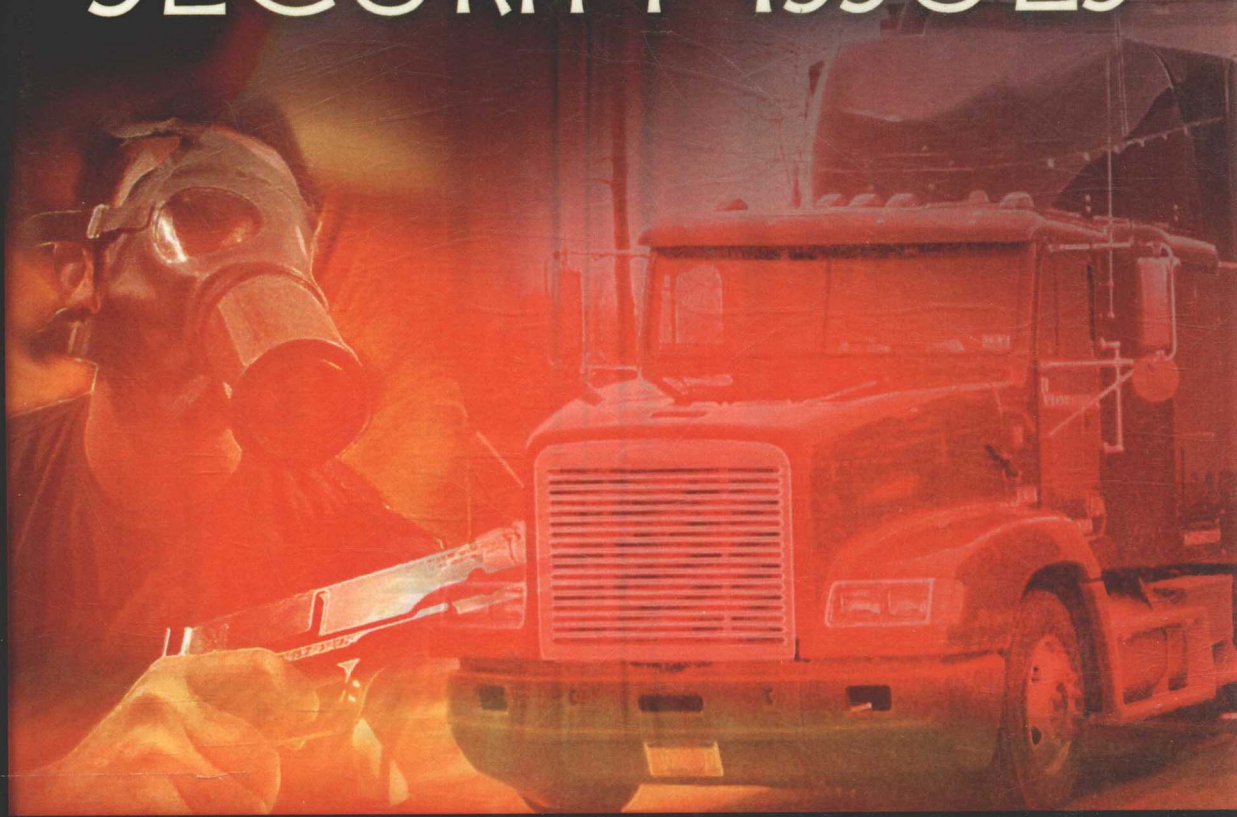
Cristina N. Morales
Editor

TERRORISM and SECURITY ISSUES

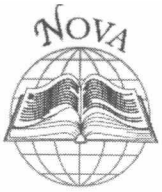


Terrorism, Hot Spots and Conflict-Related Issues

NOVA

TERRORISM AND SECURITY ISSUES

CRISTINA N. MORALES
EDITOR



Nova Science Publishers, Inc.
New York

LIBRARY OF CONGRESS CATALOGING-IN-PUBLICATION DATA
Terrorism and security issues / editor, Cristina N. Morales.
p. cm.
Includes index.
ISBN 978-1-60876-090-9 (hardcover)
1. Terrorism--United States. 2. Terrorism--United States--Prevention. 3. Civil defense--United States. 4. Bioterrorism--United States. I. Morales, Cristina N.
HV6432.T447 2010
363.3250973--dc22
2010026186

