United States Government Accountability Office

Testimony
Before the Subcommittee on Emergency Preparedness, Response, and Communications, Committee on Homeland Security, House of Representatives

For Release on Delivery
Expected at 2 p.m. ET
Thursday, February 11, 2016

BIOSURVEILLANCE

Ongoing Challenges and Future Considerations for DHS Biosurveillance Efforts

Statement of Chris Currie, Director, Homeland Security and Justice

February 11, 2016

BIOSURVEILLANCE

Ongoing Challenges and Future Considerations for DHS Biosurveillance Efforts

GAO Highlights

Highlights of GAO-16-413T, a testimony before the Subcommittee on Emergency Preparedness, Response, and Communications; Committee on Homeland Security, House of Representatives

Why GAO Did This Study

The potential threat of a naturally occurring pandemic or a terrorist attack with a biological weapon of mass destruction underscores the importance of a national biosurveillance capability—that is, the ability to detect biological events of national significance to provide early warning and information to guide public health and emergency response. The Implementing Recommendations of the 9/11 Commission Act of 2007 addresses this capability, in part by creating NBIC. The center was tasked with integrating information from human health, animal, plant, food, and environmental monitoring systems across the federal government, to improve the likelihood of identifying a biological event at an earlier stage. Similarly, DHS's BioWatch program aims to provide early indication of an aerosolized biological weapon attack.

GAO has published a series of reports on biosurveillance efforts spanning more than a decade. This statement describes progress and challenges GAO has reported in DHS's implementation of NBIC and BioWatch and considerations for the future of biosurveillance efforts at DHS.

This testimony is based on previous GAO reports issued from December 2009 through September 2015 related to biosurveillance. To conduct our prior work, we reviewed relevant presidential directives, laws, policies, and strategic plans; and interviewed federal, state, and industry officials, among others. We also analyzed key program documents, including test plans, test results, and modeling studies.

View GAO-16-413T. For more information, contact Chris Currie at (404) 679-1875, or curriec@gao.gov.

What GAO Found

Since 2009, GAO has reported on progress and challenges with two of the Department of Homeland Security's (DHS) biosurveillance efforts—the National Biosurveillance Integration Center (NBIC) and the BioWatch program (designed to provide early detection of an aerosolized biological attack). In December 2009, GAO reported that NBIC was not fully equipped to carry out its mission because it lacked key resources—data and personnel—from its partner agencies, which may have been at least partially the result of collaboration challenges it faced. For example, some partners reported that they did not trust NBIC to use their information and resources appropriately, while others were not convinced of the value that working with NBIC provided because NBIC's mission was not clearly articulated. GAO recommended that NBIC develop a strategy for addressing barriers to collaboration and develop accountability mechanisms to monitor these efforts. DHS agreed, and in August 2012, NBIC issued the NBIC Strategic Plan, which is intended to provide NBIC's strategic vision, clarify the center's mission and purpose, and articulate the value that NBIC seeks to provide to its partners, among other things. In September 2015, GAO reported that despite NBIC's efforts to collaborate with interagency partners to create and issue a strategic plan that would clarify its mission and the various efforts to fulfill its three roles—analyzer, coordinator, and innovator—a variety of challenges remained when GAO surveyed NBIC's interagency partners in 2015. Notably, many of these partners continued to express uncertainty about the value NBIC provided. GAO identified options for policy or structural changes that could help NBIC better fulfill its biosurveillance integration mission, such as changes to NBIC's roles.

Since 2012, GAO has reported that DHS has faced challenges in clearly justifying the need for the BioWatch program and its ability to reliably address that need (to detect attacks). In September 2012, GAO found that DHS approved a next-generation BioWatch acquisition in October 2009 without fully developing knowledge that would help ensure sound investment decision making and pursuit of optimal solutions. GAO recommended that before continuing the acquisition, DHS reevaluate the mission need and possible alternatives based on cost-benefit and risk information. DHS concurred and in April 2014, canceled the acquisition because an alternatives analysis did not confirm an overwhelming benefit to justify the cost. Having canceled the next generation acquisition, DHS continues to rely on the currently deployed BioWatch system for early detection of an aerosolized biological attack. However, in 2015, GAO found that DHS lacks reliable information about the current system's technical capabilities to detect a biological attack, in part because in the 12 years since BioWatch's initial deployment, DHS has not developed technical performance requirements for the system. GAO reported in September 2015 that DHS commissioned tests of the current system's technical performance characteristics, but without performance requirements, DHS cannot interpret the test results and draw conclusions about the system's ability to detect attacks. DHS is considering upgrades to the current system, but GAO recommended that DHS not pursue upgrades until it establishes technical performance requirements to meet a clearly defined operational objective and assesses the system against these performance requirements. DHS concurred and is working to address the recommendation.

