to manage risk and to identify and prioritize their security requirements and expenditures to protect facilities, operations, equipment, and material against terrorist and other threats. For example, one company adapted U.S. government threat and risk-assessment standards and applied them to more than 19 of its overseas operations. The company's risk-assessment approach involves a multidisciplinary team of experts that uses valid threat information to make judgments about the likelihood and consequences of an asset (such as a facility) being seized or destroyed, the asset's criticality, and the asset's vulnerability to various threats. The company has applied its risk-assessment process in a number of areas, from its operations and facilities in Chad to its hiring practices.

The NLD program is in the early stages of implementation, and most cities have not yet received training, assistance, or equipment. At the time of our review, threat and risk assessments were not performed by either the cities or the NLD federal program agencies for 11 of the first 27 cities selected for assistance. If properly applied, threat and risk assessments can provide an analytically sound basis for building programmatic responses to various identified threats, including terrorism. Although threat and risk assessments are not required in the NLD program, they could help cities prioritize their investments in WMD preparedness. Because the program is in the early stages of implementation, opportunities exist to make program adjustments that can help target NLD and other similar programs' training and equipment investments.

We identified the following challenges to applying an accepted threat and risk assessment process to cities selected to participate in the NLD program: (1) security issues (for example, revealing intelligence sources and methods) related to providing valid threat data from the intelligence community to city officials; (2) the lack of specificity in the intelligence community's threat information; and (3) the complexity and magnitude of

a large city as a subject of a threat and risk assessment. These challenges could be overcome through federal-city collaboration.

Qualitative Risk Assessments Are Being Used to Define Requirements and Allocate Resources

Several federal government and private sector organizations apply some formal threat and risk-assessment process in their programs. For example, the Defense Special Weapons Agency uses a risk-assessment model to evaluate force protection security requirements for mass casualty terrorist incidents at DOD military bases.⁶ DOE uses a graded approach to protect its assets based on risk and vulnerability assessments. Under the graded approach, DOE develops and implements security programs at a level commensurate with the asset's importance or the impact of its loss, destruction, or misuse. Also, as required by the Federal Aviation Reauthorization Act of 1996 (P.L. 104-264), the Federal Aviation Administration (FAA) and the FBI do joint threat and vulnerability assessments on each airport determined to be high risk. Further, three companies under contract to government agencies (e.g., DOE, the National Security Agency, the National Aeronautics and Space Administration, and the Library of Congress) use formal risk-assessment models and methods to identify and prioritize security requirements. Moreover, the President's Commission on Critical Infrastructure Protection recommended in its final report that threat and risk assessments be performed on the nation's critical infrastructures. Appendix I contains a brief description of selected organizations that use or recommend threat and risk assessments in their programs.

One private sector organization we visited—a multinational oil company—has used threat and risk assessments to determine the appropriate types and levels of protection for its assets for the past 3 years.⁷ The company's overseas facilities and operations are exposed to a multitude of threats, including terrorism, political instability, and religious and tribal conflict. The company uses risk assessments to identify and assess threats and risk and to decide how to manage risk in a cost-effective manner. For example, the company has invested in countermeasures for its physical, operations, personnel, and information security systems and practices. The company has applied its risk-assessment process to more than 19 of its operations, and according

⁶We previously reported on DOD force protection issues in *Combating Terrorism: Status of DOD Efforts to Protect Its Forces Overseas* (GAO/NSIAD-97-207, July 21, 1997) and *Combating Terrorism: Efforts to Protect U.S. Forces in Turkey and the Middle East* (GAO/T-NSIAD-98-44, Oct. 28, 1997).

⁷Some of the other organizations we identified are in the early phases of using threat and risk assessments.

to company officials, the process has resulted in enhanced security and a potential annual savings of \$10 million. Company officials highlighted the flexibility of the process in that they have used it to identify training requirements in a number of areas.

The company uses a multidisciplinary team of experts to identify and evaluate threats, assets' criticality, vulnerabilities, and countermeasures to manage or reduce risk. The multidisciplinary team that did the risk assessment of the company's facilities and operations in Chad, for example, comprised a cultural anthropologist, a physician, a transportation and logistics specialist, an intelligence analyst, and some security experts—not to exceed 25 percent of a multidisciplinary team. Company officials highlighted the importance of senior management support for threat and risk assessments and periodic reassessments to ensure that security countermeasures are appropriate and achieve their intended purpose. Over time, countermeasures may become inadequate because of changes in threat or operations. The company's objective is to review its risk assessments every 3 years.

The company's risk-assessment team generates specific threat scenarios from valid intelligence and threat data and pairs them with vulnerabilities in its critical assets. The multidisciplinary risk-assessment team then assigns weights or values to these threat-asset vulnerability pairings according to the likelihood of such events occurring and the consequences of assets being compromised or attacked. This process is based on a DOD military standard and work by the Department of Transportation's Volpe National Transportation Systems Center.

Table 1 shows the DOD standard definitions for the probability that an undesired event will occur. The company adapted these definitions for its assessments.

Table 1: Probability Levels of an Undesired Event

Probability level	Specific event
A Frequent	Likely to occur frequently
B Probable	Will occur several times
C Occasional	Likely to occur sometime
D Remote	Unlikely but possible to occur
E Improbable	So unlikely it can be assumed occurrence may not be experienced

Source: Military Standard 882C.

The company's risk-assessment team quantifies the probability levels' definitions. For example, the team might agree that "frequent" means that an undesired event or threat would occur at least two times per year or that the odds are 9 in 10 of an incident in annual operations. Company officials emphasized that it is not sound practice to base security programs on worst-case scenarios and recommended focusing on those scenarios that are more likely to occur.⁸

The company pairs the agreed-upon assessment from table 1 with DOD's standard for the severity levels of the consequences of an undesired event (see table 2). The company has adapted the DOD definitions for its purposes and included items such as loss of critical proprietary information and unauthorized access to facilities.

Table 2: Severity Levels of Undesired Event Consequences

Severity level	Characteristics
I Catastrophic	Death, system loss, or severe environmental damage
II Critical	Severe injury, severe occupational illness, major system or environmental damage
III Marginal	Minor injury, minor occupational illness, or minor system or environmental damage
IV Negligible	Less than minor injury, occupational illness, or less than minor system or environmental damage

Source: Military Standard 882C.