Published by Nova Science Publishers, Inc. ✣ New York

PREFACE

The September 11, 2001, attacks on the World Trade Center and the Pentagon have drawn attention to the security of many institutions, facilities, and systems in the United States, including the nation's water supply and water quality infrastructure. These systems have long been recognized as being potentially vulnerable to terrorist attacks of various types, including physical disruption, bioterrorism/chemical contamination, and cyber attack. Damage or destruction by terrorist attack could disrupt the delivery of vital human services in this country, threatening public health and the environment, or possibly causing loss of life. This new book discusses the tools of terrorism, not only our water infrastructure; but also commercial vehicle security, bioterrorism, maritime security and WMD proliferation.

Chapter 1- Recent reports by congressional commissions and others, in combination with the inclusion of bioterrorism issues in President Obama's State of the Union address, have increased congressional attention to the threat of bioterrorism. Federal efforts to combat the threat of bioterrorism predate the anthrax attacks of 2001, but have significantly increased since then. These efforts have been developed as part of and in parallel with other defenses against conventional terrorism. The continued attempts by terrorist groups to launch attacks targeted at U.S. citizens have increased concerns that federal counterterrorism activities are insufficient to face the threat.

The federal government's efforts to address the perceived threat of bioterrorism span many different agencies and are organized and directed through several strategy and planning documents. These agencies have implemented numerous disparate actions and programs in their statutory areas to address the threat.

Despite these efforts, many experts, including congressional commissions, non-governmental organizations, and industry representatives, have highlighted weaknesses or flaws in the federal government's biodefense activities. Recent reports by congressional commissions have stated that the federal government's efforts to address the bioterrorism threat could be significantly improved.

Key questions face congressional policymakers in these areas: Are the efforts already underway sufficient to face the threat of bioterrorism? Have the federal investments to date met the expectations of Congress or other stakeholders? Should these existing programs be altered, augmented, or terminated in the current environment of fiscal challenge? What is the appropriate federal role in response to the threat of bioterrorism, and what mechanisms are most appropriate for involving other stakeholders, including state and local jurisdictions, industry, and others?

Chapter 2- Damage to or destruction of the nation's water supply and water quality infrastructure by terrorist attack or natural disaster could disrupt the delivery of vital human services in this country, threatening public health and the environment, or possibly causing loss of life. Interest in such problems has increased greatly since the September 11, 2001, terrorist attacks in the United States.

Across the country, water infrastructure systems extend over vast areas, and ownership and operation responsibility are both public and private, but are overwhelmingly non-federal. Since the attacks, federal dam operators and local water and wastewater utilities have been under heightened security conditions and are evaluating security plans and measures. There are no federal standards or agreed-upon industry practices within the water infrastructure sector to govern readiness, response to security incidents, and recovery. Efforts to develop protocols and tools are ongoing since the 9/11 terrorist attacks. This chapter presents an overview of this large and diverse sector, describes security-related actions by the government and private sector since 9/11, and discusses additional policy issues and responses, including congressional interest.

Policymakers have been considering a number of initiatives, including enhanced physical security, better communication and coordination, and research. A key issue is how additional protections and resources directed at public and private sector priorities will be funded. In response, Congress has provided $923 million in appropriations for security at water infrastructure facilities (to assess and protect federal facilities and support security assessment and risk reduction activities by non-federal facilities) and passed a bill requiring drinking water utilities to conduct security vulnerability assessments (P.L. 107-188). When Congress created the Department of Homeland Security (DHS) in 2002 (P.L. 107-297), it gave DHS responsibilities to coordinate information to secure the nation's critical infrastructure, including the water sector. Under Homeland Security Presidential Directive-7, the Environmental Protection Agency (EPA) is the lead federal agency for protecting drinking water and wastewater utility systems.

Recent congressional interest has focused on two legislative issues: (1) security of wastewater utilities, and (2) whether to include water utilities in chemical plant security regulations implemented by DHS. In the 109th Congress, a Senate committee approved legislation to encourage wastewater treatment works to conduct vulnerability assessments and develop site security plans. Similar legislation was introduced in the 110th Congress, and has been introduced in the 111th Congress (H.R. 2883). Congress also has turned attention to legislation to extend DHS 's Chemical Facilities Anti-Terrorism Standards (H.R. 2868) and as part of that debate has been considering whether to preserve an existing exemption for water utilities from chemical facility standards or to include them in the scope of DHS security rules. Continuing attention to these issues in the 111th Congress is likely.