Chairman McSally, Ranking Member Payne, and Members of the Subcommittee:

I am pleased to be here today to discuss our work on the Department of Homeland Security's (DHS) biosurveillance efforts. Biosurveillance, as defined by the July 2012 *National Strategy for Biosurveillance*, is the ongoing process of gathering, integrating, interpreting, and communicating essential information related to all-hazards threats or disease activity affecting human, animal, or plant health, for the purpose of (1) achieving early detection and warning, (2) contributing to overall situational awareness of the health aspects of the incident, and (3) enabling better decision making at all levels.

Threats of bioterrorism, such as anthrax attacks, and high-profile disease outbreaks, such as Ebola in West Africa and emerging arboviruses like chikungunya and zika in the Americas, highlight the continued need for systems that provide early detection and warning about biological threats.[1] We have an ongoing body of biosurveillance work spanning more than a decade in which we have examined specific surveillance programs and activities carried out by DHS; the Departments of Health and Human Services; Agriculture; and several other federal departments and agencies.[2]

We have also identified broad, cross-cutting issues in leadership, coordination, and collaboration that arise from working across the complex interagency, intergovernmental, and intersectoral biosurveillance enterprise. To address these issues, in 2010 we made recommendations that the Homeland Security Council direct the National Security Council staff to identify a focal point to lead the development of a national biosurveillance strategy that would, among other things, (1) define the

[1]Arthropod-borne viruses (arboviruses) are transmitted to humans primarily through the bites of infected mosquitoes and ticks.

[2]See, for example, GAO, *Emerging Infectious Diseases: Review of State and Federal Disease Surveillance Efforts*, GAO-04-877 (Washington, D.C.: Sept. 30, 2004), which discusses select federal and nonfederal human disease surveillance in humans; GAO, *Global Health: U.S. Agencies Support Programs to Build Overseas Capacity for Infectious Disease Surveillance*, GAO-07-1186 (Washington, D.C.: Sept. 28, 2007), which discusses four key programs aimed at building overseas surveillance capacity for infectious diseases in humans; and GAO, *Homeland Security: An Overall Strategy Is Needed to Strengthen Disease Surveillance in Livestock and Poultry*, GAO-13-424 (Washington, D.C.: May 21, 2013), which discusses the Department of Agriculture's efforts to better detect and control new or reemerging diseases in animals.

scope and purpose of a national capability; (2) provide goals, objectives and activities, priorities, milestones, and performance measures; and (3) assess the costs and benefits and identify resource and investment needs, including investment priorities.[3] In July 2012, the White House released the *National Strategy for Biosurveillance* to describe the U.S. government's approach to strengthening biosurveillance, but it did not fully meet the intent of our prior recommendations, because it did not offer a mechanism to identify resource and investment needs, including investment priorities among various biosurveillance efforts.[4]

In 2014, a Blue Ribbon Study Panel on Biodefense was established to assess gaps and provide recommendations to improve U.S. biodefense. The panel's October 2015 final report identified several themes we have also highlighted in our biosurveillance work, including the lack of a centralized leader, no comprehensive national strategic plan, and no all-inclusive dedicated budget for biodefense. The panel's report highlights a sense of urgency to address the ongoing and persistent biological threats—both naturally occurring, like Ebola and zika, and from enemies, like The Islamic State of Iraq and the Levant (also known as ISIL and Da'esh) who have advocated for the use of biological weapons.

While consequences of a biologic event could be catastrophic, we have also previously reported that because the nation cannot afford to protect everything against all threats, choices must be made about protection priorities given the risk and how to best allocate available resources.[5] As we testified before this committee in 2012, without a national strategy that provides a framework and tool set to evaluate tradeoffs, it remains difficult

[3]GAO, Biosurveillance: Efforts to Develop a National Biosurveillance Capability Need a National Strategy and a Designated Leader, GAO-10-645 (Washington, D.C.: June 30, 2010). See also, GAO, Biosurveillance: Nonfederal Capabilities Should Be Considered in Creating a National Biosurveillance Strategy, GAO-12-55 (Washington, D.C.: Oct. 31, 2011), in which we recommended that the strategy also (1) incorporate a means to leverage existing efforts that support nonfederal biosurveillance capabilities, (2) consider challenges that nonfederal jurisdictions face in building and maintaining biosurveillance capabilities, and (3) include a framework to develop a baseline and gap assessment of nonfederal jurisdictions' biosurveillance capabilities.

[4]The National Security Council staff has since created an implementation plan for the national strategy. However, it is not yet clear the extent to which the plan has been widely shared among and adopted by interagency decision makers as a means to help identify opportunities to leverage resources and direct priorities.