⁸DOE commented that it believes the protection requirements for a worst-case scenario should at least be reviewed. It added that resource restrictions may preclude complete protection against the worst case but that such cases must be factored into any program.

This process results in a matrix that pairs and ranks as highest risk the most important assets with the threat scenarios most likely to occur. Figure 2 is an example of a risk assessment matrix that combines an analysis of the likelihood and severity of undesired events.

Figure 2: Risk-Assessment Matrix

Probability of occurrence	Severity level			
	I Catastrophic	II Critical	III Marginal	IV Negligible
A Frequent	IA	IIA	IIIA	IVA
B Probable	IB	IIB	IIIB	IVB
C Occasional	IC	IIC	IIIC	IVC
D Remote	ID	IID	IIID	IVD
E Improbable	IE	II E	III E	IVE

Risk Level

IA, IB, IC, IIA, IIB, and IIIA		Unacceptable (reduce risk through countermeasures)	1
ID, IIC, IID, IIIB, and IIIC		Undesirable (management decision required)	2
IE, IIE, IIID, IIIE, IVA, and IVB		Acceptable with review by management	3
IVC, IVD, and IVE		Acceptable without review	4

Source: Adapted from Military Standard 882C and multinational oil company.

The assessment team uses the results from the matrix to develop and recommend security countermeasures for those assets that are most vulnerable to the most likely threats. The team reevaluates the cost benefit and effectiveness of the recommended countermeasures before submitting them for senior management review. According to company officials, their threat and risk-assessment process typically takes 2 weeks to complete and costs about \$20,000. A description of the company's five-step risk assessment process is in appendix II.

DOE, the Defense Special Weapons Agency, and three companies under contract with other government agencies use risk-assessment models or methods that operate with principles similar to those of the oil company. These organizations assemble multidisciplinary teams to do risk assessments; identify and rank threats, assets, and asset vulnerabilities; link threat-asset-vulnerability combinations to produce a rank-ordered list of risks; and identify and prioritize countermeasures to mitigate current risk levels. Moreover, four of the organizations use assessment models that permit real-time sensitivity analyses, and all of the organizations recommend periodically reviewing risk-assessment results to verify that implemented countermeasures are working as expected.

Though Not Required, Threat and Risk Assessments Could Help Cities Prioritize NLD Investments

The NLD legislation does not require that threat and risk assessments be performed either to select the cities that will receive assistance or subsequently to determine selected cities' needs for training and equipment to deal with WMD terrorism incidents. According to information we obtained from DOD; the intelligence community, including the FBI; and data on 11 of the first 27 cities to receive NLD training and assistance, the federal government and the cities have not performed formal, city-specific threat and risk assessments using valid threat data to define requirements and focus program investments.

NLD program agencies provided the first 27 cities information and a set of questions intended to prompt city officials to examine their city's ability to respond to a WMD incident. The information included a generic list of possible terrorist targets that, if attacked, could generate mass casualties, including government facilities; commercial/industrial facilities (including financial centers, factories, shopping malls, hotels, and water supply and wastewater plants); transportation centers; recreational facilities; hospitals; and universities. The information emphasized that emergency response personnel must have the equipment necessary to protect themselves and the victims and instructed cities to determine whether

their equipment was adequate in quality and quantity to perform the emergency response mission. The set of questions led the cities to, among other things, identify additional equipment needs.

After receiving the information and questions from federal program agencies, several of the NLD cities generated lists of sites they considered vulnerable on the basis of very general threat information or local law enforcement data. From the data we reviewed on the 11 cities, it is unclear whether individual WMD threats (for example, individual chemical or biological agents) were categorized in terms of the likelihood of a successful attack on a given asset, such as a water supply system or a subway, or the severity of the consequences of an attack. Cities also established lists of equipment they believed would be needed to deal with a WMD terrorist incident without the benefit of valid threat information from the intelligence community or a formal risk assessment process using accepted analytical standards. For example, one city is using federal funds to buy chemical protective suits for emergency response personnel, decontamination trailers, and other items on the basis of general threat information and identification of heavily trafficked and populated sites. This city also is purchasing items and equipment with its own funds. NLD cities also are considering the purchase of chemical and biological detection and identification equipment. The NLD legislation does not require cities' lists of potential targets and equipment needs to be validated by the federal government.

Since the NLD program is still completing training and assistance in the first 27 cities, there are opportunities for program adjustments. The agencies implementing the NLD program and other appropriate agencies could work collaboratively with NLD city officials to do formal threat and risk assessments that use validated threat data and consider the likelihood of a chemical, biological, nuclear, or radiological attack. Officials from the multinational oil company estimate that a risk assessment on a city could be completed in 2 to 3 weeks. Therefore, if a similar type of risk assessment was done in conjunction with city visits or soon thereafter, the city could receive its training and assistance with little or no delay.

The FBI is in the best position to take the federal lead in facilitating city-specific threat and risk assessments. The FBI, through the Attorney General, is the lead agency for domestic terrorism crisis management. As a member of the intelligence community, the FBI also collects, analyzes, and reports threat information on domestic origin threats and targets. Finally,

the FBI, through its 56 field offices and various joint terrorism task forces⁹ throughout the country, has worked with many of the cities designated to receive NLD training and assistance.

Challenges to Using Threat and Risk Assessments Could Be Overcome

To perform realistic threat assessments, federal and city officials would require access to valid foreign and domestic threat data from the intelligence agencies and the FBI, respectively; local law enforcement groups; and public sources. To the extent possible, this information should focus on threats faced by individual cities. The multinational oil company we visited has personnel cleared to receive classified threat data that relate to its areas of operation for its threat and risk assessments, and U.S. and foreign intelligence agencies provide the company with such data. We discussed intelligence security issues raised by providing threat information to city officials with the Community Counterterrorism Board¹⁰ and FBI officials. These representatives stated that, in principle, the intelligence community could work with the cities to provide valid threat data and to validate any threat scenarios generated by multidisciplinary teams performing city threat and risk assessments.

