E-Notes The Question of Bioterrorism Preparedness

by Stephen Gale and Gregory Montanaro

March 31, 2005

This is the text of testimony before the Senate Committee on Public Health & Welfare, Commonwealth of Pennsylvania, on March 22, 2005. **Stephen Gale**, Ph.D., is Co-Chair of the Foreign Policy Research Institute's **Center on Terrorism, Counter-Terrorism, and Homeland Security**; **Gregory Montanaro** is Executive Director of FPRI's Center on Terrorism, which is supported in part by a grant from the Department of Community and Economic Development, Commonwealth of Pennsylvania. The views expressed are those of the authors alone.

> "Let me emphasize this: Homeland security does not simply rest upon federal action; it requires collective national action. When it comes to the protection of our people, our infrastructure, our companies, our communities, our country, we all have a role to play if we are to frustrate the enemy's intentions. For two years now, it has been the responsibility of Homeland Security to lead the unified national effort to daily and consistently improve our security and preparedness measures. The federal government has unique access to intelligence, powerful investigative tools, strong resources. But the federal government cannot fund or address all of the risks involved with terrorism on its own. To complete our mission, we must and do count heavily on partnerships with our state and local governments and the private sector." —Remarks of Secretary Michael Chertoff, U.S. Department of Homeland Security, before the George Washington University Homeland Security Policy Institute, Washington, D.C.

Mr. Chairman, Senator Hughes, members of the Public Health & Welfare Committee:

We want to thank you for the opportunity to be here today. We are honored that the Senate has invited us to testify on the Commonwealth's preparedness with respect to potential bioterrorism attacks.

Neither Mr. Montanaro nor I are healthcare professionals. However, we do have a broad understanding of terrorism, the potential effects of bioterrorism, and the measures that the Commonwealth needs to employ in order to prevent and/or mitigate the effects of bioterrorism attacks.

As we understand it, the primary reason for this hearing is to address reports that suggest that the Commonwealth is prepared for neither bioterrorism attacks nor natural health-care crises such as pandemic flu epidemics. As we see it, while it is useful to analyze the general state of the health care infrastructure, treatment facilities, and manpower, it is critical that you understand that the Commonwealth must deal with preparations for bioterrorism attacks independently of the procedures used in standard healthcare planning. Terrorist attacks are volitional and, unlike natural events, bioterrorism attacks will be planned and executed in order to achieve objectives that are only indirectly related to the loss of lives or the disruption America's healthcare system. As we see it, then, to the extent that any of the states is "prepared" to deal with the threat

of a bioterrorism attack, the Commonwealth of Pennsylvania is certainly not in a worse position—and, in fact, may be significantly better.

Given our understanding of terrorism and bioterrorism, we offer this Committee a clear message today:

As we all know, much of what is now called "homeland security" is, today, a mission of state and local governments, and those private sector firms that provide and support the public infrastructure. As such, we believe that the Commonwealth, through its Office of Homeland Security, PEMA, and the State Police, must take at least the following four Steps in the near future:

- Use the full range of detailed, integrated intelligence from federal, state, and other agencies to identify those terrorist organizations—both international and domestic — that are either capable of executing bio-terrorism attacks or can provide support to such groups;
- In cooperation with other states, develop a detailed, unified account of the Commonwealth's vulnerabilities, the potential attack scenarios, and the full range of the impacts of bioterrorism attacks using the frameworks outlined in the Homeland Security Council's July, 2004 report, "Planning Scenarios," and the General Accounting Office's (GAO) 1998 report on "Combating Terrorism: Threat and Risk Assessments Can Help Prioritize and Target Program Investments."
- Using the steps outlined in the GAO report, adopt procedures for using a standardized "security impact assessment" (SIA) to determine allocations and set priorities for investments in security;
- Based on the results of the SIA, develop and implement effective and efficient policies, programs, and measures that meet the Commonwealth's objectives.
- Given these recommendations, we thus see the concerns about the shortcomings of the Commonwealth's preparedness for bioterrorism attacks and natural healthcare crises as moot. Evaluating "preparedness" for bioterrorism attacks and major healthcare crises is, today, a far more complex task than it was in what seems now to be a distant past and, without directly addressing the following issues, such evaluations are probably impossible:
- Assuming that there are groups that have the resources and capacities to carry out bioterrorism attacks, what is the Commonwealth's current projection of the likelihood of specific kinds of attacks and attack scenarios?
- Given intelligence on the potential for specific bioterrorism attack scenarios, what level and kinds of counter-terrorism and healthcare resources will be required to prevent the attacks and/or mitigate the effects?
- Based on the Commonwealth's assessment of the general resources needed for counter-terrorism and healthcare programs, what additional resources will the healthcare system require to successfully manage the effects of each specific type of bioterrorism attack?

