

# **Challenges to Leadership: Responding to Biological Threats**

Paul Rosenzweig

**Center for Technology and National Security Policy  
National Defense University**

**October 2011**

---

The views expressed in this article are those of the author and do not reflect the official policy or position of the National Defense University, the Department of Defense or the U.S. Government. All information and sources for this paper were drawn from unclassified materials.

---

**Paul Rosenzweig** is Principal, Red Branch Consulting, PLLC, and Professorial Lecturer in Law, George Washington University School of Law. He served as Deputy Assistant Secretary for Policy in the Department of Homeland Security and twice as Acting Assistant Secretary for International Affairs. In these positions he had responsibility for developing policy, strategic plans, and international approaches to the entire gamut of homeland security activities, ranging from immigration and border security to avian flu and international data protection rules.

He serves as a Senior Editor of the Journal of National Security Law & Policy and on the Board of Advisors for the Hanover College Center for Free Inquiry. He is a *cum laude* graduate of the University of Chicago Law School. He has an M.S. in Chemical Oceanography from the Scripps Institution of Oceanography, University of California at San Diego and a B.A from Haverford College. Following graduation from law school, he served as a law clerk to the Honorable R. Lanier Anderson, III of the United States Court of Appeals for the Eleventh Circuit.

## **Acknowledgments**

The author expresses his thanks to Dr. James J. Valdes and to an anonymous reviewer for their thoughtful review of the paper and their contributions to it. Thanks also to Nicholas Rueter, a J.D./M.A. candidate at Duke University, for his able research assistance and to the Center for Technology and National Security Policy for funding this research.

Defense & Technology Papers are published by the Center for Technology and National Security Policy, National Defense University, Fort Lesley J. McNair, Washington, DC. CTNSP publications are available at <http://www.ndu.edu/ctnsp/publications.html>.

## **Table of Contents**

Introduction	1
I. A Prelude –The Biological Threat In Context	2
II. The Evolution of U.S. Biodefense Policy	4
III. A Confusion of Federal Responsibility	6
III. Threshold Challenges: State to Federal Responsibility and the DHS/HHS Question	18
IV. Recommendations	26

## Introduction

Experts have been warning of the threat of a biological attack on the United States for many years. In the aftermath of the 2001 anthrax release, various agencies within the Federal government initiated a series of programs intended to prevent incidents and ameliorate the perceived threat. State and local first responders have also invested heavily in systems and mechanisms for responding to an unanticipated disease outbreak. Private sector actors (hospitals, doctors, vaccine providers, and others) have mobilized to enhance their readiness, resilience, and capacity to respond. After nearly 10 years of political, legal and practical ferment, many have recognized the need to take stock of our efforts thus far and to assess how effective they have been.

The proliferation of authorities and responsibilities in the arena of biological threats is not well documented. No comprehensive survey of programs and responsibilities exists.<sup>1</sup> Indeed, the field is so broad that any review of modest length risks either degenerating into platitudes or reviewing efforts at such a high level of generality that any conclusions and recommendations are of little practical value. Accordingly, this monograph has set a more modest goal. It seeks to identify a series of gaps and overlaps in existing structures and mechanisms and to advance potential solutions that can be implemented. In particular, this monograph examines two issues of concern:

- *Federal Coordination Structure*—Any fair examination suggests that at this juncture the proliferation of responsible Federal entities has bred a form of bureaucratic gridlock that is detrimental to effective decision-making. The Federal government lacks an effective centralizing coordinating function for biological incidents. Roles and responsibilities can be readily confused and authorities to act are often ambiguous.
- *Federal/State Coordination*—Few fully understand when, and how, a transition from an event of local significance to one constituting an event of national significance occurs. No concerted effort has been made to understand where the threshold for dividing Federal responsibility from State/local/private responsibility lies, nor when transitions of responsibility within the Federal government should occur.

With respect to both of these areas, this monograph seeks to identify certain gaps and overlaps that need resolution if the goal is effective action. In doing so, the paper seeks as well to outline some suggested solutions. In particular, the paper recommends that a more comprehensive set of planning and response exercises be developed in order to better understand and develop a doctrine of incident leadership suitable for a biological crisis.

---

<sup>1</sup> One useful survey, limited to international programs, can be found in Barry Kellman, Michael Kraft, Zachary Clopton & Orley Lindgren, *United States Policies and Programs to Reduce Bio-Dangers* (ISBI, March 2010) [available at <http://www.biopolicy.org/sites/default/files/documents/ISBI%20Congressional%20Report%20Final.pdf>].

## I. A Prelude—The Biological Threat In Context

There is, of course, a substantial debate regarding the scope and nature of the threat of a biological attack. Some observers consider the threat to be significant and, to a large degree, greater than has been recognized. For example, the Commission on the Prevention of WMD (Weapons of Mass Destruction) 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.”<sup>2</sup>

Others, by contrast, contend that the threat from a deliberate biological incident is overstated. As one working group of scientists put it:

“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.”<sup>3</sup>

What then, is the likelihood of a biological threat, and how might it compare with the probability and consequence of other known threats? It is, as with so many risk assessments in the area of terrorism, difficult to offer a definitive answer to these questions. While our vulnerability to, and the consequences of, a biological incident can be assessed with a moderate degree of confidence, quantifying the nature of the threat remains deeply problematic. There are, however, a number of guideposts to a realistic threat assessment that we can identify with some certainty:

First, some terrorists have affirmatively considered using biological agents as part of their activities. As a posting on one web site put it: “Biological weapons are considered the least

---

<sup>2</sup> The Commission on the Prevention of WMD Proliferation and Terrorism, *World at Risk: The Report of the Commission on the Prevention of WMD Proliferation and Terrorism*, (December 2008), xv.. Richard Danzig, a former senior DoD official has reached much the same conclusion. See Richard Danzig, *Catastrophic Bioterrorism: What Is to Be Done?* Center for Technology and National Security (National Defense University, August 2003).

<sup>3</sup> Scientists Working Group on Biological and Chemical Weapons, Center for Arms Control and Non-Proliferation, *Biological Threats: A Matter of Balance* (January 26, 2010); see also Milton Leitenberg, *Assessing the Biological Weapons and Bioterrorism Threat* (Strategic Studies Institute, U.S. Army War College, 2005).

complicated and the easiest to manufacture of all weapons of mass destruction. ... The destructive power of these [biological] weapons is no less than that of nuclear weapons.”<sup>4</sup>

Second, biological weapons are comparatively more cost-effective in creating casualties than other weapons. According to the Stockholm International Peace Research Institute, it costs roughly \$2,000 per square kilometer to inflict civilian casualties with conventional weapons, \$800 with nuclear weapons and only \$1 with a biological weapon.<sup>5</sup> This favorable cost leverage factor makes a biological attack an attractive option for those with malevolent intent and limited financial resources.

Third, though often difficult and complicated to achieve in practice, the creation of a biological attack agent is technologically feasible. Surveys published by the American Medical Association have identified potential biological agents including anthrax, botulism, Ebola, plague, ricin, smallpox and others that can be developed and deployed with lethal effect.<sup>6</sup> More significantly, we have actual experience with a biological agent being used in an attack, most recently with the anthrax releases in 2001.<sup>7</sup>

Finally, beyond human casualties, we know that the financial costs of a successful biological attack are likely to be significant. For example, the World Health Organization has estimated that a 50-kilogram anthrax attack on a city of five million would result in as many as 250,000 casualties. The Center for Disease Control’s economic models put the costs at more than \$25 billion for every 100,000 persons exposed.<sup>8</sup>

All of which is not to say that biological attacks are more likely to occur or are the greatest threat to our security, overall. Given the frequency with which cyber attacks occur, for example, it might be more productive to focus priorities on countering cyber incidents.<sup>9</sup> Likewise, the potentially devastating effects of a nuclear incident and the likely even greater economic costs associated with such an event might suggest prioritizing the development of nuclear detection

---

<sup>4</sup> This quote is from the Jihadi Lion’s Den Website, al-Ma’asada al Jihadiya (quoted in Barry Kellman & Zachary Clopton *International Anti-Bioviolence Initiatives*, (May 2009) at v, [available at [http://www.biopolicy.org/sites/default/files/documents/International%20Anti-Bioviolence%20Initiatives\\_HSI.pdf](http://www.biopolicy.org/sites/default/files/documents/International%20Anti-Bioviolence%20Initiatives_HSI.pdf)].

<sup>5</sup> Barry Kellman, *Bioviolence*, (Cambridge Univ. Press 2007), 16 n.2.

<sup>6</sup> Beginning in 1999 the Journal of the American Medical Association published a series of articles relating to biological agents as threats. Typical is “Hemorrhagic Fever Viruses as Biological Weapons: Medical and Public Health Management,” *Journal of the American Medical Association*, May 8, 2002, Vol. 287, No. 18 .

<sup>7</sup> A summary of the FBI’s investigation of the Amerithrax attacks is available at <http://www.fbi.gov/about-us/history/famous-cases/anthrax-amerithrax/amerithrax-investigation>.

<sup>8</sup> Kellman, *Bioviolence*, 34.