Chapter 3- A key challenge for U.S. policy makers is prioritizing the nation's maritime security activities among a virtually unlimited number of potential attack scenarios. While individual scenarios have distinct features, they may be characterized along five common dimensions: perpetrators, objectives, locations, targets, and tactics. In many cases, such scenarios have been identified as part of security preparedness exercises, security assessments, security grant administration, and policy debate. There are far more potential attack scenarios than likely ones, and far more than could be meaningfully addressed with limited counter-terrorism resources.

There are a number of logical approaches to prioritizing maritime security activities. One approach is to emphasize diversity, devoting available counterterrorism resources to a broadly representative sample of credible scenarios. Another approach is to focus counter-terrorism resources on only the scenarios of greatest concern based on overall risk, potential consequence, likelihood, or related metrics. U.S. maritime security agencies appear to have followed policies consistent with one or the other of these approaches in federally-supported port security exercises and grant programs. Legislators often appear to focus attention on a small number of potentially catastrophic scenarios.

Clear perspectives on the nature and likelihood of specific types of maritime terrorist attacks are essential for prioritizing the nation's maritime anti-terrorism activities. In practice, however, there has been considerable public debate about the likelihood of scenarios frequently given high priority by federal policy makers, such as nuclear or "dirty" bombs smuggled in shipping containers, liquefied natural gas (LNG) tanker attacks, and attacks on passenger ferries. Differing priorities set by port officials, grant officials, and legislators lead to differing allocations of port security resources and levels of protection against specific types of attacks. How they ultimately relate to one another under a national maritime security strategy remains to be seen.

Maritime terrorist threats to the United States are varied, and so are the nation's efforts to combat them. As oversight of the federal role in maritime security continues, Congress may raise questions concerning the relationship among the nation's various maritime security activities, and the implications of differing protection priorities among them. Improved gathering and sharing of maritime terrorism intelligence may enhance consistency of policy and increase efficient deployment of maritime security resources. In addition, Congress may assess how the various elements of U.S. maritime security fit together in the nation's overall strategy to protect the public from terrorist attacks.

Chapter 4- Numerous incidents around the world have highlighted the vulnerability of commercial vehicles to terrorist acts. Commercial vehicles include over 1 million highly diverse truck and intercity bus firms. Within the Department of Homeland Security (DHS), the Transportation Security Administration (TSA) has primary federal responsibility for ensuring the security of the commercial vehicle sector, while vehicle operators are responsible for implementing security measures for their firms. GAO was asked to examine: (1) the extent to which TSA has assessed security risks for commercial vehicles; (2) actions taken by key stakeholders to mitigate identified risks; and (3) TSA efforts to coordinate its security strategy with other federal, state, and private sector stakeholders. GAO reviewed TSA plans, assessments, and other documents; visited a nonrandom sample of 26 commercial truck and bus companies of varying sizes, locations, and types of operations; and interviewed TSA and other federal and state officials and industry representative

Chapter 5- The aftermath of that day of infamy, Americans wanted to know how could it have happened. The joint congressional inquiry and the independent 9/11 Commission were established to investigate. The 9/11 Commission held its first public hearing in this place on March 31st, 2003.

When the commission reported to the American people in 2004, it wrote, 'the greatest danger of another catastrophic attack in the United States will materialize if the world's most dangerous terrorists acquire the world's most dangerous weapons.' Congress received this warning through the efforts that Speaker Pelosi, Minority Leader Mainor [phonetic], Senate Majority Leader Reid, and Minority Leader McConnell. Congress passed House Resolution

1, which concludes a provision establishing this new commission, our mandate to build on the work of the 9/11 investigations and complete a critical task to assess how is our nation doing at preventing the proliferation of weapons of mass destruction and terrorism, and to provide a road map for greater security with recommendations for improvement.

This commission is distinguished in that it is not focused on the rearview mirror. There has not been an attack for us to investigate, and for that, we are all incredibly fortunate. But it gives us an opportunity to be forward looking, to examine the government's current policies and programs, identify the gaps in our prevention strategy, and to recommend how best to close those gaps. Our report will be issued this fall; our audience will be the next President of the United States of America, and the next congress.