Addressing these issues—rather than simply making the ad hoc judgments based on out-dated guidelines — will, we believe, provide the foundation for informed responses to the Commonwealth's ultimate concerns: "What do we need to do to put the fears of the Commonwealth's citizens to rest about (1) the effectiveness of Pennsylvania's support for national efforts to prevent bioterrorism attacks and (2) the effectiveness of the State's plans and programs for providing healthcare treatment should such attacks occur?"

Consistent with risk management planning in all organizations, the operational message today is that the Commonwealth must conduct what amounts to structured due diligence analyses before making unsupported judgments about exposures, vulnerabilities, and changes in healthcare delivery systems — judgments that generally reflect only the standards that have been used in the past to justify requests for supplemental funding. If nothing else, the descriptions provided in the Homeland Security Council's "Planning Scenarios" should remind all of us that planning for responses to bioterrorism attacks cannot be based on procedures that have served us in the past. Or, put even more directly, the prospect of bioterrorism attacks means that we can no longer rely on "business- as-usual" to guide planning for the Commonwealth's healthcare systems.

For the record, we should also state that the Foreign Policy Research Institute's (FPRI) Center on Terrorism, Counter-Terrorism, and Homeland Security has already circulated a draft public policy initiative that outlines a proposed "Security Impact Assessment" process. [See **"From MAD to MUD: Dealing with the New Terrorism,"** by Stephen Gale and Lawrence Husick, ***FPRI Wire***, February 2003.

As will be discussed later on, our research indicates that effective and efficient counter-terrorism and security can only be identified where there are clear standards for due diligence evaluations—and where the standards and analyses use methods and decision-support technologies that reflect the potential for bioterrorism attacks.

Unlike the actuarial assessments used by insurers, the SIA process integrates procedures that employ detailed intelligence data, expert-driven scenario generation, and financial analysis tools to provide evaluations of the likelihood of attacks and estimates of the added value—the net present value — of specific recommendations for investments in healthcare security and infrastructure.

Understanding Terrorists and Bioterrorism

As noted earlier, in order to address the potential for specific bioterrorism attacks, we believe that the Commonwealth's due diligence process must be based on the use of detailed intelligence information to identify the terrorist groups that are capable of carrying out such actions and the expected results of a successful attack.

Aside from the odd psychopath usually found in most terrorist groups, killing per se is only rarely the objective of the leadership. Rather, the leaders of the most dangerous groups analyze and plan in much the same way as venture capitalists: actions are selected based on maximizing the expected return on investment relative to their objectives. To protect against such attacks and their effects, the Commonwealth must, therefore, use the same procures and methods now used by experts in terrorism intelligence: assessing the potential impacts of terrorist actions through the identification of (1) the objectives, capabilities, and resources of each group; and (2) the ways in which specific actions can exploit the gaps and vulnerabilities of current security systems. And keep in mind that, while there is never certainty on either side, as with venture capital investments, informed planning and execution can substantially lower risks.

The "Benefits' of Bioterrorism

Bioterrorism is complex and includes much more than just the use of bio-organisms to cause diseases that kill or disable.

- Biological organisms come in many different forms, strains, and strengths and the potential effects of bioterrorism attacks depends on the organism selected, the processes used in "weaponization," and the means for introducing and deploying the organism as a weapon;
- Beyond death and disability, bioterrorism attacks can also be targeted at the Commonwealth's ability to maintain the quality of the State's—and the entire nation's — healthcare production and delivery systems;
- In addition to the provision of medical treatments and antidotes, preventing and/or mitigating the effects of bioterrorism attacks also requires the development of effective and efficient systems for detecting biological threats before they are used as weapons, determining the etiology of diseases and the effects of healthcare disruptions, and organizations that are capable of managing the full range of skills and resources needed to deliver high quality healthcare.