<sup>9</sup> The Deputy Secretary of Defense has said that American cybersystems are probed thousands of times every day. See William J. Lynn, III, “Defending a New Domain: The Pentagon’s Cyberstrategy,” *Foreign Affairs*, September/October 2010, 97, [http://www.cfr.org/publication/22849/defending\\_a\\_new\\_domain.html](http://www.cfr.org/publication/22849/defending_a_new_domain.html).

technology.<sup>10</sup> With all of these high-consequence, low-frequency events, comparative risk analysis is challenging and, in the end, based on somewhat subjective judgments.

Plainly any discussion about organizational challenges faced by the Federal government (and its State, local and private partners) in responding to a biological threat begins, at least implicitly, from the premise that the threat is both real and significant. Therefore action to prevent the threat is necessary. Those who do not concur in the assessment of the threat will consider many of the difficulties identified in this report to be of lesser significance and will view the need to correct those deficiencies with less urgency.

## **II. The Evolution of U.S. Biodefense Policy**

In the years since September 11, 2001 the United States has begun the process of defining the functions and capabilities required for our efforts in the bio-threat arena. At the strategic level, there has been a steady evolution of thinking regarding how those functions should be characterized. The results of that evolution have been incorporated into the strategic objectives of our activities. The trend has been a shift from a “pure threats/terrorism” model to one recognizing the “dual use” character of biological agents.

In 2004, President Bush released the first biodefense strategy, “Biodefense for the 21<sup>st</sup> Century.”<sup>11</sup> Focused exclusively on the threat of a biological attack, the strategy characterized the “public health philosophy of the 20th Century - emphasizing prevention” as ideal for dealing with natural disease outbreaks, but insufficient for addressing deliberate threats that were part of a campaign of aggression or terror.

To counter those types of deliberate threats, the Bush-era strategy advanced measures that fall into the now common model for dealing with potentially catastrophic terrorist events—Federal efforts would center around the four pillars of “Prepare, Prevent, Respond, and Recover.”<sup>12</sup> Thus, the Bush strategy emphasized functions of: intelligence collection; threat analysis; proactive prevention; critical infrastructure protection; attack warning; attribution; response planning; medical countermeasures; and decontamination. In short, the functional structure was modeled on the same structures that might apply to any terrorist threat of significance.

---

<sup>10</sup> One study has put the cost of a one-kiloton bomb exploding in New York at in excess of \$1 trillion. See Veronique de Rugy, “Applying Strategic Risk Management to Allocating Resources for Homeland Security: A Case Example of Port Security,” *Strategic Risk Management in Government: A Look at Homeland Security* (New York: IBM 2009).

<sup>11</sup> *Homeland Security Presidential Directive-10: Biodefense for the 21st Century*, [available at <http://www.fas.org/irp/offdocs/nspd/hspd-10.html>].

<sup>12</sup> HSPD-10 characterized the functions slightly differently as Threat Awareness, Prevention and Protection, Surveillance and Detection, and Response and Recovery, but the parallel to structures in place for dealing with virtually any potentially catastrophic terrorist incident are undeniable.

By contrast, the Obama Administration’s November 2009 “National Strategy for Countering Biological Threats” more broadly recognized that biological issues involve dual use technology.<sup>13</sup> It began from the premise that the overwhelming majority of life science advances will have predominantly beneficial effects, albeit with significant risk of malfeasant uses. As a consequence, while maintaining a focus on the counter-terrorism functions of detecting and preventing biological attacks (and preparing to respond and recover if prevention efforts fail), the strategy broadened the focus of preventative efforts to encompass activities that are intended to address the behavior of law-abiding life scientists—that is, it sought to reach out to life science actors who are in a position to participate in and foster non-proliferation activities, and to seek their assistance. Rather than focus exclusively on active prevention by identifying and capturing malfeasant actors, the strategy also intends to educate law-abiding life scientists about the risks of their activities with the intent of minimizing those risks.

The Obama strategy sought to change the prevention paradigm by adding functions such as “reinforcing norms of safe and responsible conduct” and “transforming the international dialogue on biological threats.” Perhaps of even greater significance, this strategy, unlike that of 2004, recognizes the positive value of biological life science products, both on their own terms and as a means of promoting and enhancing global health security. In short, the newer strategy posits that our response to naturally-occurring infectious disease is of relevance to our preparation for, and response to, a deliberate biological attack.

In addition to clarifying this paradigm evolution, it is necessary to better understand the risks and how we might ameliorate them. Part of this understanding could come from a taxonomy of functions relating to biological threats, since in the biological domain (as much, if not more so than in other policy arenas) Federal efforts operate along several different tracks. To that end, it is helpful to identify certain subcategories of potential biologically-related activities for purposes of assessing the utility of current structures and processes. Using the current strategy as a template, one can identify several distinct types of activity.

Within the prevention domain, these might include:

- *Threat Reduction* –Education efforts; restriction of access to certain technologies or knowledge; control of source materials; research oversight; and development of situational awareness, all designed to prevent the spread of the capability to construct biological weapons.
- *Intelligence and Counter-intelligence collection*—The collection of intelligence on the intent and capabilities of those who might seek to conduct a biological attack and the counter-surveillance and risk mitigation activities designed to prevent adversaries from

---

<sup>13</sup> *National Strategy for Countering Biological Threats* (November 2009) [available at <http://geneva.usmission.gov/wp-content/uploads/2009/12/Natl-Strategy-for-Countering-BioThreats.pdf>].

gaining an understanding of vulnerabilities in the United States to particular pathogens or attack vectors.

- *Counter-terrorism*—Measures involving law enforcement, military, paramilitary, and homeland security assets intended to deter or interdict an intended biological attack.

Within the context of preparation and response one can think of the functions to be performed in any number of ways. The simplest, and most common, is to follow the characterization used by both the Bush and Obama Administrations:

- *Preparation*—Federal, State, and local efforts in advance of a biological event, encompassing everything from pre-event planning, exercises, and vaccinations to general public health measures, to the pre-positioning of medical stockpiles.
- *Detection*—The creation and operation of bio-surveillance systems for the detection of biological agents and the development of information sharing systems within the public health community to identify and characterize new outbreaks.
- *Event Characterization*—Efforts to determine the location of the impacted community at the time of an undetected release (as, for example, an aerosolized dispersal) and the location of the current hazard zone (which may have moved in the 24-36 hours from the time of the release until the time of detection/confirmation). These may represent two very different but equally significant “plume” zones, which will require characterization.
- *Medical Counter-measures*—The development of responsive vaccines and the distribution of vaccines and antibiotics to the civilian population on an outpatient basis.
- *Mass Casualty*—Medical efforts to prevent loss of life, and respond to illness, psychological trauma, and to contain the spread of potentially contagious diseases. Provision of timely preventive treatments such as antibiotics or vaccines for the purpose of saving lives, protecting scarce medical capabilities, and preserving social order.
- *Decontamination*—The development and application of decontamination and remediation standards, protocols, and capabilities to address the risks of contamination following a biological weapons attack and strategies, guidelines, and plans for decontamination of persons, equipment, and facilities.

### **III. A Confusion of Federal Responsibility**

Given the broad current scope of the American strategy, the dangers of fragmentation (lack of coordination) are even greater than they were when a solely preventative strategy was being

pursued.<sup>14</sup> What is missing from the taxonomy presented above, and what is missing from the current bio-threats strategy, is any sense of the need for a significant *coordination* role within the Federal government. This shortfall can be observed in at least two distinct situations: 1) the lack of a strong Federal coordinator at the White House and 2) the lack of clarity in the respective roles of the Secretaries of Health and Human Services and Homeland Security in preparing for and preventing a biological attack, as well as their role in interacting with other Federal institutions such as DOJ/FBI and the IC.<sup>15</sup>

A survey in 2004 identified more than 25 Presidentially-appointed and Senate-confirmed positions in the Federal government with responsibility for organizing the Federal response to biological threats.<sup>16</sup> Counting senior career and political appointees, that same survey identified more than 80 senior officials scattered through the Departments of Health and Human Services (HHS), Homeland Security (DHS), Agriculture (USDA), the Department of Justice (DOJ) and the Federal Bureau of Investigation (FBI), Commerce, State, Defense (DoD), the Intelligence Community (IC), and the Environmental Protection Agency (EPA), who share responsibility for ensuring that America is not subject to a biological attack or, if such an attack occurs, for ensuring that America is prepared to respond effectively.<sup>17</sup> These senior leaders manage organizations whose staff size is not precisely known, but which logically run into hundreds, if not thousands of people.<sup>18</sup>

The threat from biological incidents is multivariate and complex. It is, therefore, both logical and sensible to have a number of different Federal institutions with responsibility for addressing the problem.<sup>19</sup> But in the absence of a clear set of policy directions and the mechanisms for coordinating action across Federal agencies, a risk is incurred that Federal policies will be confused in development or poorly executed in practice.

---

<sup>14</sup> As Richard Danzig has noted, the fragmentation problem is not solely an issue of homeland/national security. Rather, it is equally true that the Federal biological and medical responses are dispersed across a number of agencies and within the Department of Health and Human Services where the HHS Secretary must coordinate the National Institute of Health, the Biological Advanced Research and Development Agency, the Centers for Disease Control and Prevention (CDC), the Food and Drug Administration (FDA), the Public Health Service and the Office for Emergency Preparedness and Response. See Danzig, *Policymaker's Guide*, 15– 16.

