United States Government Accountability Office

Report to Congressional Requesters

May 2021

BIODEFENSE

DHS Exploring New Methods to Replace BioWatch and Could Benefit from Additional Guidance

GAO@100
A Century of Non-Partisan Fact-Based Work

GAO-21-292

GAO@100 Highlights

Highlights of GAO-21-292, a report to congressional requesters

May 2021

BIODEFENSE

DHS Exploring New Methods to Replace BioWatch and Could Benefit from Additional Guidance

Why GAO Did This Study

Early detection of a biological attack can help reduce illness and loss of life, but DHS has faced challenges in acquiring biodetection capabilities to replace BioWatch, the current system used to detect aerosolized biological attacks. According to DHS, it is exploring the use of a new anomaly detection capability that, if developed successfully, could reduce the time to detection.

GAO was asked to examine the BD21 acquisition and assess technical maturity. This report (1) describes BD21 and the extent to which the program has followed DHS's acquisition policy, and (2) examines potential technical challenges to successful BD21 development, and actions to mitigate acquisition risks. GAO analyzed program acquisition documents against DHS acquisition policy and analyzed DHS's TRA guide against GAO's TRA best practices guide. GAO also interviewed DHS and DOD officials familiar with the BD21 acquisition effort for additional context.

What GAO Recommends

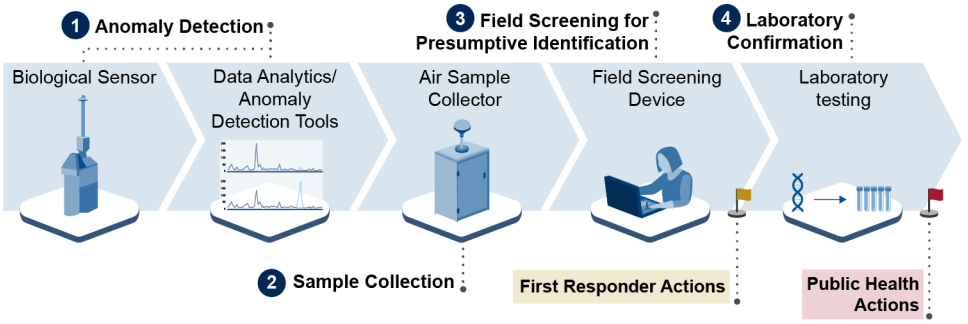
GAO makes three recommendations including that DHS incorporate best practices as outlined in GAO's TRA best practice guide into its TRA guidance, and ensures the BD21 program conducts TRAs that follow these best practices prior to the program's acquisition decision events. DHS concurred with all three GAO recommendations.

View GAO-21-292. For more information, contact Karen L. Howard at (202) 512-6888 or howardk@gao.gov or Chris P. Currie at (404) 679-1875 or curriec@gao.gov.

What GAO Found

The Department of Homeland Security (DHS) is following the agency's acquisition policy and guidance to acquire Biological Detection for the 21st Century (BD21). This system-of-systems concept—an assembly of technologies to gain higher functionality—is intended to combine various technologies, such as biological sensors, data analytics, anomaly detection tools, collectors, and field screening devices to enable timelier and more efficient detection of an aerosolized attack involving a biological agent than the current biodetection system. The BD21 program is early in the acquisition lifecycle and DHS has not yet selected the technologies to be used. Potential technologies are still being analyzed to demonstrate that certain components of the overall concept are feasible, such as an anomaly detection algorithm.

However, BD21 faces technical challenges due to inherent limitations in the technologies and uncertainties with combining technologies for use in biodetection. For example, biological aerosol sensors that monitor the air are to provide data on biological material in the environment, but common environmental material such as pollen, soil, and diesel exhaust can emit a signal in the same range as a biological threat agent, thereby increasing false alarm rates. Program officials report that the risk of false alarms produced by biological sensor technologies could be reduced by using an anomaly detection algorithm in addition to the sensor. However, it is too early to determine whether integration of an anomaly detection algorithm will successfully mitigate the false alarm rate. Specifically because the algorithms have never been developed and used for the purpose of biodetection in an urban, civilian environment.



Source: GAO analysis of Department of Homeland Security information. | GAO-21-292

BD21 program is following the agency's acquisition policy and guidance to mitigate technological risks in acquisition programs, and plans to conduct technology readiness assessments (TRA) along the way. In 2020, DHS issued a TRA guide, but it lacked detailed information about how the department will ensure objectivity and independence, among other important best practices GAO has identified. If DHS follows GAO's best practices guide, decision makers and program managers will be in a better position to make informed decisions at key acquisition decision events.

Contents

Abbreviations

ADE	Acquisition Decision Event
BD21	Biological Detection for the 21st Century
BTE	Biodetection Technology Enhancement program
CWMD	Countering Weapons of Mass Destruction office
DHS	Department of Homeland Security
DOD	Department of Defense
Gen-2	BioWatch Generation-2
Gen-3	BioWatch Generation-3
HSPD-21	Homeland Security Presidential Directive 21
JPEO	Joint Program Executive Office for Chemical, Biological, Radiological and Nuclear Defense
MRA	manufacturing readiness assessment
NBIC	National Biosurveillance Integration Center
PCR	polymerase chain reaction
TRA	technology readiness assessment

441 G St. N.W.
Washington, DC 20548

May 20, 2021

Congressional Requesters

Aerosolized biological agents may make attractive weapons for terrorists and other bad actors because these invisible, odorless, microscopic particles are difficult to detect.[1] Clandestine attacks using aerosolized biological agents could be carried out in urban areas, at sporting events, at transportation hubs, or at indoor facilities like office buildings. A terrorist attack using a biological weapon could lead to catastrophic consequences for our nation's population, agriculture, environment, and the economy. In December 2018, we reported on emerging threats facing the nation, among which were terrorism by violent extremist organizations using a biological weapon and using dual-use technology such as genetic engineering and synthetic biology, which could be used to develop new types of biological weapons.[2] Combatting the ever-changing nature and broad array of biological threats often entails developing new technologies and approaches and making decisions about how to apply limited resources to achieve the best benefit. One such approach being explored for biodetection technology is the use of artificial intelligence, specifically machine learning.[3]

In 2003, in response to the 2001 anthrax attack, the newly established Department of Homeland Security (DHS) started the BioWatch program—designed to provide early indication of an aerosolized biological weapon

[1]Aerosolized refers to the ability to disperse tiny particles or droplets suspended in air.

[2]GAO, *National Security: Long-Range Emerging Threats Facing the United States As Identified by Federal Agencies*, GAO-19-204SP (Washington, D.C.: Dec. 13, 2018). Dual Use Research of Concern (DURC) is life sciences research that can be reasonably anticipated to provide knowledge, methods, products, or technologies that could be directly misapplied to pose a significant threat with broad potential consequences to human, animal, and plant health, the environment, or national security. Genetically engineered agents are organisms that have been artificially modified to bypass traditional countermeasures or produce a more severe or enhanced disease. Synthetic biology is the engineering of biology: the synthesis of complex, biologically based (or inspired) systems, which display functions that do not exist in nature.

[3]Machine learning is a field of artificial intelligence in which software learns from data to perform a task. The field of artificial intelligence was founded on the idea that machines could be used to simulate human intelligence. According to Stuart J. Russell and Peter Norvig *Artificial Intelligence: A Modern Approach*, 3rd ed. (Hoboken, NJ: Pearson Education, Inc., 2010), artificial intelligence is defined as computers or machines that seek to act rationally, think rationally, act like a human, or think like a human.

attack.[4] Since the program's inception, DHS has pursued enhancements and replacements to the existing BioWatch system without success. These efforts were designed to further reduce the time to detection in order to limit morbidity and mortality from aerosolized biological attacks. DHS's current effort to replace BioWatch is called Biological Detection for the 21st Century (BD21). DHS describes this multi-year acquisition effort as a system-of-systems—an assembly of technologies to gain higher functionality—that will incorporate multiple technology components and use machine learning and data analytics to provide contextual information and indication that a biological attack may have occurred.[5]

Since 2012, we have done prior work assessing the BioWatch program and DHS efforts to upgrade or replace it.[6] As part of our work, we made a number of recommendations aimed at improving DHS's acquisition approach for identifying alternative technology approaches for BioWatch to help ensure that biosurveillance-related funding is directed to programs that can demonstrate their intended capabilities. We discuss those recommendations and DHS's efforts to address them in this report.

In light of DHS's past efforts and current approach, you have raised questions about the reliability of the existing BioWatch system, the approaches DHS is pursuing with BD21, and the adequacy of the science of biodetection technology. Specifically, you asked us to review DHS's efforts to follow acquisition requirements for BD21 and to assess the technical maturity of the technology under consideration. This report addresses (1) what BD21 is and the extent to which the BD21 program has followed DHS's acquisition policy, and (2) potential technical challenges to successful development of BD21, and the extent to which DHS has taken actions to mitigate risk in the acquisition.

[4]The Department of Homeland Security was established by the Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (codified as amended at 6 U.S.C. § 111). The BioWatch program aimed to reduce the time required to recognize and characterize potentially catastrophic aerosolized attacks by monitoring for the presence of certain biological agents considered to pose high risk for an aerosolized attack.

[5]A system-of-systems is a collection of technology elements that operate or function together within a larger system to create a new, more complex system, which offers more functionality and performance than simply the sum of the constituent technology elements.

[6]*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). *Biosurveillance: DHS Should Not Pursue BioWatch Upgrades or Enhancements Until System Capabilities Are Established,* GAO-16-99 (Washington, D.C.: Oct. 23, 2015).

To assess the nature, purpose, and proposed functionality of BD21 and the types of technologies under consideration for the system concept, we reviewed documents related to the need, and capabilities envisioned, for an enhanced biodetection system, including the BD21 Mission Need Statement, Capability Development Plan, and BD21 Alternatives Analysis. We also reviewed acquisition documents from prior biodetection programs leveraged to identify BD21 needs, such as the BioWatch Mission Need Statement, BioWatch Analysis of Alternatives, and the Biodetection Technology Enhancement (BTE) Alternatives Analysis. In addition, we reviewed the Fiscal Year 2020 Science and Technology Directorate and Countering Weapons of Mass Destruction office (CWMD) DHS Biosurveillance Systems Report to Congress, to identify changes to biodetection operations to improve upon the legacy program and how CWMD and Science & Technology Directorate coordinate their respective biodetection roles and activities. We also reviewed the document to characterize the status of developing and testing a successor bio-threat detection system, along with plans to complete development and field the new capability. We also reviewed strategic national priority documents, such as the National Biodefense Strategy and the Homeland Security Presidential Directive/HSPD-21 (HSPD-21), which CWMD is using to justify the BD21 acquisition.

To assess the extent to which the program has followed DHS's acquisition policy, we evaluated the BD21 program office's efforts against DHS policy and guidance governing the acquisition process. We reviewed BD21 specific acquisition documents completed to date, such as the 2019 Mission Need Statement and Capability Development Plan, BD21 Acquisition Review Board briefing slides, and BD21 Acquisition Decision Memorandums. We compared these documents to DHS policy documents valid at the beginning of our review and subsequent updates that occurred in January and February 2021. Specifically, we reviewed DHS Acquisition Management Directive 102-01 Revision 03.1 (February 25, 2019), and its associated instruction DHS Acquisition Management Instruction 102-01-001, Revision 01 (May 3, 2019), and the DHS Manual for the Operation of the Joint Requirements Integration and Management System 107-01-001-01 (April 21, 2016).[7] We also reviewed the DHS Systems Engineering Lifecycle Guidebook 102-01-103-01 (April 18,

[7]The DHS Acquisition Management Instruction was revised during the course of our review, and we reviewed the revised version of the instruction, Revision 01.3 (January 21, 2021).