[5]GAO, 21st Century Challenges: Reexamining the Base of the Federal Government, GAO-05-325SP (Washington, D.C.: Feb. 1, 2005).

for decision makers—in both the executive and legislative branches—to help ensure that biosurveillance resource allocation decisions within single departments and programs contribute to a coherent enterprisewide approach.[6]

Nevertheless, challenges we have reported in two of DHS's specific biosurveillance efforts—the National Biosurveillance Integration Center (NBIC) and the BioWatch program—demonstrate the importance of following departmental policies and employing leading management practices to help ensure that the mission of each program is clearly and purposefully defined and that subsequent investments effectively respond to those missions. NBIC, which was created to integrate data across the federal government with the aim of enhancing detection and situational awareness of biological events, has suffered from longstanding issues related to its clarity of purpose. Likewise, the BioWatch program, which is designed to detect bioterrorism attacks with specific aerosolized pathogens, has encountered challenges that stem from not precisely defining the need its technologies should fill and how the technologies it pursued (and in some cases developed and deployed) responded to that need.

Finally, DHS is currently at a crossroads for decisions regarding not only NBIC and BioWatch, but also where these efforts fall within DHS's broader Chemical, Biological, Radiological and Nuclear (CBRNE) programs. In June 2015, DHS provided Congress a report summarizing its review of the organization, operations, and communications of its Chemical, Biological, Radiological and Nuclear programs and proposed merging six CBRNE-related organizational components into one unit.[7] This provides an opportunity for DHS to look strategically at its biosurveillance efforts.

This statement describes progress and challenges we have reported in DHS's implementation of NBIC and BioWatch and considerations for the future of these biosurveillance efforts at DHS. Our statement is based on

[6]GAO, Biosurveillance: Observations on BioWatch Generation-3 and Other Federal Efforts. GAO-12-994T (Washington, D.C., Sept. 2012).

[7]The Senate explanatory statement accompanying the Consolidated and Further Continuing Appropriations Act, 2013, directed DHS to conduct a review and to provide a report of the results. On December 10, 2016, the Department of Homeland Security CBRNE Defense Act of 2015, which would establish a CBRNE Office within DHS, was passed by the House of Representatives. H.R. 3875 (114th Cong.).

our prior work issued from December 2009 through October 2015 on various biosurveillance efforts.[8] The work upon which this testimony is based was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. To conduct this prior work, we reviewed relevant presidential directives, laws, regulations, policies, and strategic plans; surveyed states; and interviewed federal, state, and industry officials, among others. We also analyzed key program documents, including test plans, test results, and modeling studies. More information on our scope and methodology can be found in each of the reports cited throughout this statement.

Background

DHS's Biosurveillance Roles and Responsibilities

According to DHS's 2014 Quadrennial Homeland Security Review (QHSR), biological threats and hazards—ranging from bioterrorism to naturally occurring pandemics—are a top homeland security risk. The QHSR acknowledges that numerous departments and agencies at the federal, state, local, tribal, and territorial levels, as well as the private sector, contribute to the national effort to address biological threats and hazards. As such, according to the QHSR, DHS aims to focus on those activities and responsibilities assigned to it through statute or presidential directive. Among the identified activities and responsibilities is one that is specific to biosurveillance—biosurveillance integration and detection—and others that can help to support efficient and effective biosurveillance action, such as information sharing and analysis, threat and risk awareness, and technical forensic analysis to support attribution.

NBIC

The Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Commission Act) established the National Biosurveillance

[8]GAO, Biosurveillance: Developing a Collaboration Strategy Is Essential to Fostering Interagency Data and Resource Sharing, GAO-10-171 (Washington, D.C.: Dec. 18, 2009); GAO, Biosurveillance: DHS Should Reevaluate Mission Need and Alternatives before Proceeding with BioWatch Generation-3 Acquisition, GAO-12-810 (Washington, D.C.: Sept. 10, 2012); GAO, Biosurveillance: Challenges and Options for the National Biosurveillance Integration Center, GAO-15-793 (Washington, D.C.: Sept. 24, 2015); GAO, Biosurveillance: DHS Should Not Pursue BioWatch Upgrades or Enhancements Until System Capabilities Are Established, GAO-16-99 (Washington, D.C.: Oct. 23, 2015).

Integration Center (NBIC) within DHS.[9] NBIC was specifically tasked with integrating and analyzing information from human health, animal, plant, food, and environmental monitoring systems across the federal government and supporting the interagency biosurveillance community. As defined in the July 2012 NBIC Strategic Plan, integration involves combining biosurveillance information from different sources and domains (e.g., human, animal, and plant health; food and environmental safety and security; and homeland security) to provide partners and stakeholders with a synthesized view of the information, and what it could mean. Primary goals of integration include creating a common picture or understanding of potential and ongoing biological events and providing insights that cannot be gleaned in isolation.