The intelligence community's threat estimates and reporting on foreign-origin terrorism are often general, rarely city specific, and without further clarification could be difficult to use for threat and risk assessments of NLD cities. To overcome this obstacle, the FAA is working with the FBI to obtain more specific threat information pertaining to its airport security program. The FAA prepared a detailed questionnaire that the FBI is using to help identify the most likely threats faced by individual major metropolitan area airports. From this threat information, a federal-city risk-assessment team could develop threat scenarios that the intelligence agencies and the FBI could compare to their foreign and domestic threat information and analysis and validate with respect to their realism and likelihood of occurrence.

Cities are larger and more complex than most entities subject to threat and risk assessments, such as military bases, ports, and petroleum processing facilities. However, size and complexity would not preclude conducting

⁹The joint terrorism task forces are to facilitate an exchange of intelligence and coordinate activities across the law enforcement community within a specific geographic area. The task forces are staffed by federal, state, and local law enforcement officers.

¹⁰The Community Counterterrorism Board is part of the Director of Central Intelligence's Counterterrorist Center. Its mission is to advise and assist the Director of Central Intelligence in coordinating national intelligence on terrorism-related issues and to promote the effective use of intelligence resources for this purpose. The Board is interagency staffed and functions as the executive secretariat to the Interagency Intelligence Committee on Terrorism.

threat and risk assessments. For example, the multinational oil company we visited performed a risk assessment for its production and export facilities and operations in Chad, a country with ongoing civil strife. For that risk assessment, company officials noted that the multidisciplinary team generated twice as many threat scenarios (46) as in the average risk assessment. In addition, the President's Commission on Critical Infrastructure Protection recommended that other complex subjects—such as the nation's telecommunications, transportation, and banking and finance systems/infrastructures—undergo threat and risk assessments.

Conclusion

Threat and risk assessments are widely recognized as effective decision support tools for prioritizing security investments, and we identified several public and private sector organizations that use them. While it is not possible to reduce risk to all potential targets against WMD terrorism, risk assessments can help ensure that training, equipment, and other safeguards are justified and implemented based on threat, the vulnerability of the asset to an attack, and the importance of the asset.

The NLD program generally allocates \$300,000 in training equipment to each city—much of which also can be used to respond to a WMD incident. Currently, cities are receiving training and deciding on equipment purchases without the benefit of formal threat and risk assessments. Threat and risk assessments, if properly done, would be cost-effective and would help cities get training and select equipment that would provide the greatest benefit, whether purchased with NLD program funds, through other federal programs, or with cities' own funds. Although there are challenges to doing WMD terrorism threat and risk assessments of NLD cities, these difficulties could be overcome through federal and city collaboration. While other federal agencies, such as DoD, the Department of Health and Human Services, and the Environmental Protection Agency, would be important players on a federal-city risk assessment team, the FBI is in the best position to lead and facilitate risk assessments.

Matter for Congressional Consideration

The Congress may wish to consider amending the Defense Against Weapons of Mass Destruction Act to require that threat and risk assessments be included and funded as part of the assistance provided under the act. The legislation should specify that the assessments be a federal-city collaborative effort, with the FBI taking the lead in facilitating such assessments, with inputs and assistance from the intelligence

community and appropriate federal agencies, including DOD. The legislation should allow the FBI to pilot a risk-assessment approach or model on one or two cities, and make any necessary adjustments to the model or process before doing risk assessments on the remaining NLD cities. The legislation should further provide that the assessments be used to guide decision-making to determine cities' training and equipment requirements and their priorities in alignment with the most likely threat scenarios with the severest consequences.

Agency Comments and Our Evaluation

The DOE, the FBI, the Federal Emergency Management Agency, the Central Intelligence Agency, and the DOD reviewed a draft of this report. These agencies provided written comments except DOD, which provided official oral comments. Written comments and our responses appear in appendixes III to VI. DOE agreed that federal-city collaborative threat and risk assessments should be required in the NLD program and noted that equipment purchases should be delayed until risk assessments are complete to ensure that the appropriate equipment is obtained. The Federal Emergency Management Agency strongly endorsed the concept of risk assessment and highlighted the value of applying such techniques to the threat posed by terrorism.

We also discussed a draft of this report with officials from the Department of Transportation, the Department of Health and Human Services, the Environmental Protection Agency, the President's Commission on Critical Infrastructure Protection, the National Research Council, four private sector organizations, and the offices of emergency management of two NLD cities and with an outside expert. These officials generally agreed that threat and risk assessments are important, beneficial, and applicable to the NLD program. All of the agencies, including the Central Intelligence Agency, provided technical comments that we incorporated as appropriate. The FBI and DOD raised concerns about using threat and risk assessments, as discussed below.

The FBI raised concerns about the feasibility and cost of doing risk assessments on subjects the scale of large cities, but was willing to support a pilot project to assess the application of a threat and risk-assessment model to cities. As noted in our report, threat and risk assessments have been performed on or recommended for other large, complex subjects such as facilities and operations throughout the country of Chad and critical national infrastructures like telecommunications, transportation, and banking and finance systems. Our matter for

congressional consideration provides for a pilot effort to test a particular model on one or two cities before proceeding with risk assessments on the other NLD cities. For example, before completing risk assessments on the remaining NLD cities, a given model may or may not need to be adjusted.

DOD disagreed with the concept of using threat and risk assessments to determine cities' requirements for training equipment. DOD stated that the threat and risk assessment process is unlikely to make any difference in the training equipment a city selects. We believe that without having properly performed a collaborative federal-city risk assessment, DOD has little basis for its position. As noted in our report, the cities are selecting training equipment without the benefit of risk assessments, and threat and risk assessments may change the content of the equipment package selected.

DOD also emphasized that it loans \$300,000 in training equipment and materials to each city. We agree that DOD is authorized to loan and not grant equipment to U.S. cities under the NLD legislation, but we note that DOD does not expect or want the cities to return the loaned equipment. Whether the equipment is provided by loan or grant has no bearing on the desirability of performing a threat and risk assessment with sound inputs and methodology to help managers make informed judgments relative to aligning resources to needs. DOD also expressed concern that the cost of performing assessments would reduce the amount of equipment cities receive by \$20,000 to \$30,000. We acknowledge the cost of risk assessments. Nevertheless, we see no reason why that should preclude a prudent, rational, business-like assessment of the priority and need for the requested equipment.