2016); and its policy revision, DHS Systems Engineering Life Cycle Instruction 102-01-103 Revision 01 (February 4, 2021).

To understand the threats BD21 is designed to address, we reviewed an unclassified Threat Basis document (December 31, 2019) and received a classified briefing by program officials. To understand the BD21 program's engagement with stakeholders, we reviewed DHS summaries of several workshops they held with state and local stakeholders designed to describe the BD21 concept and solicit feedback on their proposed approach for BD21. Specifically, we reviewed the BD21 Workshop Summary Report from the DHS CWMD BD21 Workshop held in June 12, 2019, a summary of an October 2019 workshop with first responders, and a summary of a November 2019 workshop with public health officials. Each of these summaries highlighted concerns among stakeholders which we used to help generate questions for program officials on how the program planned to address concerns and mitigate risk in the acquisition.[8]

To assess the technical challenges to successful development of BD21, and the extent to which DHS has taken actions to mitigate risk in the acquisition, we analyzed the acquisition documents, analysis, and plans used to identify, assess, and characterize the technologies being considered. These documents included technology demonstration plans and reports, alternatives analysis reports, and technology readiness assessment policies, guidance, and plans. To determine the effectiveness of DHS's risk mitigation approach to conduct technology readiness assessments of its critical technologies, we compared DHS's technology readiness assessment (TRA)/manufacturing readiness assessment (MRA) guide and assessment tool against GAO's guide, Technology Readiness Assessment Guide: Best Practices for Evaluating the Readiness of Technology for Use in Acquisition Programs and Projects.[9] We assessed DHS's TRA/MRA guidance that decision makers would rely on when conducting TRAs against selected best practices from the GAO TRA guide. Because the BD21 program had not conducted any TRAs at the time of our review, we selected a subset of eight of the 29 best

[8]We did not independently assess the methodology of DHS's workshops or conduct direct outreach to stakeholders for this review, as these workshop summaries provided sufficient contextual information for the purposes of our review about DHS's acquisition activities at this stage in the acquisition.

[9]GAO, *Technology Readiness Assessment Guide: Best Practices for Evaluating the Readiness of Technology for Use in Acquisition Programs and Projects,* GAO-20-48G *(Washington, D.C.: Jan 7, 2020).*

practices identified in the GAO guide. We selected the eight best practices for our assessment because they applied to the TRA process and not to specific TRA reports. Specifically, we selected best practices based on the importance of having a process for ensuring repeatability and consistency in the process, thereby ensuring assessments are conducted appropriately. To determine the extent to which DHS's TRA/MRA guide follow best practices, one analyst reviewed DHS's guide and assessment tool to identify practices that met or partially met each of the eight best practices relevant to the TRA process identified in the GAO guide. For each best practice, the analyst reviewed the materials and coded the best practice as "Met," "Partially Met," or "Not Met" using the following criteria:

- met, if the best practice was clearly identified and the guidance provides instructions on how to apply or accomplish the practice,
- partially met, if the best practice was identified but instructions are vague or non-existent on how to apply or accomplish the practice, or
- not met, if the best practice was not identified.

A second analyst reviewed the coding of the first analyst and where there was disagreement, it was resolved through discussion.

We also supplemented our analysis with findings from our prior work related to BioWatch, the 2018 National Biodefense Strategy, and emerging national security threats to provide historical perspective and contextual sophistication. These works are cited throughout the report.

To address both objectives we also interviewed officials to better understand the current state of the acquisition, the maturity level of the technology under consideration, and the risk mitigation steps the program is taking to address challenges. We interviewed officials from the following: Department of Homeland Security's BD21 program office under the CWMD office; Program Accountability and Risk Management (PARM) office; Office of Strategy, Policy and Plans; Federal Protective Service; and Science and Technology Directorate. In addition, we met with the Department of Defense (DOD) Joint Program Executive Office for Chemical, Biological, Radiological and Nuclear Defense (JPEO), U.S. Army Combat Capabilities Development Command Chemical Biological Center. In addition, we interviewed officials from Johns Hopkins University Applied Physics Laboratory, and MIT Lincoln Laboratory.

We conducted this performance audit from January 2020 through May 2021 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.

Background

Biological Threats and the Challenges of Biodetection

Biological threats are vast and evolving and include threats of biological warfare, bioterrorism, infectious disease threats to humans and animals, crop failure, and safety and security lapses at facilities that house biological threat agents. The ongoing COVID-19 pandemic—which has sickened over 30 million people and killed over half a million in the United States alone—is an example of one naturally occurring biological threat our nation faces. We also face the threat of a bioterrorism attack, like the 2001 anthrax attack—in which 22 people contracted anthrax, of whom five died, from exposure to anthrax spores sent through the mail. This event brought new awareness of the threat posed by bioterrorism. The use of biological weapons or their proliferation by state or non-state actors presents a significant challenge to our national security. A number of nations continue to pursue biological weapons programs despite prohibitions, and terrorist groups have sought to acquire biological weapons.[10]

Additionally, the biotechnology revolution presents opportunities to advance the life sciences, yet that same technology in the wrong hands could be used to catastrophic effect. For example, synthetic biology may lead to advances in public health, such as the development of biosensors that can permanently reside in the body to detect and treat abnormalities such as cancer. However, synthetic biology could also be used to create

[10]Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction, Apr. 10, 1972, 26 U.S.T. 583, 1015 U.N.T.S. 163, (entered into force Mar. 26, 1975). Signatory nations agree to never "develop, produce, stockpile or otherwise acquire or retain (1) microbial or other biological agents or toxins whatever their origin or method of production, of types and in quantities that have no justification for prophylactic, protective or other peaceful purposes; (2) weapons equipment or means of delivery designated to use such agents or toxins for hostile purposes or in armed conflicts."

and combine agents for biological weapons, posing a significant threat.[11] Finally, non-state actors such as terrorist organizations, domestic militia groups, and "lone wolves" have both the interest and, in some cases, the limited capacity to develop biological weapons.[12] Responding to the ever-changing nature and broad array of biological threats often entails developing new technologies and approaches and making decisions about how to best apply limited resources to achieve the best benefit.

Assessing the threat of potential bio-aerosolized attacks involves establishing assumptions about possible adversaries, their capabilities to carry out an attack, and their preferences for types of attacks or targets. While an adversary may have the intent to identify possible targets, the likelihood of a successful attack hinges on the adversary's abilities. Developing a sophisticated biological weapon requires the ability to acquire an agent and the subject matter expertise to weaponize and mass produce it so as to cause infection. It also requires having the equipment and technologies necessary for proper handling and production that minimizes the risk of accidental exposure.

Programs aimed at detecting such attacks must consider the capabilities and limitations of the detection systems they are deploying to determine the extent to which current technology and information can address the threat. For example, issues affecting a system's successful detection include location of the attack (indoor or outdoor), size of the attack (amount of agent used), dispersal method (wet or dry agent), and ability to distinguish the agent from other organic or inorganic material that may be present in the air, such as pollen or brake dust. This information can then be combined to develop program requirements, including technical performance requirements—such as the system's sensitivity, specificity,

[11]GAO-19-204SP.

[12]According to a 2015 report of the Blue Ribbon Study Panel on Biodefense, U.S. domestic militia members have produced ricin (a biological toxin and chemical weapon) and sarin (a chemical weapon) on a larger scale than previously reported, demonstrating increasing capabilities. The report also identifies the threat posed by lone wolves, who are individuals who do not operate within the organizational constructs offered by militias, domestic violent extremist groups, or terrorist groups, and are thus more difficult to monitor. A lone wolf who obtains biological agents or weapons should be expected to use them with little hesitation. Additionally, U.S. citizens who sympathize with the Islamic State of Iraq and the Levant and likeminded groups may present an equal or even greater danger than terrorist groups. See, Blue Ribbon Study Panel on Biodefense, *A National Blueprint for Biodefense: Leadership and Major Reform Needed to Optimize Efforts* (Washington, D.C.: Hudson Institute, October 2015). As of September 17, 2019, the Blue Ribbon Study Panel is now the Bipartisan Commission on Biodefense.

and limit of detection—needed for a system to detect a potential attack.[13] This information also informs the concept of operations by focusing on what attack situations are possible and likely, and what methods or technologies would be most likely to detect a possible attack under a given set of conditions.

However, the evolving biological threat landscape creates unique challenges for biodetection capabilities, including the following:

- Variability. The variability of biological agents is vast by comparison to chemical, radiological, or nuclear agents, which have specific structures that can be used in designing a detection system. For example, a biological attack could stem from the use of viruses, bacteria, or toxins, each of which would need a specific assay—or test—to identify. Also, because biological agents exist in nature, it cannot always be quickly determined whether an attack has occurred or if it is part of the background environment. For example, in 2015 we reported on this challenge which prompted false positive alarms from BioWatch but were attributed to detections of a non-disease-causing relative, or near-neighbor, of a biological threat agent that occurs naturally in the environment.[14]
- Changeability. Biodetection can also be challenging due to the unpredictable nature of naturally occurring disease. For example, the genetic compositions of some viruses naturally change, as exemplified in 2009, when an H1N1 influenza virus emerged with a new combination of genes, causing a global pandemic. The ongoing COVID-19 pandemic also demonstrates how viruses naturally change, as new variants have emerged throughout the pandemic. Biological agents can also be modified by design, which presents challenges to biodetection because verifying such agents are in the environment requires specific detection capabilities for the specific structures that may be unknown to anyone but the attacker. Conversely, chemical agents have specific chemical structures—of which specific parts are the causative aspect that threatens human health—and generally cannot be changed. Developing detection

[13]Sensitivity refers to the probability of detecting the presence of a targeted agent. Specificity refers to ability to distinguish between agents of interest and other, genetically similar agents.

[14]GAO-16-99.

capabilities for biological threats that change can be more challenging than developing them for threats that do not.

- Traceability. The ability to attribute the source of a biological attack and quickly apprehend and prosecute the perpetrator is essential to our nation's safety. Attribution relies on many facets of an investigation—one of which is bioforensics.[15] Bioforensics capabilities may show how, when, and where microorganisms were grown and potential methods for dissemination, which would help attribute an attack to a source or a perpetrator.[16] In 2017, we reported that DHS and Federal Bureau of Investigation officials identified bioforensic gaps, such as the difficulties in interpreting metagenomics data, limited sequences for select organisms in its reference database, and the need for a greater ability to examine proteins—which we reported could be important in future investigations.[17] Because of the variability and changeability challenges noted above, biological agents are more difficult to trace because they do not have defined characteristics, like those that make tracing chemical agents more straightforward. Additionally, attribution can be difficult because biological agents exist naturally and can change naturally.

Understanding BioWatch and Its Limitations

In 2003, in an effort to provide early warning, detection, or recognition of a biological attack, the newly established DHS created the BioWatch program, but in 2015 we reported on limitations to understanding the system's capabilities.[18] Currently, the BioWatch program collaborates with more than 30 BioWatch jurisdictions throughout the nation to operate

[15]Microbial forensics characterizes, analyzes, and interprets microbial evidence for attribution purposes. The field has grown from the multidisciplinary fields of genomics, microbiology, and forensics, among others. Microbial forensics has also been referred to as "bioforensics" and "forensic microbiology."