Our commission is focused on nuclear and biological terrorism. We do that for a simple reason. A terrorist attack using those weapons would be a game changer. The impact on the United States' foreign policy, on our national life, would be so momentous that it could usher in a new world disorder. A nuclear or biological terrorist attack would be so catastrophic and so consequential that our government must explore every option, take every precaution, pursue every sensible means to deter and prevent it.

CONTENTS

In: Terrorism and Security Issues
Editor: Cristina N. Morales
ISBN: 978-1-60876-090-9

Chapter 1

FEDERAL EFFORTS TO ADDRESS THE THREAT OF BIOTERRORISM: SELECTED ISSUES FOR CONGRESS*

Frank Gottron and Dana A. Shea

SUMMARY

Recent reports by congressional commissions and others, in combination with the inclusion of bioterrorism issues in President Obama's State of the Union address, have increased congressional attention to the threat of bioterrorism. Federal efforts to combat the threat of bioterrorism predate the anthrax attacks of 2001, but have significantly increased since then. These efforts have been developed as part of and in parallel with other defenses against conventional terrorism. The continued attempts by terrorist groups to launch attacks targeted at U.S. citizens have increased concerns that federal counterterrorism activities are insufficient to face the threat.

The federal government's efforts to address the perceived threat of bioterrorism span many different agencies and are organized and directed through several strategy and planning documents. These agencies have implemented numerous disparate actions and programs in their statutory areas to address the threat.

Despite these efforts, many experts, including congressional commissions, non-governmental organizations, and industry representatives, have highlighted weaknesses or flaws in the federal government's biodefense activities. Recent reports by congressional commissions have stated that the federal government's efforts to address the bioterrorism threat could be significantly improved.

Key questions face congressional policymakers in these areas: Are the efforts already underway sufficient to face the threat of bioterrorism? Have the federal investments to date

---

* This is an edited, reformatted and augmented edition of a United States Congressional Research Service publication, Report R41123, dated March 18, 2010.

met the expectations of Congress or other stakeholders? Should these existing programs be altered, augmented, or terminated in the current environment of fiscal challenge? What is the appropriate federal role in response to the threat of bioterrorism, and what mechanisms are most appropriate for involving other stakeholders, including state and local jurisdictions, industry, and others?

Congressional oversight of bioterrorism crosses the jurisdiction of many congressional committees. As a result, such oversight is often issue-based. Because of the diversity of federal biodefense efforts, a complete view of the complete federal bioterrorism effort is beyond the scope of this chapter. Instead, this chapter focuses on four areas critical to the success of the biodefense enterprise that the 111th Congress is likely to consider: strategic planning; risk assessment; surveillance; and the development, procurement, and distribution of medical countermeasures.

Congress, through authorizing and appropriations legislation and its oversight activities, continues to influence the federal response to the bioterrorism threat. Congressional policymakers will likely be faced with many difficult choices about the priority of maintaining, shrinking, or expanding existing programs versus creating new programs to address identified deficiencies. Augmenting such programs may incur additional costs in a time of fiscal challenges while maintaining or shrinking such programs may be deemed as incurring unacceptable risks, given the potential for significant casualties and economic effects from a large-scale bioterror attack.

INTRODUCTION

Recent reports by congressional commissions and others, in combination with the inclusion of bioterrorism issues in President Obama's State of the Union address,[1] have increased congressional attention to the threat of bioterrorism. Federal efforts to combat the threat of bioterrorism predate the anthrax attacks of 2001, but have significantly increased since then. These efforts have been developed as part of and in parallel with other defenses against conventional terrorism. The continued attempts by terrorist groups to launch attacks targeted at U.S. citizens, including in transit to U.S. soil,[2] have increased concerns that federal counterterrorism activities, and the investments that underlie them, are insufficient to face the threat.