<sup>15</sup> The same lack of clarity is present when determining the roles of the two Secretaries in responding to a successful biological attack. The challenges in the “respond and recover” domain are addressed in the next section.

<sup>16</sup> Ari Schuler, Joseph Fitzgerald, Thomas Inglesby & Tara O’Toole, “Executive Government Positions of Influence in Biodefense: The Bio Plum Book, Biosecurity and Bioterrorism: Biodefense Strategy,” *Practice and Science* 4:2 328 (2004), [available at [http://www.upmc-biosecurity.org/website/resources/publications/2004\\_orig-articles/2004\\_article\\_pdfs/2004-12-15-execgovtpositionsbio-plumbook.html.pdf](http://www.upmc-biosecurity.org/website/resources/publications/2004_orig-articles/2004_article_pdfs/2004-12-15-execgovtpositionsbio-plumbook.html.pdf)].

<sup>17</sup> *Ibid.*

<sup>18</sup> Though the technical microbial expertise within the Federal government is small compared to that in the private sector, this monograph suggests the number of individuals with responsibilities related to biological threat prevention, detection, and response is much greater than the simple catalog of those with the requisite scientific expertise to diagnose the attack at a technical level.

<sup>19</sup> The challenge is further magnified when one realizes that the primary responsibility for preparedness and response lies with State and local authorities who manage State-level health systems and that the delivery of a response ultimately relies on a complex web of private sector actors. The transition from State to Federal responsibility is addressed in the next section.

The proliferation of responsible agencies suggests the need for a well-defined set of organizational structures and procedures to develop and implement policies regarding biological threat prevention, preparedness and response. These structures should, of course, be optimally designed to implement the chosen underlying policies adopted by the Federal government.

*High-Level Federal Coordination:* The current bio-threats strategy focuses principally on prevention and makes little mention of a Federal coordinating function, implicitly assigning that function to existing coordinating mechanisms within the National Security Council (NSC).

Contrast that silence with the Obama administration's approach to cyber security policy. In that context, the complexity of the coordination task was highlighted by the principal recommendation of President Obama's Cyber Space Policy Review, a comprehensive review of American cyber policy undertaken at the start of the President's administration.<sup>20</sup> The Review called for the appointment of a White House-level policy coordinator (colloquially known as a "Cyber Czar") who would "anchor" leadership on cyber issues within the White House.<sup>21</sup> Indeed, the need for leadership was so palpable that the Review's first chapter was entitled "Leading from the Top."<sup>22</sup>

The current approach to biological threats reflects only a partial recognition of the need for greater coordination. At the highest levels, the President has appointed a senior official in the NSC with responsibility for coordinating Federal efforts in arms control, the proliferation of weapons of mass destruction (WMD) and terrorism.<sup>23</sup> But the official responsible for coordinating efforts to prepare for and respond to the use of WMD has responsibilities that are broader than the response to biological threats. Those organizational responsibilities also include such (very significant) concerns as nuclear non-proliferation matters. Thus, even with this high-level attention, the salience of the Federal response to the biological threat is diluted by the need to be attentive to other notable threats.

*Operational Counter-Terrorism Coordination:* The situation is likewise a muddle when one looks at the next level down and considers the large number of officials who are responsible for preparing for and addressing purposeful biological threats before they occur. At an operational level, this makes coordination challenges significant. These challenges cross functions (such as intelligence and law enforcement, threat reduction and detection); these challenges cross institutions (such as the judiciary and the military).

---

<sup>20</sup> Executive Office of the President, *Cyber Space Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (May 2009).

<sup>21</sup> *Cyber Space Policy Review*, 7; vi (recommendation #1, calls for appointment of NSC-level policy cyber coordinator).

<sup>22</sup> Responding to this call, in December 2009, President Obama appointed Howard Schmidt as the first Special Assistant to the President and Cybersecurity Coordinator.

<sup>23</sup> The appointment of such an official was called for by the Commission on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism, co-chaired by former Senators Bob Graham and James Talent. See *Prevention of WMD Proliferation and Terrorism Report Card* (January 2010) [available at <http://www.preventwmd.gov/static/docs/report-card.pdf>].

*Intelligence and Law Enforcement Activities Overseas*—There are a number of different actors who are responsible for the collection and analysis of information related to biological threats that originate overseas (activities that, in the taxonomy, would constitute counter-terrorism and counter-intelligence activities). Principal responsibility for the intelligence collection aspects of these activities resides, naturally enough, with our intelligence agencies. Any successful effort to collect and analyze biological threat intelligence will necessarily involve the coordination of the intelligence activities of the Central Intelligence Agency (CIA), military intelligence activities of the Defense Intelligence Agency, and signals intelligence from the National Security Agency (NSA),<sup>24</sup> as well as internationally-based law enforcement assets deployed by the Department of Justice/FBI and DHS.

Strategic-level IC-wide coordination of these activities is the responsibility of the Office of the Director of National Intelligence (ODNI) which, broadly speaking, is responsible for setting intelligence collection and analysis priorities based upon the requirements articulated by the consumers of its products. To assure that biological threats are particularly scrutinized, the ODNI has a directorate tasked with examining the Global Biological Threat within the National Counter-Proliferation Center (NCPC).<sup>25</sup>

To accomplish its coordination mission, the NCPC has developed strategies intended to focus intelligence collection and analysis on current and projected WMD proliferation issues. It also attempts to evaluate the scope of existing knowledge about threats with an eye toward eliminating critical intelligence gaps on the U.S. Government's highest priority WMD proliferation concerns. Most notably, in response to a recommendation from the WMD Commission,<sup>26</sup> it has created and chartered the Biological Sciences Experts Group to tap the expertise of our nation's scientific talent in academia and industry to address biological threats. The focus remains largely "intelligence," rather than "science," driven, and the IC's relative lack of direct experience with biological agents and the underpinning science and technology can result in unrealistic threat assessments.

Despite these efforts, intelligence collection and analysis of biological threat information remains a challenge. Our record of detecting biological threats is poor at best, and at times is even counter-productive and erroneous.<sup>27</sup> As one senior intelligence officer told the WMD

---

<sup>24</sup> The basic architecture of the intelligence community was first defined in the National Security Act of 1947 and most recently revised in the Intelligence Reform and Terrorism Prevention Act of 2004. The core definition of the authorities and limitations of the intelligence agencies is particularized in Executive Order 12333, first adopted by President Reagan in 1981 and subject to many revisions since.

<sup>25</sup> A fuller description of the work of the NCPC can be found at <http://ncpc.dni.gov/>

<sup>26</sup> The WMD Commission (also sometimes called the Silberman-Robb Commission) is the colloquial name for The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction. For this particular recommendation, see *Commission Report to the President* (March 31, 2005) 510. The existence of a biological directorate within the NCPC was another recommendation of the Commission. *Ibid.* 512.

<sup>27</sup> The most notable example of this latter fact was our over-reliance on an agent, code named "Curveball" who quite literally conned our intelligence services into believing that Iraq had a biological weapons program. Bob Drogin, *Curveball: Spies, Lies and the Con Man Who Caused a War* (Random House, 2007).

Commission: “We do not understand biological weapons better now than five years ago: five years from now, we will understand them less well.”<sup>28</sup> This is due in large part to the fact that there remain few scientists and engineers—“weaponeers”—who have actual hands-on experience with these weapons and who understand their limitations.

The problem is exacerbated when the geographic location of the potential threat changes from nation states outside the U.S. borders with whom we have no close relation, to one where the threats arise in or are transiting allied nation states (e.g., European nations or Japan). In many of these allied nations, for example, the FBI works cooperatively with foreign law enforcement to track weapons of mass destruction.<sup>29</sup> Similarly, the DHS typically engages with international partners to jointly enhance border security.<sup>30</sup> These cooperative law enforcement activities must be coordinated with and layered on top of existing intelligence sharing agreements and traditional military-to-military cooperative activities.<sup>31</sup>

Collectively, these several efforts represent a significant investment of American resources in cooperative counter-terrorism. At least in theory, all of these efforts are coordinated locally through the U.S. Embassy and, in Washington, through the NSC. But here again, the infrastructure for effective coordination of our response to biological threats is lacking. In each American Embassy there is a coordinative mechanism for law enforcement activity generally, but biological threats are subsumed within the everyday concerns of counter-narcotics and military training.

Nowhere in the multitude of agencies is there an overall operational coordinator. The closest analog would be the State Department’s Bureau of International Security and Nonproliferation but, even within the State Department, that Bureau must coordinate its efforts with other Bureaus, including Intelligence and Research, Counterterrorism and International Narcotics and Law Enforcement. The coordination challenge overseas merely becomes magnified as the operatives of additional agencies (DOD, DOJ and DHS) are also involved. Though their activities in foreign countries must, *de jure*, be coordinated with the U.S. Ambassador in that country, in practice the absence of a strong coordinative function in Washington has a “trickle

---

<sup>28</sup> *Commission Report*, 506.

<sup>29</sup> The FBI’s overseas engagement can occur through the local Legal Attache, seconded to the US embassy. In many instances, however, the substantive expertise will come from dedicated counter-terrorism and weapons of mass destruction investigators primarily based in the United States.