DOD further noted that the FBI is the lead federal agency for domestic intelligence and has provided no identifiable or specific WMD terrorist threat to NLD cities. On the basis of information we obtained from the intelligence community and organizations that use risk-assessment processes, judgments about the likelihood of a variety of chemical and biological agents' successful use in threat scenarios can be made in the absence of specific threat warning data. The Community Counterterrorism Board and FBI also told us they could assist the federal-city risk-assessment teams in validating scenarios as to their realism and likelihood. Finally, DOD stated it is exploring the possibility of using NLD funds to apply the threat and risk-assessment process in one city to determine its usefulness for other domestic preparedness programs. We are encouraged by DOD's willingness to consider risk assessments for use

in other programs but continue to believe it also is appropriate for the NLD program.

In a draft of this report, we recommended that NLD program agencies require the NLD cities to collaborate with appropriate federal agencies to perform formal threat and risk assessments with valid threat data. We also recommended that the assessments be used to help define and prioritize NLD cities' requirements for federally funded equipment purchases for dealing with WMD terrorism. Based on comments received and further discussions with agency officials, we have determined that legislation would be needed to achieve the intent of our recommendations. Therefore, we have deleted the recommendations and included a matter for congressional consideration that contains the key elements of our original recommendations.

Scope and Methodology

To identify organizations that apply risk management principles to safeguard assets against numerous threats and assess the applicability of these principles for the NLD domestic preparedness program, we interviewed officials and reviewed related documents at the following organizations:


- Exxon Company International, Florham Park, New Jersey;
- Trident Data System, Oakton, Virginia;
- Computer Sciences Corporation, Springfield, Virginia;
- Science Applications International Corporation, San Diego, California;
- President's Commission on Critical Infrastructure Protection, Rosslyn, Virginia;
- Defense Special Weapons Agency, Force Protection Office, Alexandria, Virginia;
- DOE, Office of Safeguards and Security, Germantown, Maryland;
- FBI, National Security Division, Domestic Terrorism/Counterterrorism Planning Section, Washington, D.C.;
- Office of the Director of Central Intelligence, Community Counterterrorism Board, Washington, D.C.;
- FAA, Office of Civil Aviation Security Operations, Washington, D.C.;
- Department of Transportation, Research and Special Programs Administration, Washington, D.C.; and
- National Academy of Sciences, National Research Council, National Materials Advisory Board, Washington, D.C.

We also met with officials from DOD, DOE, the FBI, and the Community Counterterrorism Board to discuss the WMD terrorism threat and reviewed pertinent documentation, including a relevant National Intelligence Estimate and update.

To determine how cities that were selected for the NLD domestic preparedness program established their emergency response requirements for dealing with WMD terrorist incidents, we reviewed documents and met with DOD officials from the Office of the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict; the Office of the Army Deputy Chief of Staff for Operations and Plans, Military Support Division; and the Army Chemical and Biological Defense Command, Domestic Preparedness Office. We also reviewed documents and met with officials from the FBI's Domestic Terrorism/Counterterrorism Planning Section; DOE's Office of Emergency Management; and the Federal Emergency Management Agency's Terrorism Coordination Unit. Additionally, we spoke with city emergency management officials from New York City, New York, and Philadelphia, Pennsylvania. We also reviewed documents available at the time of our review for 11 of the first 27 cities scheduled for NLD program assistance.

We conducted our review from September 1997 to January 1998 in accordance with generally accepted government auditing standards.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution of this report until 5 days after its issue date. At that time, we will send copies to the appropriate congressional committees; the Director, Office of Management and Budget; the federal agencies discussed in this report; and other interested parties. If you have any questions about this report, please contact me at (202) 512-3504. Major contributors to this report were Davi M. D'Agostino and Marc J. Schwartz.



Richard Davis
Director, National Security
Analysis

Contents

Letter		1
Appendix I		20
Selected	Federal Aviation Administration—Federal Bureau of Investigation Joint Threat and Vulnerability Assessments	20
Organizations That	Defense Special Weapons Agency Vulnerability Assessments	20
Use or Recommend	Department of Energy's Ongoing Nuclear Security Program	21
Threat and Risk	Surface Transportation Vulnerability Assessment	21
Assessments in Their	The President's Commission on Critical Infrastructure Protection	22
Programs		
Appendix II		23
A Multinational Oil	Step 1: Determine the Value of Assets and Judge Consequences of Loss	23
Company's Five-Step	Step 2: Identify Threats and Pair With Assets	23
Qualitative	Step 3: Identify Asset Vulnerabilities	23
Risk-Assessment	Step 4: Determine Risk Through Scenarios	23
Process	Step 5: Identify Actions, as Necessary, That Lead to Risk Reduction	24
Appendix III		25
Comments From the		
Department of Energy		
Appendix IV		29
Comments From the		
Federal Bureau of		
Investigation		
Appendix V		32
Comments From the		
Federal Emergency		
Management Agency		

Appendix VI Comments From the Central Intelligence Agency	35
Related GAO Products	39
Tables	
Table 1: Probability Levels of an Undesired Event	7
Table 2: Severity Levels of Undesired Event Consequences	7
Figures	
Figure 1: Factors Considered in Making Risk Management Decisions	3
Figure 2: Risk-Assessment Matrix	8

Abbreviations

DOD	Department of Defense
DOE	Department of Energy
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
NLD	Nunn-Lugar-Domenici
WMD	Weapons of Mass Destruction

Selected Organizations That Use or Recommend Threat and Risk Assessments in Their Programs

Federal Aviation Administration— Federal Bureau of Investigation Joint Threat and Vulnerability Assessments

Section 310 of the Federal Aviation Reauthorization Act of 1996 (P.L. 104-264) requires the Federal Aviation Administration (FAA) and the Federal Bureau of Investigation (FBI) to conduct joint threat and vulnerability assessments every 3 years, or more frequently as necessary, at each airport determined to be “high risk.” The FAA has identified a number of airports likely to be high risk based on the operational characteristics of an airport, such as flight activity and the number of carriers. These airports account for about 92 percent of all passenger airplane boardings in the United States.