Experts differ in their assessments of the threat posed by bioterrorism. Some claim the threat is dire and imminent.[3] The congressionally mandated Commission on the Prevention of WMD Proliferation and Terrorism concluded that

> ... unless the world community acts decisively and with great urgency, it is more likely than not that a weapon of mass destruction will be used in a terrorist attack somewhere in the world by the end of 2013.
>
> The Commission further believes that terrorists are more likely to be able to obtain and use a biological weapon than a nuclear weapon.[4]

In contrast, other experts assert the bioterrorism threat is less severe or pressing than that posed by more conventional terrorism or other issues facing the United States.[5] The Scientists Working Group on Biological and Chemical Weapons concluded that

> Public health in the United States faces many challenges; bioterrorism is just one. Policies need to be crafted to respond to the full range of infectious disease threats and critical public health challenges rather than be disproportionately weighted in favor of defense against an exaggerated threat of bioterrorism.[6]

Federal efforts are often measured against the perceived magnitude of the threat. Thus, experts who believe bioterrorism poses a relatively low threat tend to conclude that the government has done too much. In contrast, experts who perceive a greater threat conclude that the federal government needs to do more, whether under existing programs or new ones. Many experts come to mixed conclusions: they regard some programs as effective but identify others as insufficient.

The federal government's biodefense efforts span many different agencies and vary widely in their resources, scope, and approach. For example, the Departments of State and Defense have engaged in nonproliferation and counterproliferation efforts.[7] The Departments of State and Commerce have strengthened export controls of materials that could be used for bioterrorism.[8] The Department of Health and Human Services (HHS) has made investments in public health preparedness; response planning;[9] and research, development, and procurement of medical countermeasures against biological terrorism agents.[10] The Intelligence Community has engaged in intelligence gathering and sharing regarding bioterrorism.[11] The Department of Justice performs background checks on people who want to possess certain dangerous pathogens.[12] The Department of Homeland Security (DHS) has engaged in preparedness, response, and recovery- related activities,[13] developed increased capabilities in environmental biosurveillance (see "Biosurveillance" below), and invested in expanding domestic bioforensics capabilities.[14] The Environmental Protection Agency (EPA) has explored post event infrastructure decontamination.[15] Many agencies, jointly or separately, have invested in expanded biodefense infrastructure, including public and private high containment laboratories for research, diagnostic, and forensics purposes.[16] Lastly, White House-led efforts and other coordinating groups have engaged in risk assessment and strategic planning exercises to coordinate and optimize federal investment against bioterrorism and response capabilities.[17]

Conflicting views of the bioterrorism threat and the breadth of the federal biodefense effort, which crosses congressional committee jurisdictions, complicate congressional oversight of the overall biodefense enterprise. In contrast to addressing the entirety of the biodefense enterprise at once, providing oversight and direction to individual components or agencies is relatively easy; but such an approach may be too narrowly focused to improve the overall efforts. An alternative to these approaches is to identify key areas or activities that shape the effort performed by different agencies. The Bush Administration identified four such "pillars" as organizing principles for the federal biodefense efforts: threat awareness; prevention and protection; surveillance and detection; and response and recovery.[18] Each of these pillars may have several agencies performing critical parts of the activity. Congressional oversight and direction of biodefense efforts has followed a similar but not identical path. Congress has provided oversight and direction on the basis of both individual agency biodefense activity and on those cross agency themes and policies deemed most important by congressional policymakers.

Because of the diversity of federal biodefense efforts, this chapter cannot address all aspects and associated programs related to this issue. Instead, this chapter focuses on four

areas deemed critical to the success of the biodefense enterprise that the 111th Congress is likely to consider: strategic planning; risk assessment; surveillance; and the development, procurement, and distribution of medical countermeasures. This chapter also focuses on the effectiveness and sufficiency of programs implementing these aspects of the federal biodefense efforts, outside analysts' suggestions for improving the government's efforts, and current issues under congressional consideration. This chapter does not attempt to address all biodefense issues of potential congressional interest. The footnotes provide references to related CRS reports and other sources for further information.