<sup>30</sup> Overseas border control programs operated by the Department range from cooperative inspection programs (like the Container Security Initiative) to data-collection programs (like the Electronic System for Travel Authorization) to immigration systems (like the Immigration Advisory Program).

<sup>31</sup> For example, since WWII, the United States and the United Kingdom have had a cooperative relationship regarding the sharing of signals intelligence. In subsequent years, the agreement (known as the UKUSA Agreement) was broadened to include sharing with Australia, Canada, and New Zealand.

down” effect overseas.<sup>32</sup> The reality is a lack of focus and attention, perhaps because in relation to other more tangible and visible threats, biological threats seem remote.

*Domestic Law Enforcement*—The situation is rather better structured when we turn our attention to domestic law enforcement efforts to counter biological threats. In the domestic arena, the FBI has taken lead responsibility for the operation of Joint Terrorism Task Forces (JTTFs)—one in each of the 93 Federal judicial districts of the United States. These JTTFs are, in turn, coordinated through a National JTTF headquartered in Washington.<sup>33</sup>

The JTTFs serve a positive function coordinating efforts on a local or regional basis amongst the various law enforcement agencies with domestic responsibility. Typically, a JTTF will also have representatives from various other DHS and DOJ investigative offices such as Immigration and Customs Enforcement and Secret Service from DHS or the Drug Enforcement Agency from DOJ. They will also incorporate State and local law enforcement officials from the major urban areas within the domain of the JTTF (e.g., the Chicago Police Department and the Cook County Sheriff’s Office). Working through the National JTTF, the local and regional JTTFs have access to intelligence and analysis through the FBI’s participation in the National Counterterrorism Center (NCTC).<sup>34</sup> Overall, this system appears to be reasonably effective, notably in getting intelligence to State and local officials not formally considered part of the IC.

The problem, however, is one of focus and attention rather than structure. JTTFs are, properly, concerned with all forms of potential terrorist activity. This encompasses acts ranging from violent kinetic terrorism to nuclear threats. Given the breadth and scope of the JTTFs’ domain in the domestic law enforcement context, investigations relating to biological threats risk being given inadequate attention and resources. The contrast with how domestic law enforcement investigates cyber threats is instructive. To provide a unified focal point for cyber investigations, the DOJ has chartered a threat-specific task force, the National Cyber Investigative Joint Task Force, tasked with coordinating cyber-related terrorism investigations throughout the United States.<sup>35</sup> No comparable task force exists for biological threats.

---

<sup>32</sup> Department of State policy, for example, requires embassy clearance for any official travel to a foreign country. See 22 U.S.C. § 3927 and E.O. 10893, Part II (establishing country authority of Ambassadors and Chiefs of Mission). Other regulations, 22 C.F.R. §181.4, require any formal agreements with a foreign country to be approved by the Secretary of State.

<sup>33</sup> The authority for the FBI to lead in the coordination of domestic law enforcement counter-terrorism efforts is found in 28 U.S.C. §553; 28 CFR §0.85 and NSPD 46/HSPD 15. In recognition of the coordination efforts of JTTFs, the Deputy Chief of the National JTTF is a supervisory agent from the Immigration and Customs Enforcement (ICE) component of DHS.

<sup>34</sup> The operational arms of the intelligence community and the military are, generally, prohibited from participating in domestic investigations and, therefore, pose little coordination concern in this arena. See 50 U.S.C. §403-4a(d)(1)(CIA’s has “no police, subpoena, or law enforcement powers or internal security functions”); 18 U.S.C. §1385 (prohibiting military from exercising law enforcement or peace officer powers).

<sup>35</sup> In addition, both the FBI and the Secret Service have purpose-dedicated cyber crime investigative divisions. To be fair, the prevalence of cyber crime (principally fraud and identity theft) assuredly warrants the devotion of greater resources to cyber issues on a day-to-day basis. But the similarities between the two types of threats (their diffuse

*Threat Reduction and Detection/Surveillance*—An entirely different set of fragmentation and coordination issues arises when our focus turns from challenges related to counter-terrorism, intelligence, and law enforcement to areas of cooperative threat reduction and biological threat surveillance.

*Threat Reduction*—In addition to the counterterrorism/intelligence activities aimed at detecting and interdicting biological threats, there are, in theory, two other components to any program to reduce the threat of a biological attack: limiting access to source materials and technology and reducing the spread of technical know-how. In practice, both of these tactics are exceedingly difficult, but not impossible, to implement.

The types of tactics that might, theoretically, be used to reduce the likelihood of a biological attack range from modest activities intended to enhance situational awareness, such as a simple census of the location of sensitive technologies or pathogens, to more aggressive efforts to require those working with certain materials to register their activities. Today, there is no such requirement, though there is a professional code of best practices that researchers often follow. Good policy might consider making some requirements mandatory as they are today for aspects of human subject research and research animal treatment.<sup>36</sup>

Beyond situational awareness, threat reduction efforts could seek to deny problematic actors supplies of critical pathogens by restricting access to sources of origin, to the laboratories in which the pathogens are located, or to the equipment with which pathogens might be manipulated. Perhaps most controversially, these efforts might even seek to limit the spread of biological knowledge by monitoring the activities of individual life scientists and/or preventing certain individuals from participating in the biosciences.<sup>37</sup> Such a policy is inimical to the practice of modern science, in which collaboration is the norm. In addition, a counter argument notes that, by making the knowledge ubiquitous, the scientific community would be more likely to be self-policing. That is, anomalous research activities would be more likely to be noticed and reported.

Needless to say, some of these threat reduction activities are highly controversial. Most have not been implemented yet and those that have been begun are in their infancy. Some, such as restricting access to bioscience learning, are unlikely ever to be adopted. Others, such as limiting access to equipment, are most certainly fruitless since that equipment is freely available in the global market. And, given the dual use nature of all biological research activity, any effort at

---

nature, difficulties of attribution, and international character) suggest that a similar organizational model (albeit with fewer resources) might be appropriate in the biological threat domain.

<sup>36</sup> CDC, “Biosafety in Microbiological and Biomedical Laboratories (5<sup>th</sup> Ed. 2009) [available at <http://www.cdc.gov/biosafety/publications/bmb15/BMBL.pdf>].

<sup>37</sup> By way of example, one recent news report focused on the limited security provided by Ugandan laboratories to the anthrax stored at their facilities and the challenges faced by the United States in assisting Uganda in upgrading that security. Josh Kron, “Uganda Seen as a Front Line in the Bioterrorism Fight,” *The New York Times*, November 10, 2010, accessed at <http://www.nytimes.com/2010/11/11/world/africa/11uganda.html>.

threat reduction must be careful not to collaterally diminish the potential for positive biological advances.

In short, the threat reduction problem is a complex one and achieving results will require coordination both domestically and internationally. Within the Federal government, the coordination of efforts to address international biological threats is spread amongst a host of agencies and programs. Some of the more prominent ones (and this is not a comprehensive list) include:

- The Biological Threat Reduction Program managed by DOD with the cooperation of HHS and the Department of Agriculture (USDA), works to help upgrade bio-facilities and training overseas;
- The Bio-Industry Initiative at the Department of State, targeted at transforming biological facilities in the former Soviet Union;
- The Bio Security Engagement Program, also at the Department of State (a broad-based program in cooperation with international agencies to foster bio-safety training and surveillance worldwide) that operates in conjunction with the International Biological Threat Reduction Program at Sandia National Labs.

Domestically, HHS/CDC and USDA run pathogen registry programs collectively known as the National Select Agents Registry (NSAR) Program. The NSAR catalogs and manages the possession of biological agents and toxins that have the potential to pose a severe threat to public, animal or plant health, or to animal or plant products. Under the NSAR, facilities including government agencies, universities, research institutions, and commercial entities that possess, use or transfer the identified biological agents and toxins are required to register with the government. To the extent that new threats, whether naturally occurring or man-caused, are identified, the National Institutes of Health (NIH) will be responsible for coordinating with the private sector to develop new vaccines for possible distribution.

More recently, President Obama has directed HHS and USDA to begin a process of prioritizing the identified select agents and providing enhanced security measures for those that pose a greater risk. Those standards will include “practices to ensure reliability of personnel with access” to the new, Tier 1, select agents, and the “establishment of physical and cyber security practices for” Tier 1 facilities.<sup>38</sup> Emblematic of the coordination problem, more than two dozen agencies and offices within the Federal government will participate in the process of designation and in the development of the new standards.

*Surveillance and Diagnosis* -- Unlike most other events, a biological attack could occur without anyone realizing it had happened. It is perfectly plausible to imagine scenarios where victims are infected without their knowledge and do not develop symptoms for many days. Thus,

---

<sup>38</sup> “Executive Order 13546, “Optimizing the Security of Biological Select Agents and Toxins in the United States,” 75 Fed. Reg. 39439 (July 8, 2010) [available at <http://edocket.access.gpo.gov/2010/pdf/2010-16864.pdf>].

a biological attack may, at first, be confused with the outbreak of a naturally-occurring disease. National security and public health officials must not only identify an illness that has occurred, but also determine whether it is of natural or man-made origin. This makes the development of surveillance techniques critical -- the sooner an attack is identified and its nature determined, the sooner countermeasures can be developed and deployed and infected individuals can be treated.<sup>39</sup>

To achieve early detection within the United States, the Federal government has adopted a varied series of detection and diagnostic approaches, including environmental detection, syndromic surveillance, and information sharing. These programs include the deployment of the BioWatch program, the development of the Biological Warning and Incident Characterization System, the establishment of the National Biosurveillance Integration Center (all through DHS), the establishment of the BioSense Program through the Centers for Disease Control and Prevention (CDC), and the expansion of the Electronic Surveillance System for Early Notification of Community-based Epidemics, or ESSENCE, program in the DOD.