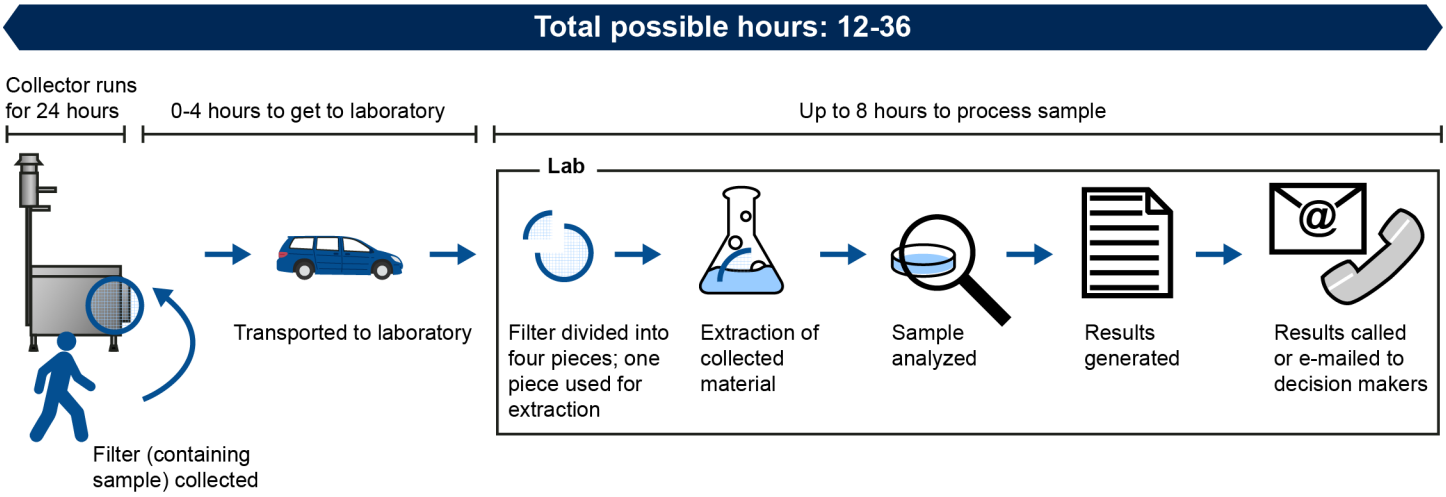
[16]According to one expert we contacted during our 2017 review, it would be difficult to determine a specific dissemination method from evidence left behind after biological weapons were aerosolized. Although it might be possible to differentiate between wet and dry dissemination and maybe gain some additional general information, determining the specific methods would be challenging.

[17]GAO, Bioforensics: DHS Needs to Conduct a Formal Capability Gap Analysis to Better Identify and Address Gaps, GAO-17-177 (Washington, D.C.: Jan 11, 2017); and GAO, Anthrax: Agency Approaches to Validation and Statistical Analyses Could Be Improved, GAO-15-80 (Washington, D.C.: Dec. 19, 2014).

[18]GAO-16-99. The BioWatch program monitors for six distinct biothreat agents, but two of these are closely related, although they cause different diseases, and the BioWatch program has treated them as a single agent.

approximately 600 aerosol collectors.[19] It is a federally managed, locally operated system with collectors deployed primarily in outdoor locations. The time to determine whether a public health threat exists based on information from the BioWatch program can take 12 to 36 hours after an agent is initially captured by the aerosol collection unit. This 36-hour timeline consists of up to 24 hours for air sampling, up to 4 hours for retrieving the sample from an aerosol collection unit and transporting it to the laboratory, and up to 8 hours for laboratory testing (see fig. 1).

Figure 1: How the Existing BioWatch Detection Program Works



Source: GAO analysis of Department of Homeland Security information, Sandia National Laboratories, and the National Academies. | GAO-21-292

In 2015, we reported that when DHS was established in 2002, a perceived urgency to deploy useful—even if immature—technologies in the face of potentially catastrophic consequences led to the rapid deployment of the initial BioWatch system which modified air monitoring technology used for other missions. According to a 2011 report from the National Academies, this rapid deployment meant that BioWatch was deployed without sufficient testing, validation, and evaluation of its

[19]BioWatch Generation-1 (Gen-1) deployed in 2003. The current system, Generation-2 (Gen-2), refers to the increased deployment of collectors to additional jurisdictions and increased indoor monitoring capability in 2005.

technical capabilities.[20] In 2015, we reported that DHS lacked reliable information about the current system's technical capabilities to detect a biological attack, in part because DHS had not developed technical performance requirements for the system.[21]

As a result, in our 2015 report, we made a recommendation 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 inform cost-benefit decisions about possible system upgrades. Specifically, we recommended that DHS not pursue upgrades or enhancements to the current BioWatch system until DHS: (1) establishes technical performance requirements necessary for a biodetection system to meet a clearly defined operational objective for the BioWatch program; (2) assesses the Gen-2 system against these performance requirements; and (3) 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 with the recommendation, but this recommendation remains open, and we will continue to monitor DHS's progress while it pursues a replacement for the current BioWatch system.

Additionally, our 2015 work on BioWatch evaluated DHS's efforts to test an autonomous detection system, known as BioWatch Gen-3, from 2010 through 2011 against GAO-identified 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 the current Gen-2 system. DHS concurred and stated that its updated acquisition guidance largely addresses these best practices. However, this recommendation also remains open, and we will continue to monitor DHS's progress while it pursues a replacement for the current BioWatch system.

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

[21]GAO-16-99.

DHS Efforts Intended to Upgrade or Replace BioWatch

Since 2003, DHS has considered other technologies either to enhance the existing detection method or to replace the current BioWatch technologies. However, DHS experienced challenges in these efforts for a variety of reasons.

In 2003, DHS began to develop an autonomous detection capability (Gen-3)—envisioned as a laboratory-in-a-box—that would automatically collect air samples, conduct analysis to detect the presence of biological threat 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.

In 2012, while the Gen-3 acquisition was ongoing, 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.[22] We also found that DHS did not evaluate a complete set of alternative solutions, consider complete information on cost and benefits, or include a cost-benefit analysis. This information would have been valuable in making trade-off decisions. 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, directed the BioWatch program to complete an updated Analysis of Alternatives.[23] In April 2014, DHS canceled the acquisition of Gen-3 because the analysis did not confirm an overwhelming benefit to justify the cost of a full technology switch.

Additionally, at the time of our 2015 report on the current BioWatch program, DHS was considering upgrades to the Gen-2 system. This effort, discussed in detail below, was known as the Biodetection Technology Enhancement program (BTE). It was envisioned as an incremental improvement using non-developmental technologies to

[22]GAO-12-810.

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

integrate into the existing BioWatch capability. In our 2015 report, we concluded that effective and cost-efficient decisions could not be made regarding upgrades and reinvestments to the existing BioWatch program if the operational capabilities of the Gen-2 system were uncertain. We recommended that before DHS took any efforts to improve the existing system, like BTE, the operational capabilities of the Gen-2 system would need to be assessed against technical performance requirements directly linked to an operational objective. We reported that taking this action would help ensure that decisions about future investments were actually addressing a capability gap not met by the current system and address a clear mission need. Although DHS agreed with our recommendation, it still moved forward with a technology demonstration of BTE and awarded a contract for an Alternatives Analysis assessment. As a result of the findings of these two activities, in 2018, DHS concluded that the present state of the art in technologies did not provide a cost-effective way forward for incremental improvement to the BioWatch system. DHS cancelled BTE in September 2018.

Biodetection Technologies Considered for BD21

Based on the 2018 Alternatives Analysis for BTE, DHS began a new biodetection technology acquisition program in 2019 called Biological Detection for the 21st Century (BD21). Rather than making an incremental improvement to existing BioWatch capabilities, DHS plans for BD21 to replace the BioWatch program. BD21 will use multiple technologies to accomplish its biodetection goals. Some of these technologies are currently used by the existing BioWatch program, such as collectors and polymerase chain reaction (PCR)-based laboratory testing[24]. BD21 will also incorporate other technologies, such as biological sensors, field screening devices, and anomaly detection tools. Figure 2 describes several technologies DHS is considering to work in concert for BD21's biodetection capability.

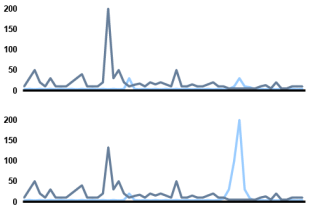
[24]Polymerase chain reaction (PCR) is a technique used to produce many copies of segments of DNA, the building block of genetic material. By targeting specific segments, PCR can be used as the basis for a test, or assay for the presence of genetic signatures associated with specific biological organisms.

Figure 2: Technologies the Department of Homeland Security (DHS) Is Considering for Biological Detection for the 21st Century (BD21) to Detect Aerosolized Biological Threats

Biological Sensor

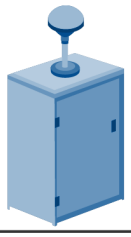
- Sensors continuously monitor air to provide real-time analysis of the environment.
- They can alarm if conditions indicate the possible presence of aerosolized biological particles of concern, and send an alert to an operator.
- They can be used in conjunction with air collection and field screening technology.

Data Analytics/ Anomaly Detection Tools



- Biological particles are present in almost all environments. Anomaly detection tools may use data analytics and machine learning to train an algorithm to differentiate background biological particles from possible threat agents.
- Algorithms are intended to detect anomalies or strong deviations from 'normal.' Machine learning builds a mathematical model from historical data to make decisions on new data.

Air Sample Collector

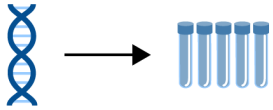


- Collectors draw air from the environment, and some are capable of adjustable collection times up to 24 hours.
- Collection can be initiated by a trigger if it senses a biological particle in the air.

Field Screening Device

- Field Screening Devices analyze samples at the collection site, in conjunction with collectors.
- They prescreen environmental samples in the field in order to prioritize laboratory analysis.
- They may be a single unit or two separate systems, one for screening and one to collect samples for laboratory analysis.

Laboratory testing



- Polymerase chain reaction (PCR) is a technique used to produce many copies of (or amplify) segments of DNA, the building block of genetic material. By targeting specific segments, PCR can be used as the basis for a test, or assay, for the presence of genetic signatures associated with specific biological organisms.
- Immunoassay-based testing is a technique used to detect the presence or quantity of a substance (such as a protein) based on its capacity to activate an immune response.