The FBI is providing threat data (i.e., intelligence and law enforcement information) that the FAA is using to develop threat assessments specific to the airport or the metropolitan area in which the high-risk airport is located. The FAA has developed a questionnaire to assess, quantify, and rank airport vulnerabilities. The questionnaire, which contains almost 400 items, was field tested in December 1997 at Baltimore-Washington International Airport. Washington-Dulles International Airport was assessed in January 1998, and beginning in February 1998, two airports per month will be assessed. A team of FBI, FAA, and airport officials are completing the questionnaire; however, the FAA is interpreting the results and recommending countermeasures.

Defense Special Weapons Agency Vulnerability Assessments

In response to the Khobar Towers bombing in Saudi Arabia in 1996, the Chairman of the Joint Chiefs of Staff tasked the Defense Special Weapons Agency with performing vulnerability assessments. Assessment teams plan to visit more than 500 of the highest priority Department of Defense (DOD) facilities located within the United States and abroad, with the goal of conducting 100 assessments per year.¹ After the first 6 months, 47 assessments had been completed. These vulnerability assessments focus mainly on mass casualty incidents caused by high-intensity explosives, considered to be the most likely threat, but incidents involving weapons of mass destruction are also being considered.

A vulnerability assessment team consists of experienced military and civilian personnel from a range of disciplines, including structural and civil engineering, security, and operations readiness. The assessment team uses a risk-assessment model to identify and rank order a site’s strengths and weaknesses. The specific elements of the model include asset criticality,

¹The Defense Special Weapons Agency defines a DOD facility as a fixed installation with at least 300 persons.

site vulnerability, and the ease with which a threat can gain access to an asset.

Department of Energy's Ongoing Nuclear Security Program

The Department of Energy (DOE) states it uses a Design Basis Threat to develop security policy and requirements, to help plan its security program, and to help with facility design. The Design Basis Threat is based on a fusion of threat and intelligence assessments provided by numerous sources that address potential threat activities and adversaries. DOE develops and models threat scenarios that link specific threats to specific asset vulnerabilities. DOE uses these scenarios to select countermeasures designed to reduce the current level of risk. This analysis is based on a graded protection concept,² under which varying levels of protection are acceptable based on the value of the assets being protected.

Each DOE facility is required to conduct a vulnerability assessment to identify possible paths a threat may take to reach an asset. Threats are prioritized according to their potential impact and assigned consequence values that reflect their relative ranking. For example, a compromised assembled nuclear weapon has a significantly higher consequence value than does a stolen or diverted Category III material. DOE notes that the vulnerability assessment process provides a method for allocating security resources according to the level of risk. DOE has several automated tools it uses to conduct its vulnerability assessments.

Surface Transportation Vulnerability Assessment

In accordance with the Omnibus Consolidated Appropriations Act for Fiscal Year 1997, the Department of Transportation's Research and Special Programs Administration is conducting a comprehensive vulnerability assessment of the U.S. surface transportation infrastructure (i.e., road, rail, transit, pipeline, and maritime). The goal of the assessment is to (1) identify and rank key threats to and critical vulnerabilities of the national transportation infrastructure and (2) recommend possible countermeasures to improve infrastructure protection from a host of threats such as terrorism, accidents, and natural disasters. This assessment is scheduled to be completed in June 1998.

Based on the results of the vulnerability assessment, a National Research Council Advisory Study will attempt to identify technologies and processes to improve surface transportation security against threats that

²DOE designates each of its facilities as Category I, II, III, or IV. A facility designated as a Category I is the highest priority, followed by II, III, and IV in descending order of priority.

**Appendix I
Selected Organizations That Use or
Recommend Threat and Risk Assessments
in Their Programs**

could seriously disrupt safety and operations. A final report is expected in the spring of 1999.

**The President's
Commission on
Critical Infrastructure
Protection**

President Clinton signed Executive Order 13010 on July 15, 1996, establishing the President's Commission on Critical Infrastructure Protection. The Commission's mandate was to develop a national strategy for protecting the country's critical infrastructures from a spectrum of threats and assuring their continued operation. The eight critical infrastructures include the electric power system; gas and oil (storage and transportation); telecommunications; banking and finance; transportation; water supply systems; emergency services (including medical, police, fire, and rescue); and continuity of government operations. Threats to these infrastructures fall into two categories: physical threats to tangible property and computer-based attacks on the information or communications components that control critical infrastructures. Because many of the critical infrastructures are privately owned and operated, the Commission comprises representatives from the federal government and the private sector.

The Commission issued its final report to the President on October 20, 1997. The report concluded that the owners and operators of critical infrastructures lack sufficient threat and vulnerability information to make informed risk management decisions. Consequently, the Commission recommended that owners and operators, in collaboration with the federal government, conduct periodic threat, vulnerability, and risk assessments.

A Multinational Oil Company's Five-Step Qualitative Risk-Assessment Process

Step 1: Determine the Value of Assets and Judge Consequences of Loss

Critical assets that require protection are identified and ranked according to what their loss would represent. At the outset, the company forms a risk-assessment team of five to eight individuals from various disciplines, including security, emergency or asset management, finance, senior management, information systems, and cultural anthropology. Team members are generally dedicated full time to the risk assessment. The team agrees on the period of time to be covered by the risk assessment (for example, to the year 2010); the physical boundaries of the assessed activity; and the consequences of concern (for example, safety, public disruption, environmental effects, financial impact). The company uses the descriptive values in DOD's Military Standard 882C, System Safety Program Requirements, to categorize the loss as either catastrophic, critical, marginal, or negligible. The risk assessment team also assigns values to key assets.

Step 2: Identify Threats and Pair With Assets

Threat identification is the most important step in the risk-assessment process. If threats are not accurately identified, the risks they represent cannot be reduced or eliminated. Threats the company is concerned with include trusted or incompetent insiders, criminals, terrorists, and environmental and system-induced threats. In characterizing the threat, the company examines the historical record of security and safety breaches and obtains location-specific threat information from the intelligence community and open sources. These threats are then paired with company assets that represent likely targets.

Step 3: Identify Asset Vulnerabilities

The risk-assessment team identifies weaknesses in the company's critical assets that could be exploited by the threats identified in step 2 and determines their nature and source. Methods used to identify vulnerabilities include evaluating data obtained through surveys and historical data from related incidents and applying formal vulnerability analysis techniques. Asset vulnerabilities can include operations and processes, policies and procedures, physical and technical security, information security, personnel security, and operations security.