Bioterrorism Attacks

As viewed by terrorist groups, bioterrorism is simply one tactic amongst many options, a tactic to be used only where it is likely to be effective in what they see as their strategy of warfare. From the perspective of the

Commonwealth and the nation, however, even the remote chance of a bioterrorism attack warrants the immediate implementation of the type of security evaluation program that we have outlined.

- Bioterrorism may only be one of a wide variety of tactics (not an end in itself) but, due to its relatively low cost and potential impacts, it may be the tactic of choice for an increasing number of terrorist groups;
- The potential for the use of bioterrorism attacks depends on the terrorist group's internal cultural justification for the use of such weapons, the availability of weaponized disease strains, training in their use, and a clear determination of what they see as the expected "benefits;"
- Since terrorist groups evaluate the potential use of bioterrorism attacks in terms of the value provided as part of a strategy of warfare — not as symbolic actions—such attacks might be just one element of a broader strategy that includes the simultaneous use of other tactics.

Status of U.S. Preparedness

Where does the US stand today with respect to making an SIA framework operational? Just what have the nation's public agencies and the private sector done to put all of the pieces of this extremely complex puzzle together and use it as a guide for developing policies and programs for protecting America and Americans? And, most importantly, what steps must be taken to implement the policies and programs?

Looking back over the three and a half years since September 11th, what we must realize is that the nation's counter-terrorism efforts have been reasonably effective only in moving the active conflict to places such as Afghanistan and Iraq. By doing this, the nation hopefully bought the time needed to address the soft-underbelly of the "War on Terror:" creating meaningful homeland security programs in an environment that values the rule of law, democracy, and freedom. (It is also wise to keep General Sullivan's keen observation in mind here: whatever else we might believe, "hope is not a method.")

That said, the dead of September 11th should always remind us that, without life, there is no liberty or pursuit of happiness. Ultimately, in a time of war — whether with nation states or terrorist organizations—the US can expect to face heightened threat levels. And, as most of the nation's security professionals and government agencies have repeatedly pointed out, it is impossible to protect everything. It is possible, however, to protect those "somethings" that are vital to the lives of Americans and the continuity of the nation's economy and society. The question, of course, is "How should we allocate resources and set priorities?"

In this context, it is easy to see just why any questions about the Commonwealth's current allocation of healthcare resources is moot. Since we have not as yet developed the standards and principles that are relevant to evaluating the likelihood of bioterrorism attacks and their expected consequences, any assessment of the Commonwealth's allocation of resources could only have been based on pre-September 11th standards or newly-created rules-of-thumb. To assume that the old standards still work or that it is simply a matter of distributing resources pro rata based on population size or targeting those areas that may have been under-serviced in normal circumstances, just misses the point: September 11, 2001 changed the meaning of "business-as-usual" and, therefore, the standards employed in such evaluations.

What is the basis for allocating healthcare resources where bioterrorism attacks are not only technically feasible, but where terrorist groups are known to be working on obtaining these weapons? What are the standards that should be used to determine and prioritize the allocations? And what processes should federal agencies and state, and local governments employ in developing the mission critical standards for due diligence reviews and determining the allocation of healthcare resources?

The research group at FPRI has established what most experts felt intuitively: that the vast majority of the high priority vulnerabilities in the nation's security systems are controlled by private sector

organizations—not governments. Thus, in the absence of national and state legislation to institutionalize standards based on something on the order of an SIA, comprehensive security due diligence reviews and the implementation of the resulting security recommendations will probably be suspect and politically unworkable.

Worse still, without the use of an SIA process, it will be virtually impossible to identify the secondary and tertiary effects of bioterrorism attacks on, for example, the availability of healthcare workers, the delivery of medical equipment and pharmaceuticals, and the maintenance of the public utility, sanitation, communications, communications, and transportation infrastructures.