These efforts are intended to address a wide range of potential biological threat events, from large-scale releases of biological agents to small-scale releases that affect a smaller area or fewer people. Domestically, these efforts must be undertaken in collaboration with State and local jurisdictions whose health professionals will often be the first to identify outbreaks. The efforts must also include coordination with the private sector—the hospitals where infected individuals will present themselves for treatment and the network of public health laboratories responsible for handling and analyzing the clinical samples related to potential bioterrorism events. Thus, beyond the several Federal agencies with surveillance and diagnosis responsibilities, there are literally hundreds of other State and local organizations that are also involved as well as an unspecified number of private sector organizations.

When the focus turns from domestic detection and diagnosis to overseas detection, the problems of coordination become even more complex and daunting. The Federal government has invested in a number of global health activities partly in order to help identify when an emerging disease might pose a threat to the United States.<sup>40</sup> Most notably, the CDC's Global Disease Detection (GDD) efforts aim to "protect the health of Americans and the global community by developing and strengthening public health capacity to rapidly detect and respond to emerging infectious diseases and bioterrorist threats."<sup>41</sup>

---

<sup>39</sup> In general, earlier treatment increases the likelihood of survival and recovery and reduces the likelihood of casualties or fatalities. L.M. Wein, D.L. Craft, and E.H. Kaplan, *Emergency Response to an Anthrax Attack*, Proc. Natl. Acad. Sci., 100(7), 2003, 4346– 51.

<sup>40</sup> See CRS Report R40239, *Centers for Disease Control and Prevention Global Health Programs: FY2001-FY2011* (2010).

<sup>41</sup> CDC, *Global Disease Detection*, Policy Paper, June 2008, [available at [http://www.cdc.gov/cogh/pdf/GDD\\_At\\_a\\_Glance\\_2008.pdf](http://www.cdc.gov/cogh/pdf/GDD_At_a_Glance_2008.pdf)].

CDC's efforts are, naturally, coordinated with both the Department of State and the World Health Organization (WHO). There are seven GDD centers in China, Egypt, Guatemala, India, Kazakhstan, Kenya, and Thailand. During health emergencies, such as the emergence of pandemic flu in 2009, the CDC can use the centers for bilateral response or as part of the Global Outbreak Alert and Response Network (GOARN), which is coordinated by WHO.<sup>42</sup>

*The Judiciary* -- The Nation's judiciary represents a key target for terrorists for two reasons. First, legal decisions regarding jurisdiction, criminal intent and the parameters within which local and Federal officials and responders could operate will be affected by the courts, and thus disruption of the judicial system could be catastrophic. Second, the legal system and courts are important symbolic targets, a characteristic that has been very attractive to terrorist organizations such as *al Qaida*. The courts are relatively "soft" targets, being high-traffic areas largely open to the public. For example, the Court of Appeals in Washington, DC. is visited by more than 7,000 people per day. In the event of a biological incident, judges will be confronted with many decisions, some with scant legal precedence or precedence largely irrelevant to the prevailing conditions. Some examples include whether or not a suspected perpetrator can be coerced into providing bodily samples for diagnosis, the question of the legality of quarantines, and the rights of defendants as either criminals or illegal combatants, to name just a few. In extreme situations with a large number of affected people, decisions regarding distribution of limited stockpiles of medical supplies may also be required. Therefore, it is imperative that contingency plans be made to keep the judicial system functioning.

It is equally important that judges be trained *a priori* to address these issues, which will differ in situations where a disease outbreak is naturally occurring versus where it is intentionally caused, and between outbreaks which target humans versus those that affect economic targets, such as livestock. One key DOJ program is the Advanced Science and Technology Adjudication Resource (ASTAR) program. ASTAR is a program that trains State and Federal high court judges in the basics of the key scientific issues of the day and certifies judges to adjudicate cases involving science and technology. While ASTAR is aimed at science writ large, it has components related to bioterrorism and medicine which are relevant to decisions which the judiciary may face during a biological incident.

*Military Activities*-- Finally, our lack of biological threat coordination is notable in the lack of a strong coordinating structure within the military that would have responsibility for mobilizing military resources devoted to biological threat prevention, preparation and (in the event of failure) response. Once again, the contrast with the cyber domain is instructive.

For cyberspace, the Secretary of Defense has created a new command, the U.S. Cyber Command, a sub-unified command subject to the authority of the commander of the U.S.

---

<sup>42</sup> A summary of the GOARN program can be found at <http://www.who.int/csr/outbreaknetwork/en/>.

Strategic Command.<sup>43</sup> Under the DOD Unified Command Plan, Cyber Command is tasked with securing American freedom of action in cyberspace and mitigating the risks to national security that come from dependence on cyberspace. It is, therefore, the home of both offensive and defensive military cyber missions of all sorts.

There is no comparable institution in the military for biological threats, nor should there be. Cyber attacks are, rightly, perceived as having a higher threat level for American interests and a greater ongoing impact on the American economy. In addition, cyber issues pervade military command and control in a way that biological threats do not. It is, therefore, appropriate for DOD to have created a command devoted to exclusively to cyber warfare.

No such command is needed for biological threats. But the military lacks any command structure or other strong coordination structure for biological events. While various commands have frequently conducted exercises in an effort to develop practical responses to potential biological events, those exercises are often necessarily regional in character – given that most combatant commands are regionally-based. To date, there exists no single center of excellence within DOD’s operational commands to which the military can readily turn for a comprehensive national approach (if one is ever needed). To be sure, the military scientists at Fort Detrick have significant expertise.<sup>44</sup> But they conduct principally scientific research that is defensive in nature, focusing on diagnostics, preventives, and treatments for biological warfare infections. It is not an operational command.

Indeed, if tomorrow a purposeful biological outbreak were to occur in the United States and the President were to ask the Secretary of Defense for support, the Secretary would not have any clarity in which DOD entity to task with providing an operational response. While on-going exercises and planning are being used to develop DOD doctrine for a response, that doctrine has yet to be fully resolved. Presumably, for an outbreak in the United States, the Secretary would turn to the Commanding General of the U.S. Northern Command (NORTHCOM), the unified command tasked with providing homeland defense, civil support and security cooperation to defend and secure the United States and its interests. However, NORTHCOM has not identified any particular units with the responsibility for planning and training for a biological response, but could draw on such activities as the U.S. Army’s 20<sup>th</sup> Support Command CBRNE (Chemical, Biological, Radiological, Nuclear, and High Yield Explosives) based at the Aberdeen Proving Grounds.

---

<sup>43</sup> The new commander of USCC is dual-hatted and also serves as the Director of the NSA. A useful summary of the political considerations that led to this unusual result can be found in Richard A. Clarke & Robert K. Knake, *Cyber War* (Harper Collins 2010), 32–44.

<sup>44</sup> Fort Detrick is the military’s center for biomedical research and development, medical material management, global medical communications and the study of foreign plant pathogens. It is home to the U.S. Army Medical Research and Materiel Command (USAMRMC), with its bio-defense agency, the U.S. Army Medical Research Institute of Infectious Diseases (USAMRIID). In years past, it was also the home for the U.S. biological weapons program.

The closest we come to a dedicated unit with biological threat responsibility is the Fort Monroe, Va.-based Joint Task Force-Civil Support (JTF-CS). This small military unit is tasked with providing oversight of DOD Title 10 forces responding to a CBRNE incident. But to actually function, this JTF-CS must, in turn, draw from various military assets held by the four services.

The problem is compounded by the poor state of readiness of those military assets. As a 2007 GAO study concluded: “Most Army units tasked with providing chemical and biological defense support are not adequately staffed, equipped, or trained to perform their missions.”<sup>45</sup> Indeed, the National Guard and Reserve units that would be particularly responsible for responding to biological or chemical incidents within the homeland “report[ed] low readiness ratings—in other words, they are not considered sufficiently qualified for deployment. The low readiness ratings reflect critical personnel shortages” in the units.<sup>46</sup>

In short, at the operational level, there are a significant number of largely-uncoordinated Federal agencies and sub-agency components that are engaged in biological threat prevention, threat reduction, event characterization, and surveillance and diagnosis. They are joined in that effort by international organizations and State, local and private-sector actors. The lack of a higher-level coordinating function makes the unification of their efforts a daunting task.

**Table 1—Bio Threats: Prevent & Detection**

	<b>Within the US</b>	<b>Outside the US—Allies</b>	<b>Outside the US—Non-Allied Nations and Non-State Actors</b>
<b>Counter Terrorism</b>	FBI NCTC DHS	FBI State CIA/DIA DHS DOD	FBI ODNI NCTC/NCPC CIA/DIA/NSA DOD
<b>Threat Reduction</b>	DHS HHS/CDC/NIH	State HHS/CDC/NIH	FBI CIA

<sup>45</sup> *Chemical and Biological Defense: Management Actions Are Needed to Close the Gap between Army Chemical Unit Preparedness and Stated National Priorities*, at 5 (GAO-07-43) [available at <http://www.gao.gov/new.items/d07143.pdf>].