Step 4: Determine Risk Through Scenarios

The risk-assessment team develops credible risk scenarios to describe how undesired events may occur and to determine the effect of each undesired event on the company's assets. The set of scenarios may not be an exhaustive list of all possible undesired events, but each valid threat that has been identified should be represented in at least one scenario. The

oil company typically develops 20 to 25 scenarios for each of its risk assessments. The team assigns a high-, medium-, moderate-, or low-risk rating for each scenario based on the severity of consequences and the likelihood of each scenario occurring. Before likelihood values are assigned, the team must agree on the time period under study and a quantitative definition of the descriptive rankings. For example, the team might agree that "frequent" means that an undesired event or threat would occur at least two times per year, or that the odds are 9 in 10 of an incident occurring in annual operations for the duration of the study period. Company officials stated that they avoid focusing on worst-case scenarios that are not likely to occur.

Step 5: Identify Actions, as Necessary, That Lead to Risk Reduction

Countermeasures are actions that either eliminate the causes or reduce the effects of one or more vulnerabilities. Countermeasures could include additional checkpoints controlling access to a facility, security cameras, personnel background investigations, new procedures, or chemical protective gear. Countermeasures are identified and inserted into a scenario, and the risk rating for that scenario is recalculated to account for the effect of the countermeasure. The company selects countermeasures on the basis of factors such as whether they reduce the probability of an undesired event occurring, their implementing cost, and any additional enforcement and audit requirements. Countermeasures can be prioritized by considering a number of factors, including the amount of resulting risk reduction, cost, difficulty to implement, or a combination thereof. Usually, there is a point beyond which adding countermeasures will raise costs without appreciably enhancing the protection afforded.

Comments From the Department of Energy

Note: GAO comments supplementing those in the report text appear at the end of this appendix.



Department of Energy
Washington, DC 20585

March 9, 1998

Mr. Richard Davis
Director, National Security Analysis
National Security and
International Affairs Division
U.S. General Accounting Office
Washington, D.C. 20548

Dear Mr. Davis:

The Department of Energy appreciates the opportunity to review report NSIAD-98-74, "COMBATING TERRORISM: Threat and Risk Assessments Can Help Prioritize and Target Program Investments." The General Accounting Office reviewed the implementation of the Nunn-Lugar-Domenici domestic preparedness program prescribed by the Defense Against Weapons of Mass Destruction Act of 1996. The Department agrees, in general, with the content of the report and is providing the attached specific comments.

Sincerely yours,

A handwritten signature in cursive script, appearing to read "Thomas S. Ryder".

Thomas S. Ryder
Director
Office of Resource Management
Office of Nonproliferation
and National Security

Comments on
General Accounting Office Draft Report

COMBATING TERRORISM
Threat and Risk Assessments
Can Help Prioritize and Target Program Investments
NSIAD-98-74

Specific Comments

Page 6, paragraph 2, following "...DOD military bases."

Now on p. 5.

See comment 1.

add **"The Department of Energy (DOE) uses a graded approach to protect site safeguards and security interests based on risk and vulnerability assessments. Under the graded approach, DOE elements develop and implement protection and control programs at a level of effort commensurate with the security interest's importance or the impact of its loss, destruction, or misuse."**

Page 8, last sentence (comment)

Now on p. 7.

See comment 1.

DOE is of the opinion that a site should at least review the protection requirements against a worst case scenario. In the case of an oil company, a likely target may be more practical than worst case. However, in the case of a city responding to a weapon of mass destruction threat, the assessment must consider adversarial capability, not just intent. Resource restrictions may preclude complete protection against worst case, but worst case must be factored into any program.

Page 11, first paragraph

Now on p. 9.

See comment 1.

following "Defense Special Weapons Agency"

add **"the Department of Energy,"**

Page 13, second paragraph (comment)

Now on p. 11.

See comment 1.

DOE is of the opinion that cities must be either given access to, or be briefed by, the FBI on terrorist capabilities, methods of operations, likely targets, and any incidents known to have occurred in or around their city.

Page 15, second paragraph (comment)

Now on p. 12.

See comment 2.

DOE is of the opinion that cities must continue to identify equipment and resources necessary to respond to a WMD incident in parallel to a vulnerability assessment or risk

Appendix III
Comments From the Department of Energy

assessment. Purchase of equipment should be delayed until vulnerability assessment or risk assessment work is complete to ensure that the appropriate equipment is obtained. Finally, cities should plan their strategy around "graded" protection levels. DOE has training courses developed on the conduct of vulnerability assessments, risk assessments, approach methodology, and strategy development that can be provided to cities.

Page 20, Appendix I, DOE section, first paragraph

Now on p. 21.

See comment 1.

add **"The Department of Energy's Design Basis Threat serves as a foundation on which all safeguards and security policy and requirements are developed and a basis for security program planning and facility design. The Design Basis Threat is a document broadly based on the fusion of current threat assessments and intelligence provided by numerous sources. The Design Basis Threat addresses a range of potential threat activities and potential adversaries. Protection of national security, to include nuclear assets, is central and the DOE has developed a layered protection strategy. Each layer is designed to be mutually complementary while the whole system is designed to provide a high degree of protection."**
before the first sentence of the first paragraph.

See comment 1.

add **"The VA process provides a method for acquiring and analyzing the information necessary in coordinating and allocating resources and to provide information necessary to establish levels of risk as required by national-level or DOE directives. Over the years DOE, in conjunction with the national laboratories, has developed several automated vulnerability assessment programs which could be available for use by other agencies.**

See comment 3.

DOE is also a member of a research group which, in association with the above mentioned oil company, and a highly recognized business school of a major U.S. university, is developing an automated security management tool which has been designated Value Added Model (VAM). VAM reviews the application of alternate security strategies to specific threat postures and estimates the optimal net present value resulting from investments in these strategies. Using data on the estimated costs and expected effectiveness of security strategies and on scenarios and VA's the model produces a variety of measures of financial effectiveness of security strategies, including net present value, return on investment and/or cost/benefit ratio."
after the last sentence, first paragraph, page 21.