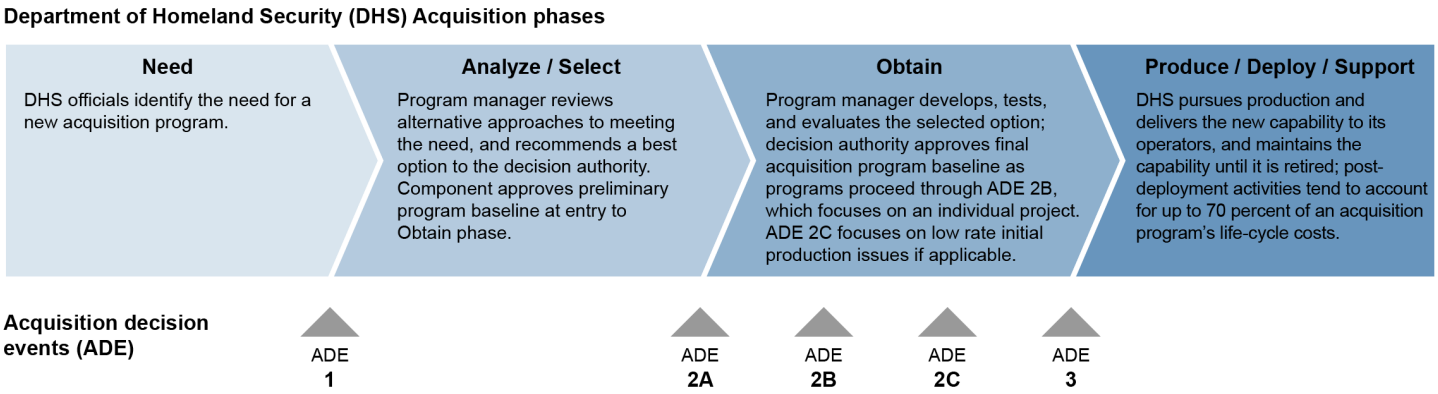
Source: GAO analysis of Department of Homeland Security information. | GAO-21-292

DHS Acquisition Process

To help manage its multi-billion dollar acquisition investments across its components, DHS has established policies and processes for requirements validation, acquisition management, and budgeting. The department uses these to monitor and guide delivery of the acquisition programs the components need to address critical capability gaps, enabling DHS to execute its missions and achieve its goals.[25] Within the components, program management offices are responsible for planning and executing individual programs within cost, schedule, and performance parameters, and preparing required acquisition program documents.

DHS's policies for managing its major acquisition programs are primarily set forth in its Acquisition Management Directive 102-01 and Acquisition Management Instruction 102-01-001.[26] These policies outline an acquisition life cycle that includes a series of predetermined milestones—known as acquisition decision events (ADE)—at which the acquisition decision authority reviews a program to assess whether it is ready to proceed to the next phase of the acquisition life cycle (see fig. 3 below).

Figure 3: Department of Homeland Security's (DHS) Acquisition Life Cycle for Major Acquisition Programs



Source: GAO analysis of Department of Homeland Security information. | GAO-21-292

[25]DHS generally defines a capability as the means to accomplish a mission or objective that may be achieved through materiel and non-materiel solutions.

[26]These documents are frequently revised, and the most recent version of the Acquisition Management Directive 102-01 was issued in February 2019, while the most recent Instruction Manual was issued in January 2021. DHS defines major acquisition programs as those with life-cycle cost estimates of $300 million or more. In some cases, DHS may define a program with a life-cycle cost estimate less than $300 million a major acquisition if it has significant strategic or policy implications for homeland security.

Changes at DHS and the National Biodefense Strategy

From 2007 to 2018, the BioWatch program was managed by DHS's Office of Health Affairs.[27] When the CWMD was established in December 2018, pursuant to the Countering Weapons of Mass Destruction Act of 2018, responsibility for BioWatch and other DHS biodefense activities were transferred to CWMD.[28] CWMD serves to elevate and focus the CWMD missions within DHS and to provide a focal point for the interagency. CWMD's objective is to support the President's National Security Strategy. CWMD leads the department's efforts to develop and enhance CWMD programs and capabilities that defend against weapons of mass destruction, and combat bio-threats and pandemics. CWMD works to protect against the dangers posed by hostile state and non-state actors who seek to acquire and use nuclear, chemical, radiological, or biological materials in the form of weapons of mass destruction to harm Americans or U.S. interests. CWMD's mission focus is to close gaps and reduce the risk of terrorism by detecting and disrupting WMD and the pathways to the United States. Further, CWMD leads the department's emerging infectious disease preparedness and response activities.[29]

The Countering Weapons of Mass Destruction Act also gave CWMD the responsibility for coordinating with other federal efforts and developing a strategy and policy for the Department to plan for, detect, and protect against the importation, possession, storage, transportation, development, or use of unauthorized chemical, biological, radiological, or nuclear materials, devices, or agents in the United States.[30] Prior to 2018, the Office of Strategy, Policy, and Plans was responsible for policy and priorities setting, but now the Secretary of Homeland Security relies on the CWMD for policy and priority matters for detection and prevention against biological weapons threats. These priorities are reflected in CWMD's annual budget submission. As such, the Office of Strategy,

[27]Prior to 2007, DHS's Science and Technology Directorate managed the BioWatch program.

[28]Countering Weapons of Mass Destruction Act of 2018, Pub. L. No. 115-387, 132 Stat. 5162 (codified as amended at 6 U.S.C. §§ 590 et seq. and note).

[29]Specifically, since December 2018, the role and responsibilities of the Department's Chief Medical Officer resides within the CWMD. This official serves as the principal advisor to DHS leadership on medical and public health issues related to natural disasters, acts of terrorism, and other man-made disasters. The Chief Medical Officer also provides operational medical support to DHS components and coordinates with federal and nonfederal stakeholders on medical and public health matters.

[30]6 U.S.C. § 591. The Assistant Secretary for the CWMD reports to the Secretary of Homeland Security.

Policy, and Plans does not normally play an independent role in prioritizing and implementing CWMD programs.

As part of its responsibility, CWMD has oversight responsibilities for some of its acquisition management to ensure sound management, review, support, and approval of all program types within the office. However, because BD21 is classified as a major Level 1 acquisition program—those with life-cycle cost estimates of $1 billion or more—the DHS Undersecretary for Management is the acquisition decision authority.[31] The DHS Undersecretary for Management is the senior acquisition officer for the department who exercises overall management, administration, and oversight of the department's acquisition policies and procedures. As such, the DHS Undersecretary for Management makes final acquisition decisions following Acquisition Review Board reviews at Acquisition Decision Events (ADEs).[32]

In September 2018, the White House issued the National Biodefense Strategy in an effort to promote a more efficient, coordinated, and accountable biodefense enterprise, and established a governance structure to guide the strategy's implementation.[33] In February 2020, we reported that the National Biodefense Strategy and its plans for implementation bring together the efforts of federal agencies with significant biodefense roles, responsibilities, and resources to address intentional, accidental, and naturally-occurring threats.[34] The National Biodefense Strategy and plans also provide processes for collecting and analyzing all the key elements of federal biodefense capabilities, which present an opportunity to identify gaps and facilitate enterprise-wide

[31]The senior component acquisition executive within the CWMD retains the authority and responsibility to oversee the acquisition process, including preparing the program for review.

[32]The Acquisition Review Board provides input and reviews programs for executable strategy on whether the program or concept can be accomplished or makes sense. The Acquisition Review Board also reviews funding and personnel resources, program and technical management, and alignment to strategic initiatives to provide input on whether the project should be done.

[33]The Strategy superseded Homeland Security Presidential Directive/HSPD-10 (HSPD–10), which called for a national bioawareness capability providing early warning, detection, or recognition of a biological weapon attack.

[34]GAO, *National Biodefense Strategy: Additional Efforts Would Enhance Likelihood of Effective Implementation,* GAO-20-273 (Washington, D.C.: Feb. 19, 2020).

decision-making and budget tradeoff decisions to help ensure the most efficient use of the nation's biodefense resources.

We reported that this is an important step toward the kind of enterprise-wide strategic decision-making we have called for in the past.[35] In June 2019, we testified that the National Biodefense Strategy and its interagency governing leadership offer the potential for the nation to better define the role of detection technologies in a layered, national biodefense capability to help those that pursue these technologies better articulate their mission needs and align requirements and concepts of operation accordingly.[36] For example, we have previously reported on the need to carefully weigh the costs and benefits of planned risk mitigation activities in the field of biodetection.[37] As a replacement to BioWatch, BD21's detection capability will narrowly address the threat of an aerosolized biological attack and does not cover the broader threat landscape. As part of the implementation of the National Biodefense Strategy, DHS and its interagency partners will have the opportunity to assess the role of and investment in biodetection of aerosolized attacks in a layered approach to mitigating risks of a variety of biological threats.

BD21 Envisioned To Enhance Early Biodetection, but Acquisition Documentation Is Limited and Lacks Detail

The BD21 program office plans to combine various technologies to enable timelier and more efficient detection of an aerosolized attack involving a biological agent, but has not yet selected the technologies to be used because the BD21 program is early in the acquisition lifecycle, and is still evaluating technologies. Given BD21 is in the early phase of the acquisition lifecycle, many of the key acquisition documents that are required to enter the next phase of the lifecycle are not finalized. Input from ongoing analysis, outreach, and demonstrations will be used to finalize the documents. However, existing BD21 program acquisition documentation lacks sufficient detail describing how a situational awareness and common operating picture capability—which DHS identified as a gap—will differ from or leverage an existing DHS capability, the National Biosurveillance Integration Center (NBIC).

[35]GAO, *Opportunities to Reduce Potential Duplication in Government Programs, Save Tax Dollars, and Enhance Revenue,* GAO-11-318SP (Washington, D.C.: Mar 1, 2011).

[36]GAO, *Biodefense: The Nation Faces Longstanding Challenges Related to Defending Against Biological Threats,* GAO-19-635T (Washington, D.C.: June 26, 2019).

[37]GAO-12-810.

The BD21 Concept Is a Collection of Technologies Intended to Improve Speed and Efficiency of Biodetection

The BD21 program office expects the BD21 system-of-systems concept will combine various technologies to enable timelier and more efficient detection of an aerosolized attack involving a biological agent than DHS's current biodetection system, BioWatch. BD21 is to consist of biological sensors, data analytics, anomaly detection tools, collectors, and field screening devices for use by first responders to improve the speed and efficiency of biodetection. DHS has not yet selected the technologies to be used, because the BD21 program is early in the acquisition lifecycle and still analyzing potential technologies to demonstrate that certain components of the overall concept are feasible. For example, the BD21 program office is conducting proof of concept test demonstrations of anomaly detection capabilities as part of this early acquisition phase.

Detection of biological agents is challenging due to the complexity of bioaerosol detection and the diverse scenarios, stakeholders, and end users for the proposed system. DHS's intention for BD21 is to address several capability gaps in its ability to perform its biodetection mission, which are identified in DHS's 2019 Biological Detection Mission Need Statement. DHS has been trying to address several of these capability gaps for years, including gaps in timeliness, coverage, and the ability to detect a wider range of biological agents. Table 1 describes the capability gaps DHS anticipates BD21 will address.