<sup>46</sup> *Ibid.* 5-6.

	Agriculture Private Sector	Private Sector	ODNI State DOD
<b>Surveillance &amp; Diagnosis</b>	DHS Private Sector HHS/CDC Agriculture FBI DOD EPA	State HHS/CDC Private Sector →→ World Health Organization	→→

All of which is not, of course, to suggest that creation of a unified coordination structure for biological threats would be a panacea. It will not solve all of the military coordination issues, nor will a unified civilian command fully meld the DOJ(FBI)/DHS/ODNI/HHS efforts to prevent and detect a biological attack. It is important, however, to note that the confusion of roles at the highest levels of the Federal government has filtered down to operational units, leaving them poorly-coordinated and, in many instances, poorly -staffed and -trained.

Going forward, we will need to take several steps to resolve these ambiguities. These include capitalizing on lessons learned from recent biological events like the H1N1 pandemic and the further development of coordinating structures based upon a more robust suite of Federal/State/local biological incident exercises. This is no easy task. It will take concerted leadership from the top to resolve these issues.

### **III. Threshold Challenges: State to Federal Responsibility and the DHS/HHS Question**

A different way of characterizing plans for preparation and response to a biological event turns not on the functional activity to be undertaken, but on the source or origin of the biological outbreak. Indeed, that may be a critical determinant in Federal organization because roles and responsibilities are likely to vary widely based upon the character of the event, perhaps more so than based on the nature of the function. Certainly, it appears likely that the identification of

leadership and coordination roles will turn on the character of the biological event, since it matters very much whether the event is the outbreak of a naturally-occurring disease or a biological attack.

Civilian, non-national security agencies will predominate in response to naturally occurring events. Initially, there will be virtually no Federal involvement in the response. The Federal government will become engaged only when (as with the recent H1N1 outbreak<sup>47</sup>) the scope of the incident grows so significant that the response exceeds the capacity of State, local, and private sector responders.

By contrast, DHS, DOJ and DOD will take a much earlier and far more active role when deliberate, terrorist action is suspected. Indeed, even the infection of a single individual will garner Federal attention if it is suspected that the infectious agent was deliberately introduced. Of equal significance, for a natural outbreak, the Federal responsibility will lie with our health agencies, principally coordinated by the Secretary of HHS, while the response to a suspected biological attack will likely be directed by the Secretary of Homeland Security.

Hence, another taxonomy that bears on the discussion is:

- *Natural or Non-Malicious Outbreaks*: Natural outbreaks would encompass events arising from the natural development and outbreak of an infectious disease, such as H1N1. Non-malicious outbreaks, by contrast, might arise from accidental human action, for example, through an accidental release from a laboratory or the mistaken contamination of the food supply.
- *Biological Attack*: Events arising from the deliberate introduction of a biological agent (whether by a nation-state or a non-state actor), including point source releases (e.g., a mall or a stadium), network releases (e.g., contamination of the postal system or a transportation hub), and aerosolized releases into the atmosphere. This will also include food and/or water system attacks, though those events concern not only human infection, but also contamination of the food or drinking water supply, and therefore pose somewhat different response challenges.

The greatest challenge is that, at the outset, it will be exceedingly difficult to distinguish between a naturally-occurring and a purposeful incident.<sup>48</sup> We may anticipate that all or almost all

---

<sup>47</sup> In 2009, the outbreak of an H1N1 influenza pandemic led both the U.S. Government (through the CDC) and the World Health Organization to declare a public health emergency. The Federal government led a response that included vaccinations, communication and syndromic monitoring. See *The 2009 H1N1 Pandemic: Summary Highlights, April 2009-April 2010* [available at <http://www.cdc.gov/h1n1flu/cdcresponse.htm>].

<sup>48</sup> To that end, the Federal government has undertaken a strategic initiative to enhance our bio-forensic capabilities. Under this initiative, we will develop a strategic microbial forensics research agenda that will produce a national microbial forensic capability that is ultimately capable of high confidence, robust detection, characterization and comparison of biological agents in forensic samples. See “National Research and Development Strategy for Microbial Forensics,” (2009),

deliberate biological attacks will initially appear to be nearly identical to the outbreak of a naturally-occurring disease, thus emergency room physicians cite a preclinical diagnostics capability as a top priority. As bio-forensics improve, the time period before an accurate characterization is achieved will diminish, but we cannot reasonably anticipate that it will ever be reduced to zero. This is a formula for significant confusion—if the transition of responsibility is dependent on the nature of the event, yet biological forensics are generally weak and cannot distinguish between the two circumstances, then the vital leadership transition point is left to guesswork and political will, rather than deliberate, fact-based analysis and clear, mutually-agreed standards. More importantly, if we start with the assumption that a bio-event is naturally occurring, but it turns out to be intentional, critical response time may be lost, which may directly affect our ability to save lives.<sup>49</sup>

Of perhaps even greater concern, strategic planning for this transition of responsibility from the State and local first responders to the Federal government is relatively non-existent, while planning for the division of Federal responsibility is internally inconsistent. There is little, if any, effort to define when a transition from State or local responsibility to Federal responsibility would arise or when the HHS/DHS transition might occur. Indeed, as one observer has noted:

“In fact, our situation is even worse than it would be if all we lacked was a strategy. In keeping with the long-standing division of responsibilities between the Federal and state governments, public health issues have been pretty much the exclusive province of state and local governments, each of which has been pretty much free to determine its own legal authorities, organizational structure and capability mix. That arrangement is almost certainly best when dealing with normal public health issues, but the suitability of our current mix of organizations and authorities for events which span state boundaries must be questioned. Just as public policy changes . . . may be necessary for responding to truly catastrophic oil spills, so too, public policy changes are almost certainly necessary if we are to be ready for a major biological event.”<sup>50</sup>

*State To Federal Transition:* One of the principal issues we will need to determine is when, during the course of a biological incident, authority and responsibility for leading the response

---

<http://www.whitehouse.gov/files/documents/ostp/NSTC%20Reports/National%20MicroForensics%20R&DStrategy%202009%20UNLIMITED%20DISTRIBUTION.pdf>. Unfortunately, the time-line for the development of this capability is speculative, at best.

<sup>49</sup> Though it is beyond scope of this monograph, completeness requires mention of the circumstance that State and local public health agencies have had to make serious financial cutbacks on their biodefense efforts because of tight fiscal circumstances. Since these public health agencies serve as the front line of defense in these types of incidents, a reduction in capability has a serious impact on biodefense. On details about reductions in spending at State and local levels see Trust for American’s Health, “Ready or Not?,” (2011), 15–17 (<http://healthyamericans.org/assets/files/TFAH2010ReadyorNot%20FINAL.pdf>).

<sup>50</sup> Bob Ross, *Authority and Strategy—The Legal Foundation for Successful Emergency Response*, at Biosecurity Blog, <http://biosecurityblog.com/2010/09/20/authority-and-strategy-%e2%80%93-the-legal-foundation-for-successful-emergency-response/>.

will transition from State and local to Federal authorities. Managing and defining this transition will be critically important operationally. To date, there exists no settled doctrine on how or when that transition is to occur.

To be sure, there will be events (for example, the anthrax attack on Senate offices in 2001) where a Federal response will be immediate because the biological agents are accompanied by a self-declaration as to their provenance. Put another way, if Al Qaeda or any other terrorist organization conducts a biological attack and, contemporaneously, takes public credit for the attack, it is likely, as it was with the anthrax attacks in 2001, that the response will be immediately Federalized, and no issues of a “transition” will be presented.

But an equally plausible scenario (indeed, perhaps a more plausible one) may involve the manifestation of a biological event that initially cannot be characterized as to source. When this sort of incident is initially addressed, the first response will come through the normal operation of State or local public health agencies. Federal involvement will come only when one of two factors arise: 1) the biological forensics establish that the incident is a deliberate attack and not a naturally-occurring outbreak; or 2) the scope of the outbreak (whether an attack or a natural event) becomes so great that it outstrips the capacity of State and local authorities to effectively respond.

We need no new doctrine to address the first of these situations. When and if terrorist involvement becomes reasonably clear, the Federal government will assume responsibility for addressing the incident. But no clear doctrine exists for the other portion of the transition—when, if ever, will the Federal government assume responsibility for aspects of the medical response to a biological incident, stepping in to replace State and local authorities?

Little has been done to prioritize various attack risks, nor has any significant effort been made to quantify the nature of what would constitute critical federal interests, requiring federal action. For example, the DHS National Infrastructure Protection Plan (NIPP) defines Tier 1 critical infrastructure as those infrastructure elements whose loss would equate to the effects of September 11 or Hurricane Katrina. The NIPP then prioritizes them for protection from all-hazard threats.<sup>51</sup>

For any number of reasons, this threshold seems inadequate to the task of providing doctrine on the transition of responsibility. To begin with, needless to say, such an indefinite and innumerate threshold only invites disagreement and confusion. Absent a clear line of demarcation, a transition point simply becomes a muddle.