The following are GAO's comments on DOE's letter, dated March 9, 1998.

GAO Comments

1. We modified the text to reflect DOE's comment.
2. We agree that it is prudent to delay the purchase of equipment until a vulnerability or risk assessment is complete to ensure that the appropriate equipment is obtained.
3. We were briefed on the Value Added Model in our meetings with officials from DOE and the multinational oil company, and the business school that DOE refers to. Oil company officials stated that they were using this model in their risk assessments to assess and compare the financial impact of various security strategies. We note, however, that other measures of effectiveness exist. Therefore, we omitted a discussion of the Value Added Model from this report to avoid emphasizing one criterion—the financial cost benefit of competing sets of countermeasures—over others that can also lead to risk reduction.

Comments From the Federal Bureau of Investigation

Note: GAO comments supplementing those in the report text appear at the end of this appendix.



U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535

March 4, 1998

Mr. Richard Davis
Director, National Security Analysis
Government Accounting Office
Washington, D.C. 20548

Dear Mr. Davis:

The Federal Bureau of Investigation (FBI) appreciates the opportunity to comment on your agency's draft report entitled, "Combating Terrorism: Threat and Risk Assessments Can Help Prioritize and Target Program Investments," and value your continued interest in this important program.

As outlined in this report, the recommendation is being made that "NLD program agencies require NLD cities to collaborate with appropriate Federal agencies, such as the FBI and other intelligence agencies, to perform formal threat and risk assessments with valid threat data," and that such threat and risk analyses be used to define and prioritize Nunn-Lugar cities' requirements for equipment purchased with Federal funds.

The legislation creating the Domestic Preparedness Program did not require that threat and/or risk assessments be performed either to select the cities which would receive assistance or determine a city's needs for equipment to deal with a Weapon Of Mass Destruction (WMD) incident. Congress recognized that it is not essential to determine or assess vulnerabilities attractive to a terrorist as a pre-condition to training and equipping emergency personnel with the knowledge and tools to adequately respond to a terrorist incident. Further, national organizations have previously conducted studies to identify basic training and equipment needs that concluded even the best prepared cities do not always have the inherent capability to manage the potential magnitude of a WMD incident. The training and equipment being provided to these cities under the Domestic Preparedness Program is considered fundamental to enhancing any city's present day capabilities. City visits conducted by the interagency community have affirmed that many of the cities have already identified their training and equipment needs and seek only additional materials and funding to accomplish their future planning.

See comment 1.

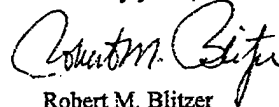
Appendix IV
Comments From the Federal Bureau of
Investigation

See comment 2.

Nevertheless, there is no question that threat and risk assessments are widely recognized as valid tools in diminishing the vulnerabilities of a specific facility or target. The FBI conducts such assessments on a regular basis in preparing for national special events and preventing acts of terrorism to critical infrastructures, such as transportation nodes. However, the fora for these events are limited in scope and size, and generally are comprised of fixed points in which to assess vulnerabilities and strengths. Applying this process to an entire metropolitan city would be challenging and possibly time-consuming since the correlation between risk analysis and the occurrence of an actual terrorist incident involving a WMD may be impossible to identify. Notwithstanding, the FBI would be willing to support a pilot project to assess the application of a threat and risk assessment model to cities and would request additional funding and manpower to carry out this initiative. Additionally, we recommend that any such undertaking be reviewed by the interagency collectively to assess the feasibility of expanding this program to all Nunn-Lugar cities or continue in the proactive course already underway as previously outlined in past studies.

We hope that you will find these comments useful in the finalization of your report. Should you have any further questions concerning this initiative, please do not hesitate to contact me at (202) 324-5386.

Sincerely yours,



Robert M. Blitzer
Chief
Domestic Terrorism/
Counterterrorism Planning Section
National Security Division

The following are GAO's comments on the FBI's letter, dated March 4, 1998.

GAO Comments

1. We agree, and our report notes, that the Nunn-Lugar-Domenici (NLD) legislation did not require that threat and risk assessments be performed either to select the cities that will receive assistance or to determine those cities' needs for training and equipment to deal with weapons of mass destruction (WMD) terrorism incidents. However, the legislative history of the Defense Against Weapons of Mass Destruction Act of 1996 contains no substantive discussion or any other indication of what criteria should be used to select the cities or determine their training and equipment needs. We agree that earlier studies have identified training and equipment that would enhance the capabilities of city emergency personnel to respond to WMD terrorism. However, as noted in our report, without a formal threat and risk-assessment process to define requirements, it is unclear that the training and equipment selected will provide the greatest benefit to the cities.

2. Our matter for congressional consideration provides for a pilot effort to test a particular model on one or two cities before proceeding with risk assessments on the other NLD cities. For example, before completing risk assessments on the remaining NLD cities, a given model may or may not need to be adjusted.

Comments From the Federal Emergency Management Agency

Note: GAO comments supplementing those in the report text appear at the end of this appendix.



Federal Emergency Management Agency

Washington, D.C. 20472

FEB 27 1998

Mr. Richard Davis
Director, National Security Analysis
National Security and International
Affairs Division
United States General Accounting Office
Washington, DC 20548

Dear Mr. Davis.

Thank you for the opportunity to review the draft report "Combating Terrorism: Threat and Risk Assessment Can Help Prioritize and Target Program Investments" (GAO/NSIAD-98-74).

The draft report consists of a discussion of the threat and risk assessment as important steps for U.S. cities to take in preparing to deal with the consequences of terrorist incidents involving weapons of mass destruction (WMD) and the following single recommendation:

...that NLD [Nunn-Lugar-Domenici] program agencies (DOD, DHHS, DOE, FBI, FEMA, and EPA) require the NLD cities to collaborate with appropriate federal agencies, such as the FBI and other intelligence agencies, to perform formal threat and risk assessments with valid threat data [in order to] help define and prioritize the NLD cities' requirements for equipment to deal with WMD terrorism that is purchased with federal funds [emphasis added].

FEMA strongly endorses the concept of risk assessment. It is the key to pre-disaster hazard mitigation which we see as the foundation of emergency management. Our efforts in this area often focus on mitigation of natural hazards; however, the value of applying such techniques to the threat posed by terrorism is clear.