Table 1: Capability Gaps the Department of Homeland Security (DHS) Anticipates Biological Detection for the 21st Century (BD21) Will Address

Capability Gap	Description
Timeliness	Delivering near real time alerts and responses to minimize the attack area and/or number of exposures
Program standardization	Standardizing implementation and alignment of alert response procedures and activities across jurisdictions
Anomaly detection	Detecting known, new, and evolving biological threat agents
Environment coverage	Covering indoor, partially indoor, and outdoor locations
Geographic coverage	Increasing coverage in existing BioWatch jurisdictions and expanding into jurisdictions not covered by BioWatch
Incident parameters	Assessing characteristics such as time, place, and type of attack
Shared situational awareness	Integrating information across DHS components and nonfederal partners into a single, centralized repository to enable a common operating picture for response activities

Source: GAO presentation of Department of Homeland Security (DHS) information. | GAO-21-292

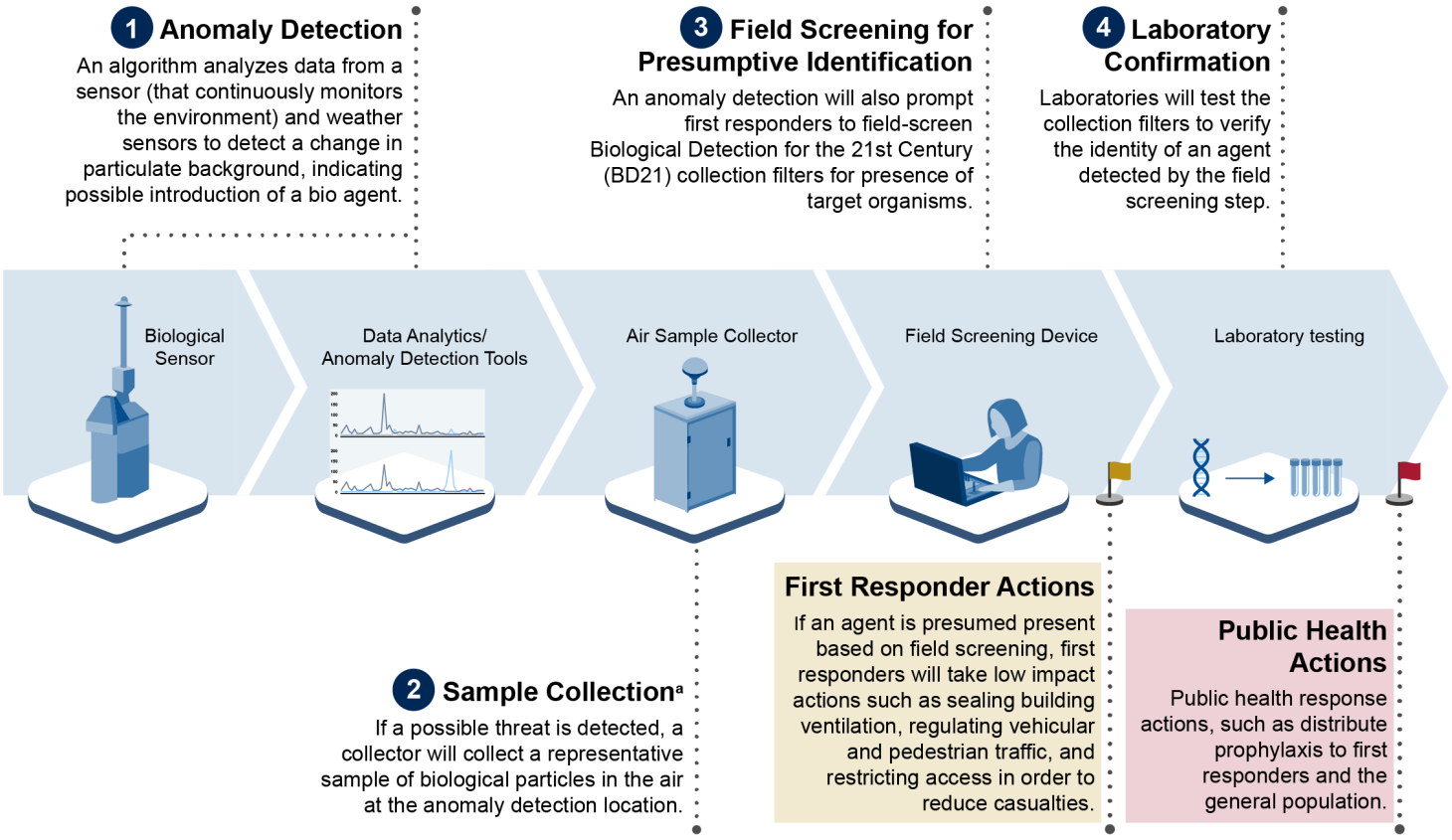
The BD21 program is intended eventually to work in both indoor and outdoor environments, but based on the results of recent analysis, DHS plans to pursue near-term solutions for indoor environments as part of an incremental acquisition approach that will include outdoor deployment in the future. Figure 4 shows the high-level concept of operations for BD21—the ideal end state of how these various technology components will work together to identify biological anomalies in the environment. Specifically, an anomaly detection algorithm is intended to use data from biological sensors that continuously monitor the air, as well as other data sources, to determine if there is a departure or deviation from the baseline environmental data, known as an anomaly.[38] If an anomaly exists in the environment, the system would produce a notification and activate the collector to collect a sample of material in the air onto a filter for subsequent analysis. The notification would signal for first responders to arrive on scene and use field screening devices to further characterize the air sample retrieved from the collector filter in order to inform immediate response actions if a biological threat agent is suspected. Finally, just as with BioWatch, samples from the collector would be taken to a laboratory for final verification. Like BioWatch, BD21 would be a federally managed, locally executed program and would primarily be used by state and local public health officials, emergency managers, and response personnel.

BD21 would also allow for low-consequence response actions upon initial detection by field screening devices—such as diverting air handing systems inside buildings or blocking people from entering a potential exposure site.[39] This is in contrast to BioWatch, which requires laboratory verification before any response actions are decided upon. In the ideal BD21 end-state design, field screening by first responders will only occur if a potential biological threat is detected by the anomaly detection algorithm. As such, BD21 is eventually intended to reduce the number of times filters are taken to the laboratory, thereby reducing costs.

[38]Baseline environmental data is the characterization of factors unique to each location or setting. Background environments vary by geography, climate, topography, and urban density, as well as by time of day, seasons, weather, animal population dynamics, farming patterns, construction, and manufacturing (emissions). Additionally, there are many naturally occurring bio-aerosols that can resemble a biological event in terms of aerosol profile, particle size range, or other characteristics.

[39]High consequence actions include distribution of prophylactic medications in response to the detection of an agent of high concern.

Figure 4: Department of Homeland Security's High-level Concept of Operations for the Ideal End State for Biological Detection for the 21st Century (BD21)



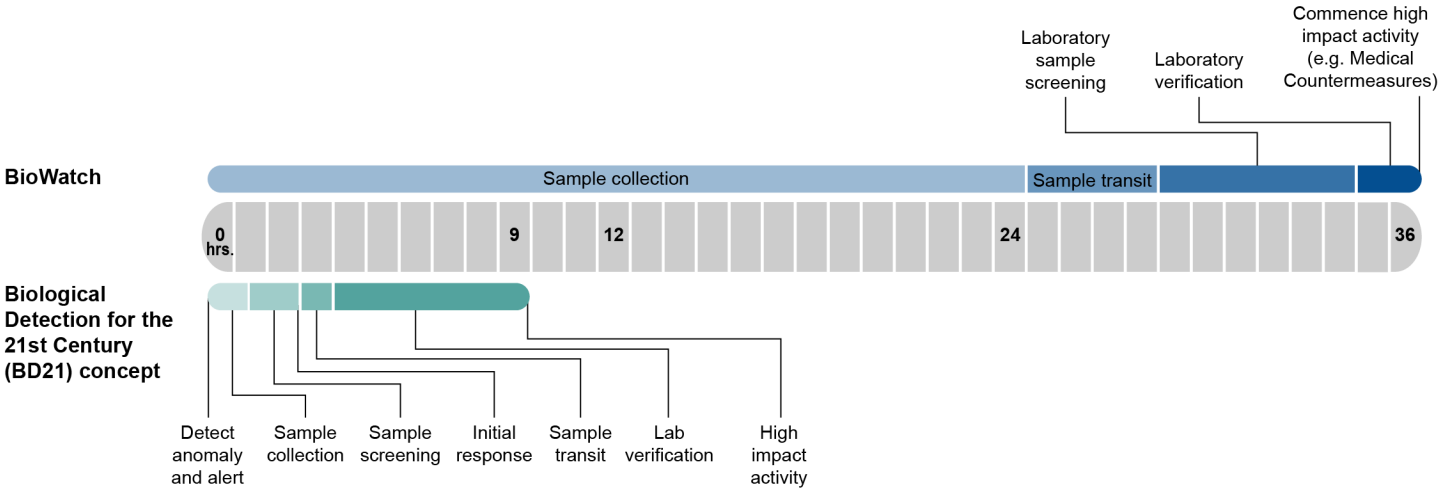
Source: GAO analysis of Department of Homeland Security information. | GAO-21-292

Note: [a]For the near term, the Biological Detection for the 21st Century (BD21) program office will use a continuous collection method to retrieve samples once per day from the collector. This is designed to help build confidence in the BD21 system as the anomaly detection capability matures.

However, for the near term, the BD21 acquisition approach will include daily scheduled retrieval of air samples continuously collected, similar to the current BioWatch sample retrieval protocol, which will not yield laboratory cost savings in this near-term approach. According to BD21 program officials, including this step as part of the near-term concept of operations will allow the program and stakeholders to assess the results of the anomaly detection capability alongside an established detection protocol. As the ability to identify biological anomalies improves and stakeholders gain confidence in the system, officials said BD21 will eventually only rely on the anomaly detection algorithm as part of the detection concept of operations.

In the long term, once the anomaly detection capability has matured, DHS aims to reduce detection time from BioWatch's 12 to 36 hours to BD21's anticipated 4 to 9 hours, thereby reducing the number of exposures, exposure levels, and the spread of a biological threat agent (see fig. 5). The largest reduction in time to determine whether a threat exists comes from the ability to detect anomalies, which would then prompt sample collection and field screening, rather than waiting up to 24 hours before a sample is collected and testing occurs. During 2019, the BD21 program office collected outdoor environmental background data from 12 jurisdictions throughout the United States to develop and test the first anomaly detection algorithm. It used additional outdoor data from a single location to test a second anomaly detection algorithm, and in November 2020, the program office began collecting indoor environmental data from two locations in the New York City metropolitan area to inform development of a third anomaly detection algorithm. More information on how the program is using these data appears later in the report.