To give you an idea of just what we have in mind, consider the following three examples of bioterrorism attacks:

Smallpox.
Of all of the bioterrorism attacks that we have reviewed, smallpox is by far the most infectious and deadly. It is also the attack that is most likely to create a national panic that, in turn, could lead to the long-term disruption of the nation's healthcare and public infrastructure systems. At a minimum, even a modest smallpox outbreak will probably make it infeasible to implement even a well-planned first-responder program.

As the "Dark Winter" simulation of a covert smallpox bioterrorism attack demonstrated, even an attack initiated at only three shopping malls in three cities would lead to over three million cases of smallpox and one million deaths—even with an all-out effort to quarantine the infected sites (based on the current allocation of resources) and Presidential-level command and control. As one of the simulation developers said to us, "As for the two million who did not die, you can expect that a significant number would wish that they were dead!"

What is the likelihood of a smallpox attack? Until recently, many (if not most) specialists in the field were convinced that the probability of a terrorist group obtaining or developing sizable amounts of a weaponized smallpox virus was very low. Recent intelligence has resulted in a far less sanguine assessment. Even more important, given the significance of religious rationales for al Qaeda's past actions, recent research indicates that the all-important religious "justification" for the use of smallpox as a weapon can be found in one interpretation of Sura 105 of the Koran.

Turning to the homeland security side of the equation, what is the status of the nation's current vulnerability to a smallpox attack? From the "prevention" perspective, most recent reports indicate that there is very little direct evidence one way or another. In effect, we simply do not "know" whether al Qaeda or any group has obtained the requisite virus strain or has the expertise to use it as a weapon.

From the homeland security/first-responder perspective, the indicators are much the same. For example, virtually every healthcare professional that we have interviewed in the past three years has made very similar comments: "Most of us have never seen a case of smallpox—no less a case in the early stages." "This hospital is unprepared for anything but a breakout that involves no more than four or five cases—and those cases would need to be identified very early." "Were there a large number of infected people entering the hospital, my guess is that most of the doctors and nurses would think seriously about leaving."

Given the current state of nation's healthcare facilities and the level of training in managing an outbreak, there is probably no healthcare system in the US that is prepared to deal with a large-scale smallpox attack—say an aerosol-based attack initiated at ten to twenty high traffic airports. In most cases, the only effective method of treatment is the early administration of smallpox vaccine and, given the decisions in recent court cases, there has been no attempt to institute a nationwide vaccination program—or even to distribute existing supplies of the vaccine to regional facilities.

We believe that, in the absence of a smallpox-oriented SIA, most—if not all — of the negative recommendations about a nationwide inoculation program have simply ignored the key fact about bioterrorism: that it is a low cost, volitional action aimed at disabling a large portion of the US population, causing nationwide chaos, and, ultimately, forcing the US to disengage entirely from its international presence in order focus solely on domestic healthcare concerns.

Water.
In general, there are four types of attacks that can be used to disrupt the nation's water infrastructure and supply systems: chemical contamination; biological contamination; physical disruption; and disruption of the computerized control network known as SCADA (Supervisory Control and Data Acquisition).

Given the spatial dispersion and decentralized management of the water processing and supply infrastructures, many engineering experts have concluded that, while chemical, biological, and physical attacks on the US water system could be executed fairly easily, the impacts would be localized and that preparedness for immediate clean-up operations would be sufficient to minimize the impacts on the nation.

Aside from the rather cavalier attitude toward impacts on, say, those states with large urban populations and communities that depend on agricultural production, the absence of an SIA again leads to a false sense of security. In this case, the "soft underbelly" is the SCADA system—a collection of roughly 25,000 independent computer systems that are used to monitor and control virtually all of the nation's water infrastructure.

For the most part, SCADA is based on relatively old, simple DOS systems that have recently been connected to the Internet—with little, if any, direct attention to network or any other form security. Our research has shown that this system is not only highly vulnerable to even a startup hacker, but that a coordinated penetration of all of the computers that make up a specific SCADA network could cause extensive contamination resulting in a massive disruption of the water supply for the entire nation. (Note that the SCADA system is also responsible for monitoring just about all the utility systems in the US—including traffic lights and railroad controls and switching circuits.)

Using the SCADA system as one of the test cases for FPRI's SIA procedure, we were able to easily identify a low cost, easily implementable security solution based on an adaptation of an existing technology used by the US Navy.