While we concur with the comments in the report and the discussion on the value of risk assessment, we have reservations regarding the recommendation to require cities to perform these assessments.

The Department of Defense is the lead agency for the NLD program, and the Federal Bureau of Investigation performs official assessments of the domestic terrorism threat. These organizations must address whether it is feasible (or legal) to: (1) require vulnerability assessments in return for NLD equipment loans; or (2) share sensitive threat information on the scale required to implement this General Accounting Office (GAO) recommendation.

See comment 1.

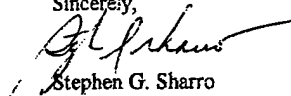
See comment 1.

**Appendix V
Comments From the Federal Emergency
Management Agency**

2

Since the Federal Emergency Management Agency is not the lead for the NLD Domestic Preparedness Program and is not a regulatory agency, it is thus not in a position to impose this requirement.

Sincerely,



Stephen G. Sharro
Acting Director
Terrorism Coordination Unit

The following are GAO's comments on the Federal Emergency Management Agency's letter, dated February 27, 1998.

GAO Comments

1. On the basis of agency comments we received and further discussions with agency officials, we added a matter for congressional consideration and eliminated our draft recommendation. The matter for congressional consideration would clarify NLD legislation to require threat and risk assessments in the program. Regarding the issue of sharing threat information, officials from the intelligence community, including the FBI, stated that they could work with the NLD-selected cities to provide valid threat data and to validate any threat scenarios generated by multidisciplinary teams performing threat and risk assessments. In addition, the Central Intelligence Agency and the FBI did not raise such concerns in their official comments on a draft of this report.

Comments From the Central Intelligence Agency

Note: GAO comments supplementing those in the report text appear at the end of this appendix.

Central Intelligence Agency



Washington, D.C. 20505

6 March 1998

Mr. Richard Davis
Director, National Security Analysis
National Security and
International Affairs Division
United States General Accounting Office
Washington, D.C. 20548

Dear Mr. Davis:

This letter is in response to your letter of 28 January 1998, which forwarded copies of your draft report "COMBATING TERRORISM: Threat and Risk Assessments Can Help Prioritize and Target Program Investments" and asked for our comments prior to its release. We appreciate the opportunity to review the draft copy.

Officials on the Community Counterterrorist Board and in the Counterterrorism Center have carefully reviewed the report and propose the following changes:

- Page 13. Second full paragraph. Change the first sentence to read: "To perform realistic threat assessments, city officials would require access to valid foreign and domestic threat data from the Intelligence Community, local law enforcement, and public sources."
- Page 14. First full paragraph. Change the first sentence to read: "The Intelligence Community's threat-reporting on foreign-origin terrorism is often general, rarely city specific, and without further clarification could be difficult to use for threat and risk assessments of Nunn-Lugar-Domenici cities."
- Page 14. First full paragraph. Change the last sentence to read: "Absent this level of specificity, the cities still can develop threat scenarios which the Intelligence Community can compare to its foreign threat reporting and validate with respect to their realism and likelihood of occurrence."

Now on p. 11.
See comment 1.

Now on p. 11.
See comment 1.

Now on p. 11.
See comment 1.

Appendix VI
Comments From the Central Intelligence
Agency

Mr. Richard Davis

If I may be of further assistance, please let me know.

Sincerely,



John H. Moseman
Director of Congressional Affairs

**Appendix VI
Comments From the Central Intelligence
Agency**

The following are GAO's comments on the Central Intelligence Agency's letter, dated March 6, 1998.

GAO Comments

1. We modified the text to reflect the Central Intelligence Agency's comment.

**Appendix VI
Comments From the Central Intelligence
Agency**

Related GAO Products

Combating Terrorism: Spending on Governmentwide Programs Requires Better Management and Coordination (GAO/NSIAD-98-39, Dec. 1, 1997).

Combating Terrorism: Efforts to Protect U.S. Forces in Turkey and the Middle East (GAO/T-NSIAD-98-44, Oct. 28, 1997).

Combating Terrorism: Federal Agencies' Efforts to Implement National Policy and Strategy (GAO/NSIAD-97-254, Sept. 26, 1997).

Combating Terrorism: Status of DOD Efforts to Protect Its Forces Overseas (GAO/NSIAD-97-207, July 21, 1997).

Chemical Weapons Stockpile: Changes Needed in the Management Structure of Emergency Preparedness Program (GAO/NSIAD-97-91, June 11, 1997).

State Department: Efforts to Reduce Visa Fraud (GAO/T-NSIAD-97-167, May 20, 1997).

Aviation Security: FAA's Procurement of Explosives Detection Devices (GAO/RCED-97-111R, May 1, 1997).

Aviation Security: Commercially Available Advanced Explosives Detection Devices (GAO/RCED-97-119R, Apr. 24, 1997).

Terrorism and Drug Trafficking: Responsibilities for Developing Explosives and Narcotics Detection Technologies (GAO/NSIAD-97-95, Apr. 15, 1997).

Federal Law Enforcement: Investigative Authority and Personnel at 13 Agencies (GAO/GGD-96-154, Sept. 30, 1996).

Aviation Security: Urgent Issues Need to Be Addressed (GAO/T-RCED/NSIAD-96-151, Sept. 11, 1996).

Terrorism and Drug Trafficking: Technologies for Detecting Explosives and Narcotics (GAO/NSIAD/RCED-96-252, Sept. 4, 1996).

Aviation Security: Immediate Action Needed to Improve Security (GAO/T-RCED/NSIAD-96-237, Aug. 1, 1996).

Passports and Visas: Status of Efforts to Reduce Fraud (GAO/NSIAD-96-99, May 9, 1996).

Terrorism and Drug Trafficking: Threats and Roles of Explosives and Narcotics Detection Technology (GAO/NSIAD/RCED-96-76BR, Mar. 27, 1996).

Nuclear Nonproliferation: Status of U.S. Efforts to Improve Nuclear Material Controls in Newly Independent States (GAO/NSIAD/RCED-96-89, Mar. 8, 1996).

Aviation Security: Additional Actions Needed to Meet Domestic and International Challenges (GAO/RCED-94-38, Jan. 27, 1994).