The 9/11 Commission Act outlines certain requirements for NBIC. Drawing upon these requirements as well as the NBIC Strategic Plan, we identified three main roles that NBIC, as a federal-level biosurveillance integrator, must carry out to achieve the duties and outcomes described by NBIC's authorizing legislation.[10] Senior NBIC officials agreed that these three roles—analyzer, coordinator, and innovator—are consistent with the center's responsibilities. These roles are not mutually exclusive and can reinforce one other. For example, NBIC's efforts as an Innovator might result in the development of data that could enhance its role as an Analyzer by providing the center with another dataset to review. The biosurveillance integrators' roles we identified:

- **Analyzer:** Use technological tools and subject matter expertise to develop shared situational awareness by creating meaningful new insights from disparate datasets and information that could not be gleaned in isolation.
- **Coordinator:** Bring together multi-disciplinary partners across interagency organizations to enhance understanding of new or potential biological events, such as through the collaborative development of products and services.
- **Innovator:** Facilitate the development of new tools, technology, and approaches to address gaps in biosurveillance integration.

[9]6 U.S.C. § 195b.

[10]GAO-15-793

BioWatch

According to Homeland Security Presidential Directive 10 (HSPD-10): *Biodefense for the 21st Century*, a national bioawareness capability providing early warning, detection, or recognition of a biological weapon attack is an essential component of biodefense.[11] To contribute to this national capability, in 2003, DHS created the BioWatch program to provide early warning, detection, or recognition of a biological attack. The BioWatch program uses routine laboratory testing designed to detect an aerosolized biological attack for five specific biological agents considered high risk for use as biological weapons.

When DHS was established in 2002, a perceived urgency to deploy useful—even if immature—technologies in the face of potentially catastrophic consequences catalyzed the rapid deployment of many technologies. DHS completed the initial deployment of BioWatch quickly—within 80 days of the President's announcement of the BioWatch program in his 2003 State of the Union Address.[12] In 2005, DHS expanded BioWatch to an additional 10 jurisdictions, for a total of more than 30. The expanded deployment—referred to as Generation 2 (Gen-2)—also included the addition of indoor monitoring capabilities in three high-threat jurisdictions and provided additional capacity for events of national significance, such as major sporting events and political conventions.

In 2015, we reported that the BioWatch program collaborates with more than 30 BioWatch jurisdictions throughout the nation to operate approximately 600 Gen-2 aerosol collectors. These units rely on a vacuum-based collection system that draws air through a filter. These filters are manually collected and transported to state and local public health laboratories for analysis. Using this manual process, a result can be generated from 12 to 36 hours after an agent is initially captured by the aerosol collection unit.

To reduce detection time, DHS began to develop an autonomous detection capability in 2003 for the BioWatch program—known as

[11]HSPD-10: Biodefense for the 21st Century (Washington, D.C., April 2004).

[12]In the initial deployment of BioWatch—known as Generation-1—DHS deployed aerosol collectors to 20 major metropolitan areas, known as BioWatch jurisdictions, to monitor primarily outdoor spaces.

Generation 3 (Gen-3).[13] Envisioned as a laboratory-in-a-box, the autonomous detection system would automatically collect air samples, conduct analysis to detect the presence of biothreat agents every 4 to 6 hours, and communicate the results to public health officials via an electronic network without manual intervention. By automating the analysis, DHS anticipated that detection time could be reduced to 6 hours or less, making the technology more appropriate for monitoring indoor high-occupancy facilities such as transportation nodes and enabling a more rapid response to an attack. DHS also anticipated a reduction in operational costs by eliminating the program's daily manual sample retrieval and laboratory analysis. However, as we reported in 2015, the Gen-3 acquisition was canceled in April 2014, after testing difficulties and after an analysis of alternatives was interpreted by DHS as showing that any advantages of an autonomous system over the current manual system were insufficient to justify the cost of a full technology switch.

DHS Has Faced Challenges, Some Persistent, In Its Efforts to Carry Out Biosurveillance Programs

NBIC Has Faced Difficulty Demonstrating Value to Interagency Partners

In December 2009, we reported that NBIC was not fully equipped to carry out its mission because it lacked key resources—data and personnel—from its partner agencies, which may have been at least partially the result of collaboration challenges it faced. For example, some partners reported that they did not trust NBIC to use their information and resources appropriately, while others were not convinced of the value that working with NBIC provided because NBIC's mission was not clearly articulated.

[13]Initially, DHS's Science &Technology Directorate, partnering with industry, led the development of technologies to support autonomous detection. DHS's Office of Health Affairs has had responsibility for overseeing the acquisition of this technology since fiscal year 2007.