Second, the NIPP, while nominally a national plan, is a DHS-generated document; no threshold will be of any utility until it is accepted universally by all Federal and State stakeholders as an

---

<sup>51</sup> See Department of Homeland Security, *National Infrastructure Protection Plan* 41 (2009). Anecdotally, some in DHS use a rough numeric measure positing that Federal involvement would be likely when casualties exceed 10,000 or economic losses exceed \$10 billion. There is, of course, no formal doctrine adopting this metric.

appropriate definition for action. Absent collective “buy-in,” a DHS-defined threshold has limited authority and budget for implementation.

More significantly, these nascent efforts to generate a threshold for Federal involvement, while salutary, are more readily suited for non-biological incidents than they are for biological ones under consideration here. A nuclear attack, for example, would be a single-point incident and readily susceptible to concrete measurement of casualties and economic effects within a confined geographic space. The same is true of natural disasters, such as a hurricane, or point-release chemical agents.

Biological incidents, on the other hand, tend to be more diffuse and geographically widespread. Certainly naturally-occurring incidents cannot be expected to be geographically localized, though an attack might be more confined in space. Likewise, biological incidents are not confined in time to a single instance, but rather play out over a period of days or weeks. Thresholds, like the NIPP Tier 1 definition, that seem designed to address a single incident would have a tendency to miscalculate the need for Federal involvement in several ways:

- Widely-dispersed naturally-occurring biological incidents might exceed the threshold of economic effects without straining any particular localities’ resources, making significant Federal involvement unnecessary;
- Conversely, even modest incidents with little significant impact might – because of their salience – cause significant public fear and concern that require Federal involvement;
- A threshold based on actual casualties (as opposed, say, to one based on the number of people who might seek treatment or testing) might understate the scope of the disruption.

For these reasons, it seems likely that any threshold for transition from State or local to Federal responsibility will be different in kind from those associated with single-incident events. In any event, the complete absence of any generally-accepted threshold (for biological or any other WMD incident) precludes appropriate planning and budgeting.

*Federal Transitions: DHS and HHS:* The coordination of preparations for and responses to a biological event is as complex (if not more complex a challenge) as the challenge of coordination of a Federal biological threat prevention and detection response. Threat reduction and detection involves the coordination of agencies that frequently conduct joint operations; though challenges exist, DOJ and DHS and DOD are all somewhat experienced at coordinating their activities with each other.

By contrast, the development of a coordinated response in the wake of a biological incident (whether a naturally-occurring outbreak or a deliberate attack) will require the efforts of a host of Federal and State-level agencies that, in many cases, are unused to participating in a coordinated effort and, in the context of a terrorism event, certainly unused to participating in efforts that have law enforcement or national security consequences.

As we've already noted, the coordination challenge begins with the necessity of engaging State and local first responders—police, emergency preparedness, and public health officials. In a significant incident, it will also include coordination with private sector actors such as hospitals, physicians, health-care equipment providers and pharmacological companies.

At the Federal level, the response to a biological incident will, obviously, require efforts from HHS/CDC and DHS in providing emergency services ranging from health care to transportation. In cases of suspected terrorist activity, the FBI and DOJ will be tasked with conducting the domestic aspects of the investigation, while State, the CIA and the ODNI would work on the international aspects of attribution. Meanwhile DOD will, in many circumstances, be obliged to provide support and technical assistance to civil authorities<sup>52</sup> and even agencies as diverse as National Oceanic and Atmospheric Administration (NOAA), which has expertise in air plume modeling that may be of use in response to an aerosolized release of a biological agent, and Department of Energy, which has expertise in an array of biological and chemical detection methodologies, may be called upon.

To see the complexity of the requirements for coordination, consider the scenario of an aerosolized anthrax attack.<sup>53</sup> The functional mission areas that will need to be engaged in response to such an attack, and the relevant agencies that would be required to assist in the effort, include:

- *Prevention/Deterrence*—DOD; CIA; ODNI; HHS/CDC; DHS; DOJ/FBI; State; USDA
- *Emergency Assessment/Diagnosis*— HHS/CDC; DHS; DOJ/FBI; NOAA; EPA; State/Local
- *Emergency Management/Response*— DHS; HHS/CDC; DOD; State/Local; Private Sector resources<sup>54</sup>
- *Hazard Mitigation*—HHS/CDC; DHS; EPA; DOT; State/Local
- *Evacuation/Shelter*—DHS; DOD; State/Local; Private Sector<sup>55</sup>

---

<sup>52</sup> This support to civil authorities will be provided consistent with existing military doctrine. DOD Directive 5111.13 (March 2009) defines Defense Support to Civil Authorities (DSCA) as: “Support provided by U.S. Federal military forces, National Guard forces performing duty in accordance with [Title 32, U.S. Code], DOD civilians, DOD contract personnel, and DOD component assets, in response to requests for assistance from civil authorities for special events, domestic emergencies, designated law enforcement support, and other domestic activities. Support provided by National Guard forces performing duty in accordance with [Title 32, U.S. Code] is considered DSCA, but is conducted as a State-directed action. Also known as civil support.”

<sup>53</sup> An aerosolized anthrax attack is one of the 15 National Planning Scenarios that form the framework for most Federal emergency response planning. The summary here is based upon the National Planning Scenario Executive Summary (April 2005) (available at <http://cees.tamtu.edu/covertheborder/TOOLS/NationalPlanningSen.pdf>),

<sup>54</sup> Under the National Response Framework, private sector resources for emergency responses are mobilized through various sector- and function-specific coordinating programs, known as the Emergency Support Functions, or ESFs. *National Response Framework*, (2009) 29, <http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf>.

<sup>55</sup> In addition the Occupational Safety and Health Administration and the National Institute of Occupational Safety and Health (a part of CDC) will participate in the setting of safety standards for any sheltering activity. Meanwhile, particular institutions like the Office of Personnel Management and Congress will be responsible for significant evacuation actions aimed at maintaining the continuity of governmental operations.

- *Victim Care*—HHS/CDC/FDA; DOD; USDA; State/Local; Private Sector
- *Investigation/Apprehension*—DOJ/FBI; ODNI/CIA; USDA; State; DHS; State/Local law enforcement; HHS/CDC; DOD
- *Recovery/Remediation*—EPA; HHS/CDC; DHS/FEMA; State/Local; Private Sector

Despite the clear need for a strong coordination function within the Federal government, the foundational documents regarding such coordination authority reflect some confusion and dissonance. As the Government Accounting Office (GAO) reported last year:

“Federal government leadership roles and responsibilities for pandemic preparedness and response are evolving, and will require further testing before the relationships among the many federal leadership positions are well understood. . . . [I]t is not clear how these would work in practice. According to the National Pandemic Strategy and Plan, the Secretary of Health and Human Services is to lead the federal medical response to a pandemic, and the Secretary of Homeland Security will lead the overall domestic incident management and federal coordination. In addition, under the Post-Katrina Emergency Management Reform Act of 2006, the Administrator of the Federal Emergency Management Agency (FEMA) was designated as the principal domestic emergency management advisor to the President, the HSC, and the Secretary of Homeland Security, adding further complexity to the leadership structure in the case of a pandemic. . . . [T]he relationship of these roles to each other as well as with other leadership roles in a pandemic is unclear.”<sup>56</sup>

This is, candidly, a bit of an understatement. To cite but one example, the GAO has, in another report, remarked upon the fact that no agency of the Federal government bears responsibility for monitoring the extent to which State and local public health agencies or private sector health providers are prepared for their role in implementing a national response to the outbreak of a pandemic disease.<sup>57</sup> Given that these stakeholders are expected to play a vital role in any national response, the lack of any mechanism for Federal accountability is striking.

The situation grows somewhat more confused when the pandemic outbreak is the product of a deliberate attack of some form. The Biological Incident Annex to the National Response Framework designates HHS as the “coordinating agency for all biological incidents, including those that are terrorist in nature.”<sup>58</sup> By contrast, the Catastrophic Incident Annex designates DHS/FEMA as the coordinating agency for all catastrophic incidents and defines “catastrophic” as “any natural or manmade incident, including terrorism, that results in extraordinary levels of

<sup>56</sup> GAO, *Influenza Pandemic: Gaps in Pandemic Planning and Preparedness Need to Be Addressed* (GAO-09-909-T, July 2009).

<sup>57</sup> GAO, *Influenza Pandemic: Monitoring and Assessing the Status of the National Pandemic Implementation Plan Needs Improvement*, (GAO-10-73, Nov. 2009) 10–12.

<sup>58</sup> “Biological Incident Annex,” [http://www.fema.gov/pdf/emergency/nrf/nrf\\_BiologicalIncidentAnnex.pdf](http://www.fema.gov/pdf/emergency/nrf/nrf_BiologicalIncidentAnnex.pdf).

mass casualties, damage, or disruption severely affecting the population, infrastructure, environment, economy, national morale, and/or government functions.”<sup>59</sup> Plainly, at least some biological incidents might be catastrophic in nature.

Yet anecdotal evidence, including discussions with current and former DHS and HHS officials, suggests that there is no agreement on this point. DHS officials believe that at some point a transition to a DHS-lead is contemplated by the existing directives—particularly in situations where a terrorist incident is suspected. By contrast, HHS officials are of the view that no transition is either expected or required, whether the incident is a natural outbreak or man-made in origin. Should such an incident occur, the conflict between the two agencies as to who would have lead authority would be unseemly, at best. At worst, such conflicts could hinder timely and appropriate response and thus exacerbate fatalities and economic damage.