Figure 5: Comparison of Detection Time Frames for BioWatch and Biological Detection for the 21st Century (BD21)



Source: GAO analysis of Department of Homeland Security information. | GAO-21-292

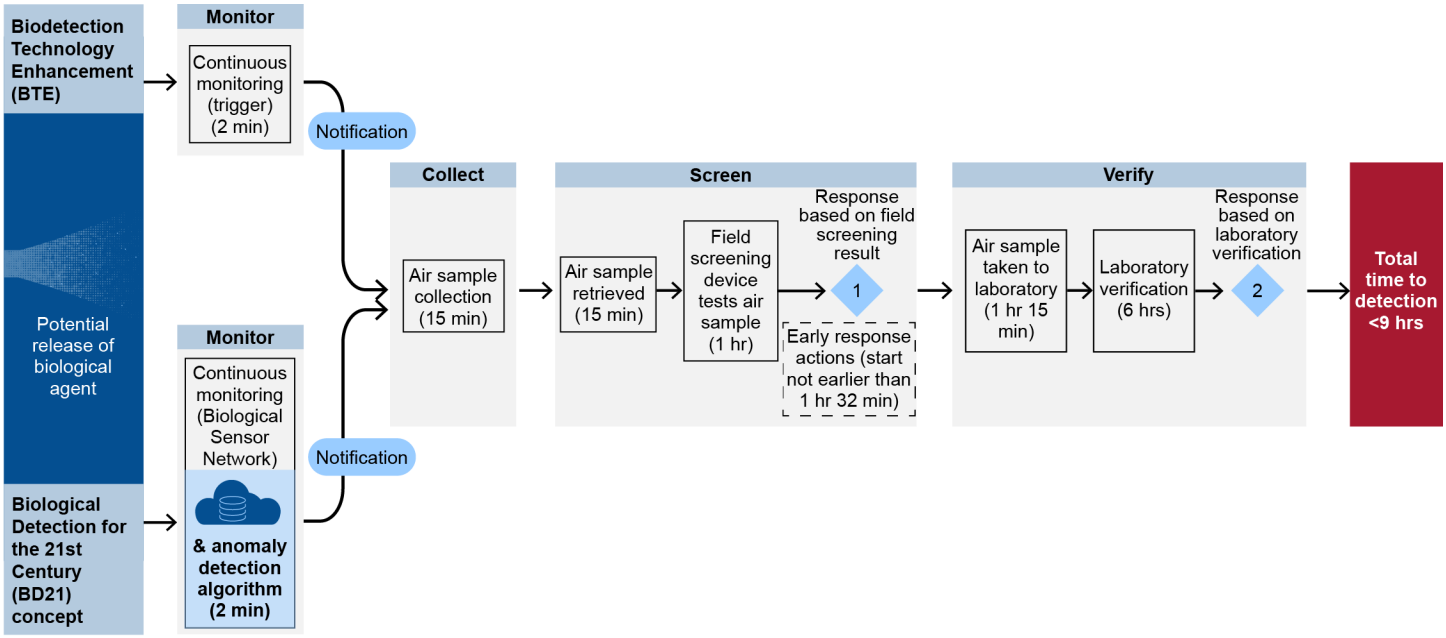
DHS is exploring the system-of-systems approach for BD21 as an iteration of a prior attempt to upgrade the existing BioWatch system, called BTE. The BTE approach used a triggering technology that would prompt a field screening response. However, due to cost considerations and the high false alarm rate of the trigger technology, DHS abandoned the BTE effort in September 2018. The BD21 concept builds on the BTE

design, adds an anomaly detection capability, and will include networked sensors.

There are key differences between the BTE and BD21 concepts. Specifically: (1) BD21 will use an anomaly detection algorithm in conjunction with biological sensors to reduce the signal-to-noise interference ratio inherent to the current trigger technology,[40] and (2) these biological sensors will be networked and have the ability to transmit signal data to a central location. DHS officials stated that as more data are collected from the air in the environment and fed to the anomaly detection algorithms, the algorithms, in theory, will adapt and begin to recognize and ignore typical, yet harmless natural airborne particles—such as pollen and dust. This training and adaptation of the algorithm will help distinguish harmless airborne particles from potentially harmful anomalies that might represent a threat and require an alert. Figure 6 depicts the key distinctions between BTE and BD21.

[40]According to BD21 program office officials, triggers will not be using their legacy (on-board) algorithms in the BD21 concept. Rather, the program will use these devices as biological sensors to monitor the air environment. Therefore, we refer to the trigger technology as sensors for the purposes of describing BD21.

Figure 6: Key Distinctions between Biodetection Technology Enhancement (BTE) and Biological Detection for the 21st Century (BD21) are the Anomaly Detection Algorithm and Networked Capability



Source: GAO analysis of Department of Homeland Security information. | GAO-21-292

DHS Developing Required Acquisition Documents

The BD21 program office is following guidance in the DHS Acquisition Lifecycle Framework, but because BD21 is in the early stages of the acquisition life cycle, the program office continues to develop key required acquisition documents. See figure 7 for a projected timeline for document completion and BD21 acquisition milestones. In order to exit the Need Phase and enter the Analyze/Select Phase, and to meet the documentation requirements in the DHS Acquisition Lifecycle Framework

for Acquisition Decision Event 1 (ADE 1), in June 2019, DHS approved the BD21 Mission Need Statement and Capability Development Plan.[41]

The 2019 BD21 Mission Need Statement updated the 2016 BioWatch Mission Need Statement, and identified the need for aerosolized biological anomaly detection across indoor and outdoor environments with near real-time alert of federal, state, and local first responders to provide early warning for response to address DHS's mission. The 2019 BD21 Capability Development Plan describes the activities and program resources required throughout the current Analyze/Select Phase of the BD21 acquisition to enable an informed Acquisition Decision Event 2A (ADE 2A) decision. In addition, it describes the top-level planning process the BD21 program is to follow to acquire a solution set that will address, or partially address, selected capability gaps identified in the Mission Need Statement.

The BD21 activities in the current Analyze/Select phase are focused on the analysis and selection of potential alternative solutions to address identified capability gaps. To analyze potential alternatives, the BD21 program office conducted an Alternatives Analysis and continues to engage in an assessment of technologies. The program office used the 2018 Alternatives Analysis from BTE as a starting point to identify potential solution types, because the focus for BD21 is to aggressively address the capability gaps that BTE could not address.[42] Specifically, the BTE Alternatives Analysis concluded that trigger technology alone—

[41]A Mission Need Statement identifies the capability gaps and functional capabilities required to accomplish DHS's mission and objectives, along with deficiencies and gaps in these capabilities. A Capability Development Plan defines how critical knowledge required to inform ADE 2 decisions will be obtained, and defines the objectives, activities, schedule, and resources for the analyze/select phase. In addition to these documents, an Acquisition Plan was required to be developed prior to ADE 1. However, DHS waived the requirement for an Acquisition Plan for BD21. DHS leadership subsequently issued a policy memo removing the requirement for programs to submit an Acquisition Plan to DHS headquarters for approval at acquisition decision events. This change was incorporated in DHS's current version of its Acquisition Management Instruction 102-01-001 Revision 01.3 (January 21, 2021).

[42]The Alternatives Analysis examines more detailed performance characteristics of various alternative ways to implement a preferred materiel solution, whereas an Analysis of Alternatives is generally used if the potential solutions encompass a wide spectrum of alternatives. When asked why an Analysis of Alternatives (which explores a broad range of solution options) was not performed, BD21 program officials said the 2013 BioWatch Analysis of Alternative results were still relevant at the time BTE and BD21 acquisitions began because no significant advancements had been made in the field of trigger technology.

absent networking, data analytics, and anomaly detection—was insufficient to provide cost-effective reductions in the identified capability gap areas. The BD21 program is focusing its analysis on existing commercial-off-the-shelf technology and technology created and used by government agencies to narrow analysis for a set of options to address this inherent limitation in trigger technology. Additionally, because no significant advancements have been made in that field, the program is focusing on ways to overcome limitations involving false alarm rates when looking at solutions for BD21, like using a combination of biological sensors and an anomaly detection algorithm.[43]

The BD21 program office describes the ongoing technology demonstration, which began in October 2018, as a proof of concept for BD21 designed to (1) collect outdoor and indoor environmental data to develop a detection algorithm; (2) evaluate the operational suitability of the technology in the environment; and (3) inform development of the concept of operations for the environmental detection of an aerosolized release of a biological agent. This stage of the acquisition also involves testing of technologies. According to BD21 program officials, the information and data obtained through the demonstration will support the development of requirements for an advanced biodetection capability and inform the BD21 acquisition approach (i.e., incremental approach).[44] The demonstration uses commercial-off-the-shelf technologies so the program office can identify capabilities available in the market. The program office will also leverage previous and ongoing DOD investments in biodetection. In addition, the program is benefiting from the CWMD Alliance, an interagency collaboration designed to identify common, compatible, and complimentary solutions.[45] Results from the technology demonstration will have an impact on decisions to either move forward with the acquisition of BD21 or spend more time maturing the algorithm in a research and development environment.

[43]While the technologies under consideration are sometimes called triggers because one of the functions of this technology can work as a triggering device, BD21 program officials said they are using the triggers as biological sensors.

[44]An incremental approach is commonly used by information technology programs where technologies are provided through a series of phases, which have their own key performance parameters that will be deployed and tested separately.

[45]The CWMD Alliance is made up of members from CWMD, the DHS Science & Technology Directorate, and DOD's JPEO.

Throughout the Analyze/Select phase, the BD21 program office will develop key acquisition documents, such as the Concept of Operations, Operational Requirements Document, and Test and Evaluation Master Plan, among others, before reaching ADE 2A—the point in the acquisition life cycle when DHS selects the best capability alternative to proceed into development.[46] According to program office officials, they will develop these documents, in part, using data and information collected in the Analyze/Select phase from the technology demonstration and input from local, state, and federal government stakeholders.[47] For example, the technology demonstration and Alternatives Analysis will inform the type of acquisition to develop, such as an incremental acquisition. In addition, officials said they are in the process of developing an Operational Requirements Document that will define the operational capabilities that are desired in the proposed solution, such as sensitivity, specificity, time to detect, and false positive and negative rates. Table 2 describes a selection of the types of documents required for ADE 2A.

Table 2: Selected Key Acquisition Documents required for Acquisition Decision Event (ADE) 2A

Document	Description
Operational Requirements Document	Captures the business or operational user requirements and identifies which of these requirements are key performance parameters. Describes the mission, objectives, and capabilities in operationally relevant terms.
Concept of Operations	Describes how different solutions could meet future challenges and correct current shortfalls in capabilities.
Life Cycle Cost Estimate	Provides an exhaustive and structured accounting of all resources and associated cost elements required to develop, produce, deploy, and sustain a particular program.
Integrated Master Schedule	Defines the oversight and management systems and tools used to monitor, oversee, and integrate cost, schedule, and technical performance goals, metrics, and resources.

[46]According to DHS acquisition policy, the decision to move into development is based on the capability meeting the required performance at acceptable cost, schedule, and risk.

[47]State and local stakeholders include law enforcement, first responder, public health, and public health laboratory officials. Federal participants include officials from DOD, Federal Bureau of Investigation, National Guard Bureau, Environmental Protection Agency, Department of Health and Human Services (HHS) Centers for Disease Control and Prevention, and HHS Assistant Secretary for Preparedness and Response.

Document	Description
Risk Management Plan	Details the processes to identify, analyze, mitigate, and report project risk. It clearly defines criteria used to define consequence and likelihood of occurrence.
Test and Evaluation Master Plan	Evaluates the overarching test and evaluation approach for the acquisition program. Describes the developmental and operational test and evaluation needed to determine a system's technical performance, operational effectiveness, suitability, and cyber resiliency.
Technology Assessment	Provides relevant information on the technical maturity, manufacturing capability, and technical risk of a planned technology.