STRATEGIC PLANNING

Although the federal government had previously undertaken efforts to address the bioterrorism threat, the events of September 11, 2001, and the subsequent anthrax mailings led to an increased focus on terrorism in general and especially on biological weapons of mass destruction (WMDs). The Bush Administration established a homeland security apparatus within the White House.[19] Congress and the Bush Administration established the DHS as a focal point in the federal preparedness, response, and recovery to terrorism and imbued it with a variety of new authorities.[20] In addition, the Bush Administration developed a series of national strategies and other guidance documents for homeland security generally and biodefense in specific.[21] Beyond these cross-governmental strategy documents, many agencies developed more focused strategic plans for their individual operations against bioterrorism. The Obama Administration has continued this focus on bioterrorism by issuing additional guidance and directives.[22]

Congress has acted to require federal strategic planning activities through provisions of the Homeland Security Act of 2002 and other legislation. As well as establishing DHS, Congress has created offices and agencies within other cabinet departments and assigned them specific planning activities.[23] Finally, Congress established an office within the Executive Office of the President charged with preventing WMD proliferation and terrorism.[24]

Policymakers, analysts, and other experts have criticized federal efforts at strategic planning.[25] With respect to the White House, some experts have criticized cross-agency planning as lacking metrics and measures, failing to encompass the full range of threats, and being insufficient to meet its stated goals.[26] Policymakers have critiqued efforts by federal agencies to develop multi- agency plans as lacking metrics.[27] Even when considering efforts within individual agencies, experts have levied criticisms of research plans, stating that the correspondence between strategic goals, operational outcomes, and program investments has not been made clear.[28]

Options for Congress

Given these criticisms, Congress could choose to recommend changes in the strategic planning process, either government-wide or at the agency level, to address specific deficiencies. For example, Congress might require a more robust and transparent government-

wide strategic plan articulating clear goals, metrics and priorities; the development of a national framework to organize and prioritize biodefense investments; or a periodic comprehensive report detailing biodefense activities government-wide. Alternatively, Congress might require the Administration to perform internal or external reviews of policies and activities to determine their sufficiency and then direct the Administration to formulate new or revised policies as recommended by the reviews.[29]

Through its oversight activities, Congress may have a key position in assessing the completeness of ongoing planning. Because of the broad oversight responsibilities of congressional committees, synergies and duplications between agency efforts may be more apparent to congressional policymakers than to decision-makers within individual agencies.[30] Congress, through its oversight activities, may also be able to identify areas where executive branch resource allocation does not reflect need or congressional intent. A congressional perspective may identify unnecessary duplication or gaps in federal planning for the various necessary stages of response to a bioterrorism event. Congress might mandate the augmentation of government-wide planning documents, such as the National Response Framework, or the development of a forward-looking planning document, similar to the Quadrennial Homeland Security Review[31] or the National Strategy for Pandemic Influenza and its implementation guide,[32] for cross-agency federal biodefense activities.

Some experts have suggested that congressional oversight of federal homeland security efforts might be optimized if fewer committees and subcommittees had jurisdiction over homeland security.[33] Proponents with this perspective argue that congressional oversight would become more focused and holistic because of the centralization of oversight authority. Additionally, this might reduce the amount of time homeland security officials spend testifying before Congress. Alternatively, such consolidation might decrease the level of congressional scrutiny, since fewer committees with broader homeland security mandates might have less time and resources to focus on individual agencies and activities.

Risk Assessment

Ideally, a full understanding of the risk posed by bioterrorism would underpin the government's biodefense efforts. By understanding the bioterrorism risk, the federal government could determine the appropriate level of federal response and investment against this risk. The Government Accountability Office (GAO) has called for increased risk assessment activities in biodefense for many years.[34] Unfortunately, the nature of the bioterrorism threat, with its high consequences and low frequency, makes determining the bioterrorism risk difficult. Additionally, the presence of an intelligent adversary who can adapt to the presence of successful countermeasures complicates the use of standard risk assessment techniques.[35] Despite these challenges, risk assessment activities can help agencies use risk-informed decision-making processes to plan, prioritize, and invest wisely. In contrast, investment based on uninformed hypotheses or on an ad hoc basis may allow certain risks to go unmitigated if not properly identified or assessed; or result in overinvestment in risks that are less than others.

The Bush Administration identified bioterrorism risk assessment as a key component of its biodefense strategy. As a consequence, DHS engages in a bioterrorism risk assessment

process on a two-year cycle. Other agencies also engage in risk assessment activities, but they vary from DHS 's efforts in approach, assumptions, emphasis, and purpose.