Here too, the multitude of agencies and the disaggregation of responsibility may be depicted in a simple chart. As this chart reflects, we lack an effective doctrine for determining vital command and control issues.

---

<sup>59</sup> “Catastrophic Incident Annex,” [http://www.fema.gov/pdf/emergency/nrf/nrf\\_CatastrophicIncidentAnnex.pdf](http://www.fema.gov/pdf/emergency/nrf/nrf_CatastrophicIncidentAnnex.pdf).

**Table 2—Bio Threats: Prepare and Respond**

*State/Federal Transition*

*HHS/DHS Transition (?)*



	<b>Routine Scale</b>	<b>Non Catastrophic–Supportive</b>	<b>Major Disruption</b>	<b>Catastrophic–Major Injection</b>
<b>Natural Outbreak</b>	S/L Public Health HHS USDA	HHS USDA State/Local DHS (?)	HHS lead DHS supportive	HHS lead (?)
<b>Biological Attack</b>	S/L Public Health S/L Hazmat HHS EPA →→ FBI-WMD →→	HHS NCTC →→ DHS →→ DOT (mode) USDA (food/water)	HHS lead (under Bio-Incident Annex) DHS (supportive) FBI ODNI/CIA	DHS lead (under Catastrophic Incident Annex) (?) HHS (supportive) FBI ODNI/CIA

## IV. Recommendations

Improved Federal Coordination: The current Administration has, through the appointment of a WMD coordinator, made an effort to address the lack of cross-government coordination for the detection and prevention of biological threats. But, as the foregoing review makes clear, there continues to be confusion and an overlap of responsibilities. The dry recitation of facts masks a traditional Washington concern—a battle over turf and budgets—and makes clear that more effort is required

No organizational plan is likely to succeed if a single Federal agency is given a comprehensive lead responsibility. One would expect that sensitivities and legislative barriers are too great to

ever permit, for example, DHS to be made responsible – and funded -- for coordinating all biological threat responses. What is required is decisive leadership from the White House to resolve the current confusion and provide a focal point for public sector coordination.

This is easier said than done. Precisely the same arguments were made in support of the creation of the ODNI and DHS. In both cases a central focal point was thought necessary to achieve effective coordination of executive branch action. Both efforts may fairly be characterized as “ongoing works in progress” whose ultimate efficacy has yet to be conclusively determined. And just as the subordinated agencies have resisted inclusion within ODNI or DHS, it is likely (indeed nearly certain) that HHS and DHS would resist the strengthening of any White House or other centralized control of biological threat issues.

If this logjam is to be broken, a new biological threat coordinator must, in effect, become the *de jure* leader of the Federal effort.<sup>60</sup> This will require a strong commitment from the White House and the creation of a single, dedicated locus empowered and funded to coordinate the response to biological threats. It will be necessary to give the coordinator authority to:

- Create a unified biological threats and security budget account within the President’s annual budget submission and work with the Office of Management and Budget and the NSC to set budget priorities with that account;
- Lead and coordinate the development of biological threat policy (including through chairmanship of a dedicated policy planning group);
- Direct agency action in conformance with the budgetary and policy priorities set;
- Have indirect and consultative authority over, and a role in the selection of, cabinet-level and sub-cabinet leaders in the agencies and their components which deal with biological threat issues; and
- Lead a process to develop a comprehensive set of objectives derived from the National Biostrategy that will contain a set of measurable performance goals and objectives for biological threat reduction and resilience.

To achieve this level of coordination and secure the cooperation of other Federal agencies, it is almost certain that the coordinator will need to have cabinet-rank and report directly to the President. Any lesser degree of empowerment will foreclose any realistic possibility of success. In short, if it wishes to advance the coordination function in a meaningful way, the White House must take ownership of the biological threat issue and endow the coordinator position with the authority necessary to achieve a set of clearly-defined and -articulated goals.

---

<sup>60</sup> In a real crisis today, it is likely that operational control would be provided by the President acting through his national security advisors with implementation being supervised by the Secretaries of Homeland Security and Health and Human Services. To the extent this structure has become the anticipated *de facto* norm, it would be prudent to institutionalize it. To the extent it has not, clarification would be most appropriate.

Finally, it is worth acknowledging that we should not be completely sanguine at the prospects for success in achieving this sort of restructuring. In addition to opposition from agencies whose roles and responsibilities will be modified, we should anticipate significant opposition from the Congress, State and local authorities, and the private sector whose activities would be regulated by such a coordinator. Congressional inertia and interest in protecting jurisdictional prerogatives is widespread; State and local officials are loath to accept Federal direction (even while asking for Federal resources; and the private sector is resistant to any activity that empowers governmental oversight. Coordinated budgeting will require the cooperation of the Appropriations Committees in both houses of the Congress in consolidating their consideration of the President's budget request. Changes to various legislation setting the roles and responsibilities of Federal agencies as well as the Federal government's authority and obligations to State and local governments will require support from an even broader range of committees. To the extent that legislative enactments are required to achieve centralizing objectives, their passage will require a significant investment of Presidential political capital.

Develop a Clear Doctrine For Transitioning Authority As a Biological Incident Develops: No coordinating system can work if the lines of authority are not carefully drawn. The only thing worse than having nobody in charge is having more than one person in charge or, worse yet, several people disagreeing as to who bears responsibility.

Of course, within the Federal government, the President will have the ultimate responsibility for coordinating any Federal response. To that end, if a strong national biological threat coordinator is appointed, that same coordinator would serve well as the individual with operational control over any coordinated Federal response.

Such a strong, centralized, operational role for the White House is unlikely to materialize any time soon, since virtually all of the assets available to the Federal government for use in a response action will be deployed by one of the constituent agencies, which will likely resist any centralizing effort. Moreover, even if a centralized authority for the Federal government were capable of being created, we would continue to have much the same problem we do today in response to any natural disaster—even a strong Federal leader has difficulty coordinating the activities of State, local and private sector stakeholders.

Thus, for the foreseeable future, the most realistic expectation is for a set of clear lines of authority and specific demarcation points to mark the transitions of authority within the response structures. We need clear doctrine to define the thresholds for: a) the transition from State to Federal level responsibility; and b) the transition (if any) within the Federal government from HHS-led to DHS-led responsibility.

As an urgent matter, the Federal government should sponsor an internal study of this matter with the goal of defining U.S. doctrine for those transition thresholds. The key characteristics of success for such a doctrine would be clarity and resolution in defining the thresholds. As noted

above, the transition points identified must be selected with the unique aspects of biological threats (e.g., geographic dispersal; time-delayed detection; and public fear) in mind.

That having been said, the following is offered as a rough approximation of a set of thresholds that make some logical sense (assuming, for now, that any threshold unit developed for a single-incident event is appropriately generalized to the biological response arena), and which (if adopted) would provide the necessary clarity:

- State to Federal Transition
  - Authority for coordination of medical response activities transitions when:
    - A state requests Federal assistance; or
    - Casualties exceed 10,000; or
    - Economic effects exceed \$10 Billion; or
    - The President so directs (most likely in situations where a delay to allow State and local responses to occur first is judged to create a risk).
  - Authority for investigation of the causes of the outbreak transitions when:
    - Actionable forensic evidence is developed indicating that the outbreak was caused by deliberate human action; or
    - A State requests Federal assistance;
    - The President so directs.
- Federal Transition—HHS to DHS
  - Authority for coordinating the medical response activities of the Federal government transition when:
    - The President so directs.
  - Authority for coordinating the non-medical response activities in response to the outbreak transitions when:
    - Actionable forensic evidence is developed indicating that the outbreak was caused by deliberate human action; or
    - The President so directs.

If these thresholds, or any similar set of thresholds, were to be developed and adopted as an affirmative statement of national policy, many of the transition challenges identified would be alleviated.

Develop a More Robust and Comprehensive Planning and Exercise Program for Biological Threats: To a very real degree the two theoretical problems outlined above (lack of a Federal coordinating structure and lack of a good sense of authority transition points) are grounded in the practical on-the-ground application of doctrine to reality. Our Federal bureaucracy is a complex organization in which the interagency battle over turf and budgets gets in the way of progress. Leadership is required at the highest levels to achieve the goal of an effective response to a biological or other weapon of mass destruction incident.

We have (thankfully) little practical experience from which to derive lessons on how to deal with a biological incident. Save for the H1N1 pandemic, we have no recent comprehensive national experience relating to the challenges of Federal coordination and the inter-governmental transfer of authority. Specific threshold measures we might use to gauge our response are, at best, educated guesses and at worse, conjecture. We need to make an effort to establish better *ex ante* rules to govern in a time of crisis, but have inadequate data to do so.

This suggests the final recommendation. The necessary experience can be gained by exercising response plans in which principals and their advisors at the Federal, State, and local government levels participate, and then by reviewing the results of those exercises for lessons learned and gaps identified. As a matter of some urgency, we may best address the leadership challenges presented by biological threats through the development of a more robust and comprehensive set of exercises and planning efforts that will afford us the requisite experience base to guide our future doctrine.