In order to help NBIC enhance and sustain collaboration, including the provision of data, personnel, and other resources, in 2009, we recommended that NBIC develop a strategy for addressing barriers to collaboration and develop accountability mechanisms to monitor these efforts. In August 2012, NBIC issued the NBIC Strategic Plan, which is intended to provide NBIC's strategic vision, clarify the center's mission and purpose, articulate the value that NBIC seeks to provide to its partners, and lay the groundwork for setting interagency roles, responsibilities, and procedures. Further, in November 2014, NBIC completed its first biannual NBIC Federal Stakeholder Survey, which NBIC uses to assess the usefulness of its products and activities and to determine what improvements should be made on the basis of those results. We believe DHS's actions addressed the recommendations in our December 2009 report.

In September 2015, we reported that NBIC had actions and activities underway to fulfill all three of the roles we identified as essential to its ability to carry out its mission—analyzer, coordinator, and integrator. For example, to fulfill its analyzer role NBIC compiled information to create and circulate a variety of products to support disease outbreak monitoring on a daily, weekly, or period basis. Similarly, in its coordinator role, NBIC had put in place a variety of procedures and protocols to convene partners on a routine basis or in response to specific emerging events. Finally, in its innovator role NBIC had efforts to conduct gap analyses, fund pilot projects that aim to develop new biosurveillance tools and technology (such as examining the use of social media data to identify health trends), sought new sources of data and information, and made efforts to enhance its internal IT system.

Although NBIC had made efforts to collaborate with interagency partners to create and issue a strategic plan that would clarify its mission and the various efforts to fulfill its three roles, we reported a variety of challenges that remained when we surveyed NBIC's interagency partners for our 2015 report. Notably, many of these partners continued to express uncertainty about the value NBIC provided. Specifically, 10 of 19 partners stated that NBIC's products and activities enhance their agencies' ability to carry out their biosurveillance roles and responsibilities to little or no extent, 4 responded to a moderate extent, and 5 responded that they did

not have a basis to judge.[14] Generally, partners that responded to little or no extent noted that NBIC products and activities do not, for example, identify trends and patterns or describe potential impacts of a biological event. For instance, one official stated that NBIC's products and activities do not "connect the dots" between dissimilar information, provide novel synthesis of information, or recommend possible courses of action. Moreover, most of the federal partners with key roles in biosurveillance (8 of 11) stated that NBIC's products help their agencies identify biological events to little or no extent, generally because they already obtain such information directly from other federal partners more quickly.

We also found in 2015, as in 2009, that a variety of challenges limited the extent to which federal agencies shared data and personnel with NBIC, as envisioned by the 9/11 Commission Act. First, data that NBIC could use to identify and characterize a biological event of national concern using statistical and analytical tools, as called for in the 9/11 Commission Act, are limited. Also, apart from searches of global news reports and other publically available reports generated by National Biosurveillance Integration System (NBIS) partners,[15] NBIC has been unable to secure streams of raw data from multiple domains across the biosurveillance enterprise that would lend themselves to near-time quantitative analysis that could reveal unusual patterns and trends.[16]

Moreover, we found that few federal partners (5 of 19) reported that they share the data they do have with NBIC, citing legal and regulatory restrictions, among other reasons. Some agencies are reluctant to share

[14]Generally, these 5 partners stated that they did not have a basis to judge because they are biosurveillance information consumers or they considered their role in biosurveillance to be relatively small.

[15]The NBIS is a consortium of federal partners that was established to rapidly identify and monitor biological events of national concern and to collect; analyze; and share human, animal, plant, food, and environmental biosurveillance information with NBIC.

[16]NBIC acknowledged in its strategic plan that the data required to carry out its mission as envisioned in the 9/11 Commission Act either do not exist or are subject to a variety of information sharing challenges that make a large information technology-centered solution less feasible than originally imagined. Additionally, NBIC and NBIS partners noted that there were several kinds of data that could be useful for this kind of biosurveillance integration, but these data may not exist or may not be in a usable form, such as real-time data on water quality and contamination from drinking water utilities and data on wildlife disease, which makes it difficult to fully understand the dynamics of zoonotic diseases. NBIC officials also noted that other kinds of data are maintained in formats that make them difficult to analyze, such as paper health records.

their data with NBIC because they are unsure how the information will be used. For example, one official explained that the agency does not share some data with NBIC because sharing such information too broadly might have substantial implications on agricultural trade or public perception of safety. Officials from another agency noted that there is sometimes reticence to share information and data with components of DHS because, given the department's roles in law enforcement and national security, the information might be shared outside of the health security community in a way that lacks appropriate context and perspective. Finally, other agencies stated that they are unable to share data for regulatory or legal reasons, or because appropriately protecting the data would take too long.[17]

Similarly, although NBIC would like to obtain liaisons from each of its federal partners, only 3 of 19 partners provided NBIC with dedicated liaisons. Officials from one agency with key biosurveillance responsibilities stated that it is difficult to provide personnel to NBIC on a full- or part-time basis because of resource constraints. Further, officials from another agency noted that the lack of clarity about NBIC's value to its partners is a barrier to providing the center with detailees.