Source: Department of Homeland Security (DHS). | GAO-21-292

Additionally, the program office is collaborating with end users, such as public health officials and first responders, to develop the concept of operations. For example, program office officials conducted several workshops to solicit initial input and distributed a survey to over 200 end user stakeholders to gather information on the types of environments they would like to protect, such as indoor versus outdoor locations.[48]

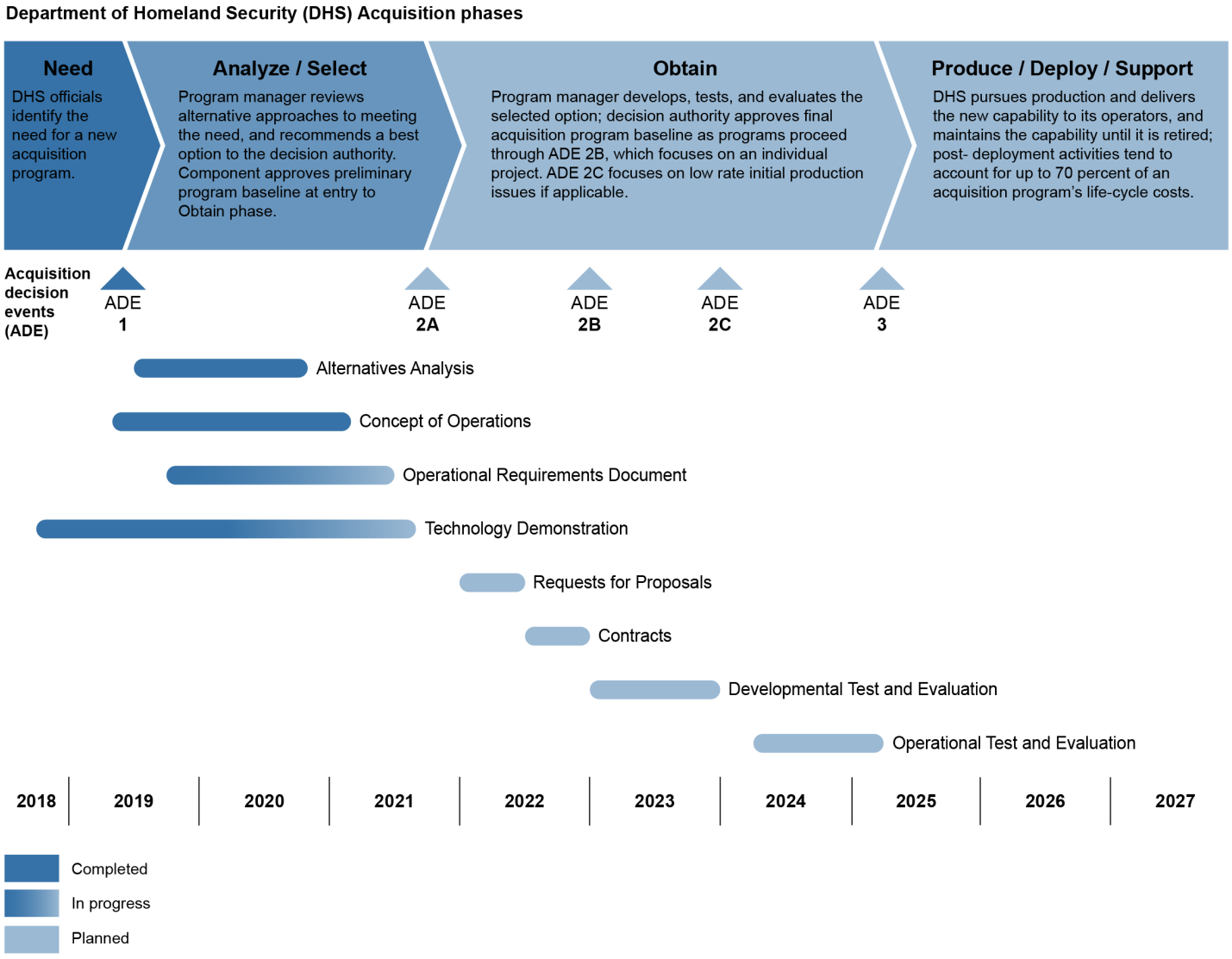
DHS recently rescheduled ADE 2A, the next major milestone event for the BD21 acquisition, from April 2021 to October 2021. Program office officials told us this change happened in an October 2020 Acquisition Review Board meeting, to allow more time to develop key acquisition documents, which had been delayed in part by COVID-19 response activities, and to assess results from the Alternatives Analysis, completed in November 2020. Due to DHS leadership interest in the success of BD21, Acquisition Review Board meetings will be held twice a year to review the BD21 program's status until ADE 2A approval. The proposed schedule for BD21 is aggressive, has been defined and refined throughout the Analyze/Select phase, and is being managed to proactively reduce risks, according to program officials. BD21 program officials maintain that the aggressive, proposed schedule is due to the number of years DHS has known about the capability gaps of the existing BioWatch system.[49] However, program officials said that if the program is unable to show at ADE 2A there is a realistic path to meeting the operational requirements, BD21 may not continue into system

[48]The program office is analyzing the results of the 2020 survey of stakeholders.

[49]In the absence of a new system, the officials stated that the existing BioWatch system can continue to be refreshed and maintained.

development. Additional detail beyond the ADE 2A decision point, should the acquisition move forward, is presented below. Figure 7 depicts the current status of BD21 in the DHS acquisition lifecycle and the program's proposed schedule of future work. The schedule may change because BD21 is in the early stages of the acquisition life cycle.

Figure 7: Current Status and Proposed Milestones of the Biological Detection for the 21st Century (BD21) Acquisition



Source: GAO analysis of Department of Homeland Security information. | GAO-21-292

Elements of the BD21 Acquisition May Overlap with an Existing Capability

The BD21 Mission Need Statement identifies a capability gap related to establishing shared situational awareness and a common operating picture that BD21 is intended to address, but it is not clear how this capability would be different from or how it may tie into or leverage DHS's NBIC, which is designed to provide a common operating picture for biosurveillance activity.

The BD21 Mission Need Statement, as required by DHS acquisition guidance, provides linkages to DHS strategic priorities and other biodefense-related doctrine to demonstrate how the capability will support broader homeland security goals and objectives. For example, the 2019 Mission Need Statement explains that the mission for Biological Detection is consistent with direction in HSPD-21, which called for the development of a near real-time biosurveillance capability.[50] As described in HSPD-21, this role includes developing a nationwide, robust, and integrated biosurveillance capability to provide early warning and ongoing characterization of disease outbreaks in near real time. The BD21 Mission Need Statement identifies a capability gap related to establishing shared situational awareness. It describes this needed capability as the ability to integrate surveillance activities and information across DHS components and other stakeholders into a single, centralized repository to enable a common operating picture. The Mission Need Statement explains that, if addressed, this capability would enable sharing of information, collaboration with partners, a common operating picture, and the communication of analytical and sampling results. It describes that these outcomes, in turn, would support an appropriate and timely response in order to contain the effects of an aerosolized biological incident.[51]

[50]The White House, "Public Health and Medical Preparedness," Homeland Security Presidential Directive/HSPD-21 (HSPD-21), October 18, 2007. HSPD-21 describes the federal government's role and goals in public health and medical preparedness and provides a detailed explanation of what a nationwide, robust, and integrated biosurveillance capability must include (e.g., epidemiological surveillance) and accomplish.

[51]Since 2003, DHS has wanted to add a networked communication capability in its upgrades or replacements to BioWatch. We understand that part of the BD21 concept is to be able to network individual collectors and automatically communicate results of an anomaly detection to local stakeholders and decision makers to prompt the field screening step. However, current BD21 program acquisition documents lack a detailed characterization of the broader situational awareness capability and common operating picture described as a capability gap.

The description of this capability is very similar to the description of NBIC's capabilities. NBIC's mission is to enable early warning and shared situational awareness of acute biological events and support better decisions through rapid identification, characterization, localization, and tracking. Specifically, the Implementing Recommendations of the 9/11 Commission Act of 2007 directed the Secretary of Homeland Security to establish, operate, and maintain NBIC to, among other things, enhance the capability of the federal government to rapidly identify, characterize, localize, and track a biological event of national concern and disseminate alerts and other information to member agencies and, in coordination with them to agencies of state, local, and tribal governments.[52]

Additionally, BD21 and NBIC officials characterized NBIC's situational awareness mission as much broader than that envisioned for BD21. Specifically, they said that NBIC provides early warning and ongoing situational awareness of biological events caused by biological, chemical, or radiologic agents affecting human, animals, and plants anywhere in the world with the potential to become nationally significant events through natural, accidental, or nefarious means. NBIC monitors population travel and trade, among other activities, through an integration of actionable information derived from a network of various highly-specialized programs and systems run by multiple government departments and agencies.[53] Conversely, NBIC and BD21 officials described BD21's planned situational awareness capability will be a more tactical, near real-time common operating picture for federal, state, and local stakeholders at the appropriate venues for each jurisdiction, to provide situational awareness and subject matter expert reach-back on those localized events. However, based on our analysis of existing BD21 program acquisition documents, including but not limited to the Mission Need Statement, this level of detail and clarification is yet to be documented. Therefore, it is not clear how the BD21 situational awareness capability is different from or how it may tie into or leverage NBIC's capabilities.

Public health and first responder stakeholders who will have responsibility for operating BD21 in their jurisdictions also expressed the need for greater clarity on the situational awareness function. Observations the

[52]Pub. L. No. 110-53 § 1101, 121 Stat. 266, 375-79 (2007) (codified as amended at 6 U.S.C. § 195b).

[53]Officials expect that as the BD21 program matures, a mechanism for the early exchange of actionable information indicating the need for consideration of a public health or similar response will be developed similar to NBIC's current participation in the BioWatch National Conference Call structure.

BD21 program office collected in 2019 from workshops with these stakeholders, which were designed to introduce the BD21 concept and solicit feedback, highlighted concerns from stakeholders about the situational awareness command center envisioned for BD21. Specifically, workshop participants were not clear whether the command center would exist at the federal level or if jurisdictions would have their own operations center. Nor were they clear on who would be involved in initial anomaly assessment or on how and in what format information would be disseminated to jurisdictions. DHS concluded after the 2019 workshops with stakeholders that the concept of operations in development may need to capture additional detail on the situational awareness capability.

DHS acquisition guidance for developing a Mission Need Statement requires an adequate description of any system currently performing the same or similar mission or function.[54] It also requires adequate discussion of any efforts to use existing systems or planned programs. According to the BD21 Mission Need Statement, the program office will leverage current and future DHS initiatives and activities to enhance efficiency and effectiveness. The statement and specifically identifies NBIC, among other efforts, but does not describe how this will be accomplished. In other words, it does not provide an adequate discussion on leveraging existing systems. According to officials from the DHS Office of Program Accountability and Risk Management—which, among other things, manages DHS-wide policy, governance, and oversight over DHS acquisition programs—the purpose of the Mission Need Statement is to describe a mission need for something to fill an existing capability gap, not describe how it will be filled.

Additionally, DHS acquisition guidance says the concept of operations document defines capabilities in greater detail than the Mission Need Statement and describes how a capability will fulfill the user requirements, its relationship to existing assets, systems, capabilities or procedures, and the ways it will be used in actual operations.[55] The concept of operations is also to communicate to stakeholders the operational tasks, processes, and associated roles and responsibilities of operators and allows stakeholders to visualize how the proposed solution operates in

[54]DHS Instruction Manual 107-01-001-01, DHS Manual for the Operation of the Joint Requirements Integration and Management System, April 21, 2016.

[55]DHS Instruction Manual 107-01-001-01, DHS Manual for the Operation of the Joint Requirements Integration and Management System, April 21, 2016; DHS Acquisition Management Instruction 102-01-001, Revision 01, May 3, 2019.

the real world operational environment and understand the associated organizational impacts.[56]

According to officials from the DHS Office of Program Accountability and Risk Management, having details articulated in the existing BD21 acquisition documents about how BD21 might leverage or connect with NBIC's situational awareness capability is a bit premature. According to BD21 program office officials, the early focus on the acquisition is to demonstrate the efficacy of the anomaly detection algorithm proof of concept.[57] However, they agreed that as they continue to develop the required acquisition documents, it will be important to clarify the situational awareness capability envisioned for BD21.