Risk assessment processes depend heavily on the information used as input, the quantitative and qualitative factors used to interpret that information, and the robustness of the assessment process. These factors complicate comparisons of bioterrorism risk assessments performed for different purposes or with assessments of other threats. The DHS has begun this comparison on a limited scale,[36] but its use of these risk assessments for planning purposes has been strongly criticized by outside experts who assert these risk assessments do not adequately address the decision-making process of the terrorist.[37] Regardless of the complexity of the risk assessment methodology, due to the inherent uncertainties associated with assessing risk in a counterterrorism context, some level of flexibility in managing risk may be necessary.[38]

Options for Congress

A key question for congressional policymakers is the extent to which bioterrorism and other risk assessments should inform agency and government-wide priorities and policies. Congress could mandate risk-informed decision making based on the intelligence community's assessment of current and future bioterrorism-related threats, endorse a particular risk assessment method, or require the establishment of measures of robustness. It could require agencies to harmonize their risk assessment methodologies or mandate the development of a government-wide risk assessment process rather than individual agency-level assessments. Alternatively, Congress could direct agencies to rely less on the risk assessment process and instead set priorities based on other factors, such as expert judgment.

BIOSURVEILLANCE

Unlike most other terrorist attacks, a bioterrorism attack may not be immediately apparent. Victims may not develop symptoms for days or weeks following exposure. The first indication of a successful bioterrorism attack might be the discovery of infected individuals by health practitioners. The Bush Administration prioritized the development and deployment of biosurveillance technologies in an attempt to identify a bioterrorism attack as soon after an attack as possible.[39] The earlier an attack could be identified, the earlier treatment of the exposed individuals could begin. Earlier treatment generally increases the likelihood of individual recovery and survival.[40]

The Bush Administration implemented a number of different detection approaches, including environmental detection, syndromic surveillance,[41] and information sharing.[42] Through these efforts, the federal government aims to identify bioterrorism events at various scales, ranging from large, aerially disseminated releases to smaller releases infecting only a few individuals. The federal government, in collaboration with state and local jurisdictions, enhanced the existing network of public health laboratories to ensure that diagnostic laboratories could correctly handle and analyze clinical samples related to potential bioterrorism events.[43] Similarly, the federal government has continued to invest in some

global health activities partly in order to help identify when an emerging disease might pose a threat to the United States.[44]

Various government and outside experts have criticized or supported these efforts.[45] Widespread deployment of environmental biosurveillance technologies began after the anthrax mailings and federal efforts to further develop these technologies have also increased. Questions remain regarding the effectiveness of their detection ability, especially in comparison to the innate detection ability of the medical system through astute physicians. A repeated criticism of biosurveillance activities is that the detection system may not be sufficiently sensitive and dependable to allow for a federal response following detection of a bioterrorism event.[46] Technical difficulties persist in making a detection system sufficiently sensitive to detect very low levels of pathogens while maintaining a very low number of false alarms. Frequent false alarms pose a high cost in terms of resource consumption and responder opportunity costs. Additionally, frequent false alarms may lead responders and the public to assume that all alarms are likely to be false and thus they may not take alarms seriously. Other widely discussed issues include the extent to which the federal government should protect the population of the United States with such systems, through environmental sensing or other methods, and how the federal government should deploy systems that are only available in limited numbers.

Options for Congress

Congress is likely to remain interested in these programs. Development and deployment of the next generation of environmental detectors has been slower than DHS originally predicted.[47] Congress could provide additional funds, oversight, or guidance to encourage the completion of the deployment of these detectors. Congress may seek to determine whether the current plans for capabilities and coverage of surveillance sufficiently protects the population. Congress may also address concerns about the interactions between DHS and local jurisdictions. Local jurisdictions have identified fiscal burdens from this federal program, and questions remain about their proper role in the response to positive tests results. Congress could attempt to alleviate these concerns by providing additional resources to local jurisdictions or by providing additional guidance to DHS regarding its relationships with local jurisdictions.