Nuclear Power Plants.
Although targeting nuclear power plants is generally not treated as a bioterrorism attack, there are circumstances in which such an action can lead to a significant—possibly catastrophic—disruption to the nation's healthcare system.

In 1998 my colleagues and I presented two scenarios in which airplanes were used as cruise missiles to the then head of the FAA's security unit. One scenario was the action we now know as September 11th. In the second scenario, the same four airplanes were used to strike four nuclear power plants in and around Eastern Pennsylvania.

Assuming that the attacks were able to cause a significant level of radiation leakage, our analysis of the immediate secondary effects of the attacks indicated that roughly seventy-five percent of the nation's healthcare production systems — everything from gauze to pharmaceuticals to surgical instruments—would be contaminated and unusable for many years.

Aside from the impacts on the Commonwealth's citizens and economy, this supposedly non-bioterrorism attack would turn out to have catastrophic impacts on healthcare operations for the entire nation—a result comparable with even the worst biologically based actions. As with our analysis of the SCADA system, in

the absence of the information provided by an SIA, projections of indirect impacts would, in all likelihood, be completely neglected.

We have no doubt that the Members of this Committee can readily see the advantages of due diligence and the importance of having the standards provided by using an SIA process to assist in determining the costs, benefits, and the priorities for security investments. And we also have no doubt that, as legislators, you will immediately recognize that, while the benefits and priorities accrue to the citizens, the Commonwealth, and the nation, due diligence reviews cannot determine just who should bear the costs.

We believe that the US system of governance, a system that is designed to balance the roles of the public and private sectors to support the most fundamental of all governmental responsibilities—security—can resolve this issue quickly and decisively. Ultimately, we also believe that the private sector will play a significant part in this process — but only if standards and usable tools are made available.

In some cases, particularly where common societal functions are at risk, direct governmental intervention and support may be necessary to initiate security reviews and fund the resulting recommendations. In most cases, however, we believe that investments in security should be treated in the same way as other business functions such as safety. While the due diligence and analysis standards will likely be developed and institutionalized by governments, only the private has the requisite detailed knowledge and experience to produce meaningful security recommendations. And just as the private sector has come to realize that environmental and safety standards are beneficial to both business and the nation, we believe that security will come to be seen as just another part of an organization's business plan and balance sheet.

In closing, we are here to recommend that the Commonwealth of Pennsylvania continue to position the State as a leader in dealing with the threat of terrorism by showing that state and local governments and the private sector can—and will—meet their responsibilities in securing America and Americans. As a start, we envision the initiation of a process that partners federal agencies, state and local governments, research institutions, and the private sector in much the same manner as the land grant colleges once served as the model for reviving the nation's agricultural production in the aftermath of the Civil War. We also believe that the SIA process that we have outlined today can serve as the foundation for the Commonwealth's efforts to support the development of both a workable due diligence process and the standards for allocating resources and setting the priorities for investments in security.

Regardless of when (or whether) a similar initiative begins at the federal level, the management of risks and setting standards for investments in security will continue to be the responsibility of state and local governments. In the "War on Terror" the front line is everywhere and local management will, we believe, result in the kind of rapid improvement of security that is, today, a necessity, not an option.

The US has thus far been fortunate that, since September 11th, the bulk of the conflicts have been fought overseas. But the "War on Terror" is far from over and there is little doubt that we will face additional horrific actions in the future. We believe, however, that with the nation's preparedness planning based on relevant information and clear review procedures and standards, we can avoid catastrophic attacks. At a minimum, we can and should seek to coordinate the allocation and prioritization of all of our security-related resources and focus our investments and prevention measures on those potential attacks that can have catastrophic consequences to America and Americans.

at (215) 732-3774 x105.

- **Become an FPRI member**

FPRI Articles

- **By Subject**
- **By Author**
- **By Date**
- **By Publication**

Orbis

- 

Current Issue

Other Resources

- **Audio/Video Library**
- **Publications**
- **Transcripts and Testimonies**

Foreign Policy
Research Institute
1528 Walnut St, Ste 610
Philadelphia, PA 19102
Tel. 215-732-3774
Fax 215-732-4401
fpri@fpri.org

Site developed by **Argo Potomac**