We also reported in September 2015 that NBIC faces challenges prioritizing developmental efforts to identify and address needs for new biosurveillance tools. For example, partners noted limitations in NBIC's ability to address gaps, like limited resources and the difficulty in prioritizing the center's innovation efforts because its partners have diverse needs.

[17]For example, according to Centers for Disease Control and Prevention (CDC) officials, their agency receives electronic data from state, territorial, local, and tribal sources for a variety of programs and purposes that are covered by data use agreements that do not allow CDC to share the data outside the terms of those agreements and as allowed or required by applicable federal laws, such as the Privacy Act of 1974 and the Freedom of Information Act, 5 U.S.C. § 552a; 552. CDC officials said of the data they can share, it would take extensive, time consuming work to appropriately redact the data to ensure that individuals may not be identified and that privacy is protected, which results in the release of the data being postponed to the point that the data are no longer actionable.

Multiple Structural and Policy Considerations Could Help Focus NBIC's Efforts

NBIC officials stated that the center is working to improve its products and its ability to contextualize the information it collects from open sources, and has sought partner input to do so. For example, beginning in late June 2015, partly on the basis of feedback the center received from its November 2014 Federal Stakeholder Survey, NBIC modified its daily Monitoring List to include an up-front summary that identifies the status of ongoing biological events as worsening, improving, unchanged, or undetermined. Further, NBIC officials noted that the center is also working to better integrate forecasts and projections into its products and activities by collaborating with others and developing a common interagency vision for specific federal capabilities and practical next steps leading to the application of reliable infectious disease forecasting models in decision-making processes.

Nevertheless, a persistent challenge NBIC faces is skepticism on the part of some of the NBIS partners regarding the value of the federal biosurveillance mission as well as NBIC's role in that mission. In our 2009 report, most of the NBIS partners we interviewed at that time expressed uncertainty about the value of participating in the NBIS or confusion about the purpose of NBIC's mission. In September 2015, the NBIS partners and other major stakeholders in the biosurveillance community acknowledged—and we agreed—that no single problem limits NBIC's mission to integrate biosurveillance data. Rather, over the years, several long-standing problems have combined to inhibit the achievement of this mission as envisioned in the 9/11 Commission Act. We identified options in our 2015 report for policy or structural changes that could help better fulfill the biosurveillance integration mission, which are summarized below. We identified these options and their benefits and limitations, on the basis of the roles of a federal-level biosurveillance integrator we identified in the 9/11 Commission Act, NBIC's strategic plan, and the perspectives of the NBIS partners obtained during our structured interviews. These options are not exhaustive, and some options could be implemented together or in part.[18]

[18]In developing these options, we did not evaluate the financial implications of implementing each option, to the extent they are knowable, but we acknowledge they are likely to result in an increase, decrease, or shifting of funding based on the changes described.

Table 1: Benefits and challenges of options for policy or structural changes for the National Biosurveillance Integration Center (NBIC)

Option	Description	Benefits	Challenges
Reinforce NBIC's Analyzer Role	Under this option, NBIC would be provided with new authorities and resources designed to access additional public and private data sources and statistical and modeling tools to develop meaningful information.	Developing meaningful information not otherwise available. Capitalize on new data sources and analysis techniques.	Uncertainty in knowing whether an event would be detected more quickly by overlaying various data streams and applying statistical and analytical tools to them. There may not be a significant amount of meaningful data available that is not already being provided to facilitate advanced analytical techniques. The concept of whether a federal biosurveillance integrator would be able to identify patterns or connections that would lead to earlier warning of emerging events is unproven. Unknown impact of earlier detection. Increased costs.
Strengthen NBIC's Coordinator Role	Under this option, NBIC would be provided with greater authority for coordinating the federal biosurveillance enterprise.	This option would create clear leadership across the interagency. Better institutional connection. Routine, institutionalized channels to monitor for emerging trends and patterns. Enhanced accountability for implementing the *National Strategy for Biosurveillance.*	Some of these responsibilities overlap with responsibilities that have historically been the purview of the National Security Council staff. It may be difficult for an agency at NBIC's level to successfully influence decision making across the interagency.
Expand NBIC's Innovator Role	Under this option, NBIC would be provided with new authorities and resources to lead research and development investments of new tools and technology that would address gaps across the biosurveillance community.	NBIC could foster the development of tools and technology that benefit multiple federal partners and other members of the National Biosurveillance Integration System (NBIS). Coordinate research and development efforts.	Increased costs. A national integrator that focuses on innovation would likely need to acquire more expertise in research and development. Focusing attention on this role may represent a significant mission shift from the status quo, and may require very different sets of resources and procedures.
Continue to Execute the 2012 *NBIC Strategic Plan*	In this option, NBIC would continue to implement the mission, goals, and objectives detailed in the August 2012 *NBIC Strategic Plan* or subsequent NBIS-approved updates.	NBIC has made progress in this area and may continue to do so. Some agencies currently find value in NBIC's products.	NBIC will likely continue to face challenges in obtaining all the biosurveillance data it needs. Partners remain skeptical of NBIC's value.