Medical Countermeasures

Effective medical countermeasures[48] could significantly decrease the impact of a bioterrorist attack. The federal government has devoted many resources to the development, procurement, and distribution of medical countermeasures that could help respond to a bioterrorist attack. Since 2001, the federal government has often reexamined programs in these areas. Outside observers, Congress, and the executive branch have scrutinized, suggested improvements to, and further refined these policies.[49]

Research and Development

Many potential bioterrorism agents lack available medical countermeasures.[50] Therefore, the federal government has invested billions of dollars in research and development that might lead to effective medical countermeasures. The Department of Health and Human Services has played a key role in supporting the development of medical countermeasures, mainly through the National Institutes of Health (NIH) and the Biomedical Advanced Research and Development Authority.[51] Additionally, efforts undertaken by the Department of Defense to protect warfighters may also contribute to civilian biodefense.[52]

Some scientists have criticized the federal investment in biodefense countermeasures. They claim that the large investment in biodefense is not justified by the relative threat of bioterrorism and that these efforts would provide greater benefits if directed to other areas of research and development, such as more conventional public health threats.[53] Additionally, Congress has questioned the balance of investment among the various stages of research and development, identifying funding gaps that may pose barriers to the conversion of research results into deployable countermeasures. Congress also identified deficiencies in executive branch management of the countermeasure development process. These observations led Congress to establish the Biomedical Advanced Research and Development Authority to fund and coordinate the conversion of promising research results into deployable products.[54]

Options for Congress

Policymakers often face the challenge of determining the optimal balance of funding between competing stages of the research and development process. While Congress has supported a historic increase in biodefense-related basic research funding at NIH, critics have suggested that the federal government has underfunded the next stages of research and development that are critical for converting promising research results into usable products.[55] Current fiscal pressures will likely exacerbate the difficult decisions regarding appropriate funding levels. Policymakers may also continue to consider whether the dominant role of the federal government in countermeasure research and development should be reduced in favor of a greater role for investment by industry. Congress may again consider incentive-based approaches such as tax cuts and credits or patent protections, or demand-based approaches, such as increased funding to support larger contract awards.[56] Alternatively, Congress might conclude that the government needs to take a larger role in developing countermeasures in areas where the private sector has failed to produce desired countermeasures.

Procurement

The federal government is by far the largest procurer of bioterrorism medical countermeasures. It stockpiles them and keeps them ready for deployment to respond to a bioterrorism event.[57] The relatively small market for most bioterrorism countermeasures provides little incentive for companies to invest in developing a countermeasure when compared with the larger potential market of other products of the same industry, such as

anti-cholesterol drugs. The federal government has experienced difficulties in obtaining desired countermeasures because of this relatively small market. The executive branch and Congress have taken several steps to encourage companies to enter the medical countermeasure field. These activities include providing liability protection to companies developing medical countermeasures, guaranteeing a government market for countermeasures, and more clearly communicating the government's countermeasure needs and priorities.[58] These efforts have met with mixed success.[59] In the face of a need for medical countermeasures against emerging natural threats, such as pandemic influenza, HHS has also invested in medical countermeasure infrastructure to provide a more rapid response.[60]

A variety of experts, commissions, and policymakers have assailed these efforts as being underfunded, unclear, or insufficient.[61] Given the large costs of bringing a product to market, government assurances of a planned purchase seem to be insufficient to entice companies into this field. Private companies faced with the potential for liability following adverse reactions to a fielded medical countermeasure are sometimes reluctant to develop countermeasures. This led Congress to enact measures to protect companies from such liability.[62] Companies and think tanks have continued to state that the government should better communicate to developers the countermeasures it would like to procure. Think tanks and industry have also criticized actions they interpret as weakening the government's commitment to guaranteeing a government market by diverting funds designated for that program to other uses.[63] This may be interpreted as reinforcing industry's fear that the government is an unreliable partner in the development enterprise. In addition, GAO has cautioned against the federal government failing to have and make clear expectations regarding countermeasure and company performance.[64]

Options for Congress

Congressional policymakers will likely face decisions in the 111th Congress regarding the transfer of funds from an account designated for the procurement of countermeasures to one that is devoted to the development of countermeasures.[65] In addition, policymakers may be called upon to assess whether previously enacted programs are succeeding in drawing new investors into countermeasure manufacturing, or whether other, more novel manufacturing incentives need to be considered. Congress may also examine whether the procurement prioritization matches the risk assessments and the strategic plans developed by the executive branch. Finally, the results of a recently announced end-to-end assessment of HHS 's investment strategy may provide recommendations and requests for congressional action.[66]

Distribution

Even when effective medical countermeasures against potential bioterrorism pathogens exist, their distribution to individuals affected by an attack remains a challenge. The federal government has attempted to address this need through programs that stockpile and distribute stores of medical countermeasures, the development of alternative distribution mechanisms