Option	Description	Benefits	Challenges
Repeal the NBIC Statute	In this option, national biosurveillance integration would not be pursued through NBIC.	The cost of operating NBIC may not be worth its benefits.	Although federal partners generally thought that NBIC's products and activities did not provide meaningful new information, they largely thought that the concept of having a federal entity to integrate biosurveillance information across the federal government was important. Defunding NBIC could create a loss of investment, institutional learning, and progress made toward developing a federal biosurveillance integrator. Another integrator may experience similar challenges.

Source: GAO analysis of DHS information. GAO-16-413T

BioWatch's Ability to Detect Attacks Uncertain Because It Lacks Performance Requirements that Correspond to a Clearly Defined Mission

Since 2003, DHS has focused on acquiring an autonomous detection system to replace the current BioWatch Gen-2, but has faced challenges in clearly justifying the BioWatch program's need and ability to reliably address that need. In September 2012, we found that DHS approved the Gen-3 acquisition in October 2009 without fully developing critical knowledge that would help ensure sound investment decision making, pursuit of optimal solutions, and reliable performance, cost, and schedule information. Specifically, we found that DHS did not engage the early phases of its Acquisition Life-cycle Framework, which is designed to help ensure that the mission need driving the acquisition warrants investment of limited resources and that an analysis of alternatives (AoA) systematically identifies possible alternative solutions that could satisfy the identified need. BioWatch officials stated that they were aware that the Mission Needs Statement prepared in October 2009 did not reflect a systematic effort to justify a capability need, but stated that the department directed them to proceed because there was already departmental consensus around the solution. However, we found that the AoA prepared for the Gen-3 acquisition did not reflect a systematic decision-making process. As with the Mission Needs Statement, program officials told us that they were advised that a comprehensive AoA would not be necessary because there was already departmental consensus that autonomous detection was the optimal solution. Because the Gen-3 AoA did not evaluate a complete solution set, consider complete information on cost and benefits, and include a cost-benefit analysis, we concluded that it did not provide information on which to base trade-off decisions.

To help ensure DHS based its acquisition decisions on reliable performance, cost, and schedule information developed in accordance with guidance and good practices, in our September 2012 report, we recommended that before continuing the Gen-3 acquisition, DHS reevaluate the mission need and possible alternatives based on cost-benefit and risk information. DHS concurred with the recommendation and in 2012, DHS directed the BioWatch program to complete an updated AoA.[19] In April 2014, DHS canceled the acquisition of Gen-3 because the AoA did not confirm an overwhelming benefit to justify the cost of a full technology switch to Gen-3.

Having canceled the Gen-3 acquisition, DHS continues to rely on the Gen-2 system for early detection of an aerosolized biological attack. However, we found DHS lacks reliable information about BioWatch Gen-2's technical capabilities to detect a biological attack, in part, because in the 12 years since BioWatch's initial deployment, DHS has not developed technical performance requirements for Gen-2. We reported in 2015 that BioWatch has been criticized because it was deployed quickly in 2003 to address a perceived urgent need, but without sufficient testing, validation, and evaluation of its technical capabilities.[20] In 2015, we reported that DHS officials said that the system can detect catastrophic attacks, which they define as attacks large enough to cause 10,000 casualties. DHS has commissioned tests of Gen-2's technical performance characteristics, but DHS has not developed performance requirements that would enable it to interpret the test results and draw conclusions about the system's ability to detect attacks.[21] According to DHS guidance and standard practice in testing and evaluation of defense systems, in order to assess Gen-2's capability to detect a biological attack, DHS would have to link test results to its conclusions about the deployed detectors' ability to detect attacks in BioWatch operational environments. This would ordinarily be done by developing and validating technical performance requirements based on

[19]DHS contracted with the Institute for Defense Analyses to conduct the updated AoA, which they issued in December 2013.

[20]GAO-16-99. See also Institute of Medicine and National Research Council, BioWatch and Public Health Surveillance (Washington, D.C.: National Academies Press, 2011).

[21]In addition to these tests, DHS commissioned a demonstration of the system in an outdoor environment and conducts quality assurance tests on an ongoing basis. Both of these provide additional information about the system's capabilities; however, we do not include them in our list of key tests because neither was designed to produce estimates of key performance characteristics, including sensitivity, or to support conclusions about the types and sizes of attack the system can reliably detect.

operational objectives, but DHS has not developed such requirements for Gen-2.

In the absence of technical performance requirements, DHS officials said their assertion that the system can detect catastrophic attacks is supported by modeling and simulation studies. However, we found none of these studies were designed to incorporate test results from the Gen-2 system and comprehensively assess the system against the stated operational objective. The modeling and simulation studies were designed for purposes other than to directly and comprehensively assess Gen-2's operational capabilities. For example, one set of modeling and simulation studies, conducted by Sandia National Laboratories (Sandia) in collaboration with other national laboratories, did not incorporate information about the actual locations of Gen-2 collector units, because they were designed to model hypothetical BioWatch deployments in which collectors were placed in optimal locations. Sandia also analyzed ranges of hypothetical system sensitivities rather than incorporating the test results on the performance characteristics of Gen-2. Therefore, these studies drew no conclusions about the actual capabilities of the deployed Gen-2 system.[22] DHS officials also described modeling and simulation work that used a measure of operational capability that does not directly support conclusions about the BioWatch objective of detecting attacks large enough to cause 10,000 casualties.[23]

Additionally, we found that because none of the modeling and simulation work was designed to interpret Gen-2 test results and comprehensively assess the capabilities of the Gen-2 system, none of these studies has provided a full accounting of statistical and other uncertainties—meaning decision makers have no means of understanding the precision or confidence in what is known about system capabilities.[24] Because it is not

[22]Additionally, DHS had not prepared an analysis that combines the modeling and simulation studies with the specific Gen-2 test results to assess the system's capabilities to detect attacks.

[23]In general, these studies use a measure called fraction of population protected, or *Fp*. Roughly speaking, *Fp* represents a system's probability of successfully detecting simulated attacks, but calculated in a way that gives more weight to attacks that infect more people and less weight to attacks that infect fewer people.

[24]Best practices in risk analysis and cost-benefit analysis require an explicit accounting of uncertainties so that decision makers can grasp the reliability of, and precision in, estimates to be used for decision making. See Morgan and Henrion, Uncertainty, OMB Circular A-94, and OMB Circular A-4.

possible to test the BioWatch system directly by releasing live biothreat agents into the air in operational environments, limitations of the tests described earlier limit the applicability of the results and underscore the need for a full accounting of statistical and other uncertainties, without which decision makers lack a full understanding of the Gen-2 system's capability to detect attacks of defined types and sizes.

Understanding BioWatch's Current Capabilities Could Help Inform Future Biodetection Investments

At the time DHS canceled the Gen-3 acquisition, it also announced that S&T will explore development and maturation of an effective and affordable automated aerosol biodetection capability, or other operational enhancements, that meet the operational requirements of the BioWatch system. As such, DHS officials told us they are considering potential improvements or upgrades to the Gen-2 system. However, because DHS lacks reliable information about Gen-2's technical capabilities, decision makers are not assured of having sufficient information to ensure future investments are actually addressing a capability gap not met by the current system. Also, because DHS lacks targets for the current system's performance characteristics, including limits of detection, that would enable conclusions about the system's ability to detect attacks of defined types and sizes with specified probabilities, it cannot ensure it has complete information to make decisions about upgrades or enhancements.

In our September 2015 report, to help ensure that biosurveillance-related funding is directed to programs that can demonstrate their intended capabilities, and to help ensure sufficient information is known about the current Gen-2 system to make informed cost-benefit decisions about possible upgrades and enhancements to the system, we recommended that DHS not pursue upgrades or enhancements to the current BioWatch system until it establishes technical performance requirements necessary for a biodetection system to meet a clearly defined operational objective for the BioWatch program; assesses the Gen-2 system against these performance requirements; and produces a full accounting of statistical and other uncertainties and limitations in what is known about the system's capability to meet its operational objectives. DHS concurred and is taking steps to address the recommendation.

As DHS faces decisions about investing in the future of the BioWatch program, there are lessons to be learned from the program's recent attempt to acquire an autonomous detection system, Gen-3. Our recent work on BioWatch also evaluated DHS's efforts to test the Gen-3 technology from 2010 through 2011 against best practices for

developmental testing. In our 2015 report, we recommended that DHS incorporate the best practices we identified to help enable DHS to mitigate risk in future acquisitions, such as upgrades or enhancements to Gen-2. DHS concurred and stated its updated acquisition guidance largely addresses these best practices.

Chairman McSally, Ranking Member Payne, and Members of the subcommittee, this concludes my prepared statement. I would be happy to respond to any questions you may have.

GAO Contact and Staff Acknowledgments

For questions about this statement, please contact Chris Currie at (404) 679-1875 or curriec@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. Individuals making key contributions to this statement include Kathryn Godfrey (Assistant Director), Russ Burnett, Tracey King, Susanna Kuebler, Jan Montgomery, Tim Persons, and Sushil Sharma. Key contributors for the previous work that this testimony is based on are listed in each product.