Because BD21, like BioWatch, will be locally operated by nonfederal stakeholders, it will be important to detail the specific functionality and sources of information of the planned situational awareness and common operating picture capability DHS envisions, so stakeholders have a better understanding of their responsibilities and what resources will be required of their jurisdiction to implement BD21. Additionally, we recognize that BD21 is early in the acquisition lifecycle and the program office continues to develop key acquisition documents. Because the documents have not been finalized there is an opportunity to provide adequate detail on how BD21 may be integrated with or leverage NBIC's situational awareness and common operating picture capabilities. Clarifying these issues would also help ensure that none of BD21's proposed capabilities result in unnecessary duplication that could lead to inefficiency or ineffective use of the department's resources.

[56]DHS Systems Engineering Lifecycle Guidebook 102-01-103-01 (April 18, 2016).

[57]These officials stated that if the program is unable to show a realistic path forward, it is not expected that BD21 will continue into system development.

DHS Does Not Follow Some of GAO's Best Practices and Past Lessons Could Help BD21 Address Technical Challenges

DHS's concept for BD21 faces technical challenges due to inherent limitations in the technologies and uncertainties associated with combining various technologies for use in biodetection. To mitigate the technological risks, the BD21 program is following the agency's acquisition policy and guidance, including analyzing solutions and conducting technology demonstrations of various biodetection components. DHS issued its technology readiness assessment (TRA) / manufacturing readiness assessment (MRA) guide in September 2020, but we found it did not follow some of the best practices in GAO's TRA best practice guide, such as ensuring objectivity and independence of the TRA team, among other important practices. Incorporating the best practices that we outline in GAO's TRA best practice guide could help further mitigate risk in acquisition programs throughout the agency. This is particularly important with BD21 because decision makers will rely on the information provided by TRAs to move into the next acquisition phase. In addition, our previous DHS biodetection reports provide opportunities for DHS to learn from past challenges and further address risk in the BD21 acquisition.

BD21 Faces Inherent Technical Challenges, Including Unproven Applications

This section describes the inherent limitations of individual technologies, as well as other technical challenges the program faces. Addressing these limitations is central to the acquisition's success going forward.

Trigger technology limitations. According to officials from the BD21 program office and DOD, the trigger technologies currently available are known to produce frequent false positives and false negatives. Trigger devices, also known as aerosol sensors, are used for monitoring the air to provide data on biological material in the environment. Commercial-off-the-shelf trigger devices come equipped with built-in (legacy) algorithms that are designed to distinguish the presence of aerosols containing biological material of interest from background material. When the trigger devices sense aerosols containing biological material, they trigger a response, such as alerting the collection device to collect air samples.[58] Fluorescence-based aerosol triggers have an established history of deployment as well as known limitations.[59] For example, DOD's JPEO is

[58]The current BioWatch system uses a collector for continuous collection of air onto a filter, which is retrieved every 24 hours for laboratory testing for the presence of biological agents.

[59]In fluorescence-based triggers, aerosols pass through an optical illumination region where they are excited by ultraviolet light. The light pulses that scatter off the aerosolized particles are measured and if the light falls within a specific wavelength band, the particles are fluorescent and considered a biological particle.

using triggers for its Integrated Early Warning, a concept of collecting threat data from disparate sensors and other data elements to provide a commander situational awareness and actionable information. However, common environmental material such as pollen, soil, and diesel exhaust can emit a fluorescence signal in the same range as a biological threat agent, thereby increasing false alarm rates.

DHS evaluated triggers under BTE, which was CWMD's effort to upgrade the BioWatch system. The high rates of false alarms caused by triggers contributed to the 2018 cancellation of BTE. According to officials from DOD's JPEO, Army's Chemical Biological Center, and BD21 program office, the trigger technologies have not matured and still have issues with false alarms.

Under the BD21 concept, the trigger technologies would not be used in their legacy function state to trigger an alert, but rather as biological sensors that provide information to the anomaly detection algorithm which then provides an alert in case of an anomaly. BD21 officials told us that the anomaly detection algorithm could minimize the system's false alarms by:

(1) combining disparate data sources into a single anomaly detection;

(2) using an anomaly detection algorithm to characterize normal aerosol behavior in the environment in order to better suppress trigger nuisance alarms resulting from background particles; and

(3) providing a rapid, consistent, and semi-autonomous way to initiate follow-up measurements of an aerosol anomaly.

According to a CWMD official, the current proof of concept for the BD21 anomaly detection algorithm includes combining data from different types of biological and weather sensors to produce a single anomaly detection. However, it is too early to determine whether integration of an anomaly detection algorithm with trigger technologies will successfully mitigate the false alarm rate. Officials from the BD21 program office stated that they intend to compare the false alarm rates of the trigger devices using the legacy algorithms with the same trigger (biological sensor) devices using the new anomaly detection algorithm prototypes in the same environment, a step we believe is needed to determine improvement of false alarm rates.

Anomaly detection algorithm limitations. The primary limitation of incorporating an anomaly detection algorithm is that these algorithms have never been developed or used before for the purpose of biodetection in an urban, civilian environment.[60] The anomaly detection algorithm is the only new technology component being incorporated into BD21 during this early proof of concept phase of the acquisition.[61] The other technologies under consideration for the BD21 concept are used for the current BioWatch program, were evaluated during the BTE acquisition, or will be developed and tested later, if the acquisition progresses. The success of the BD21 proof of concept test demonstrations therefore depends on the successful integration of the anomaly detection algorithm. This unprecedented use of such an algorithm provides technical challenges that BD21 would need to overcome.

The use of algorithms and machine learning as tools—currently under proof-of-concept development during the Analyze/Select phase of BD21—is to be delivered first as a single node (meaning the algorithm would process data from co-located sensors) and then as a multi-node version (meaning the algorithm would process data from sensors in multiple locations, allowing for a more accurate detection of an anomaly).

According to BD21 officials, the anomaly detection algorithms under consideration for BD21 are being developed through machine learning. The environmental background data being used for the BD21 proof-of-concept technology demonstrations were collected in 2019 at 12 outdoor jurisdictions across the country. Next, a data set was created with simulated threat release data injected onto environmental background data—supervised learning—collected in the earlier step.[62] All data sets (unsupervised and supervised) were then partitioned for training and testing of the algorithms and creating prototype candidate algorithms for further evaluation.

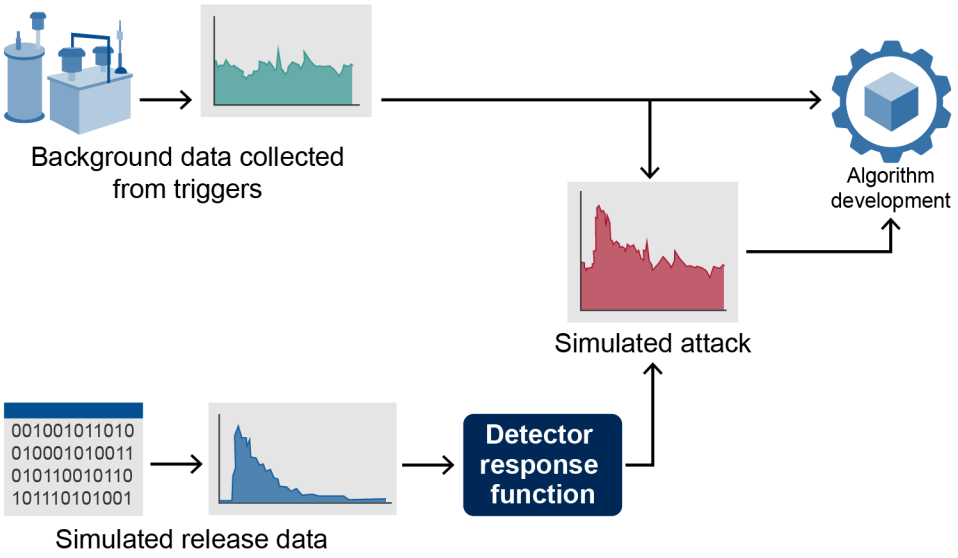
[60]According to DHS and DOD officials, DOD is developing a biological anomaly detection capability intended to support warfighter units. DOD has collaborated with BD21 program officials to share knowledge and information.

[61]The ability to network sensors and send notification will also be a new technology component, but DHS focused on the anomaly detection algorithm capability during the current phase of the acquisition.

[62]For BD21, supervised machine learning algorithms are provided data with labeled examples of background as well as labeled examples of background plus threat data. Unsupervised machine learning algorithms are provided unlabeled data.

According to CWMD, one of the reasons machine learning algorithms are of interest for BD21 is because they can adapt to different aerosol environments over time. Figure 8 shows how DHS is developing the anomaly detection algorithms.

Figure 8: How Department of Homeland Security (DHS) is Developing Biological Detection for the 21st Century (BD21) Anomaly Detection Algorithms



Source: GAO analysis of Department of Homeland Security information. | GAO-21-292

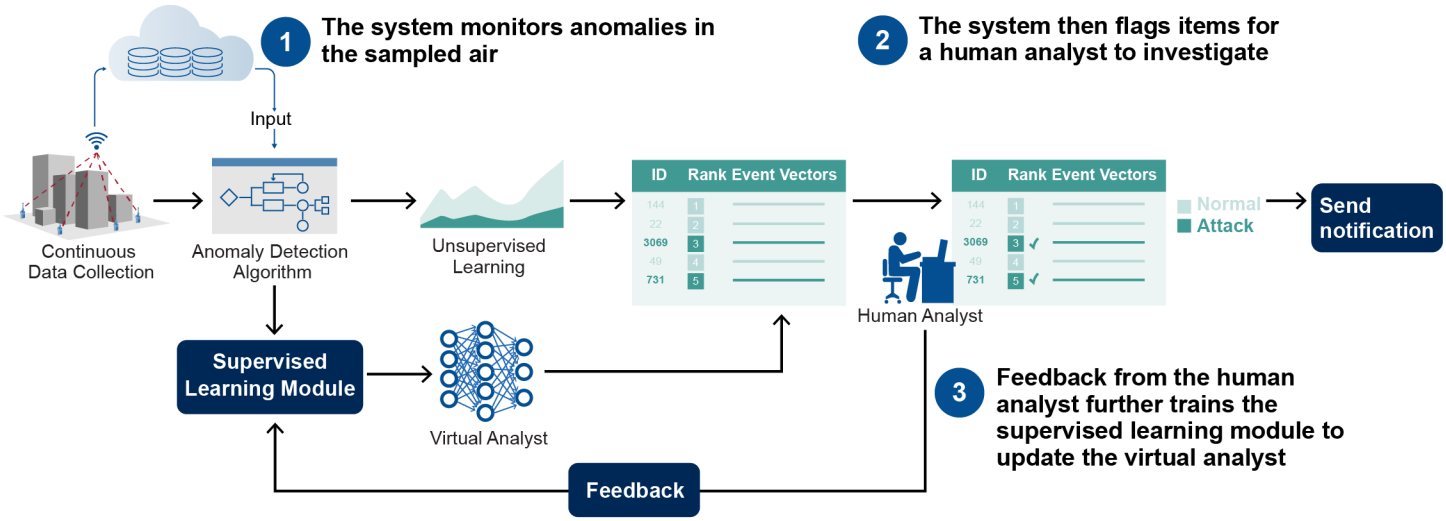
The BD21 Technical Maturity Roadmap designed by Johns Hopkins University Applied Physics Laboratory noted BD21 must demonstrate that the data provided by aerosol sensors are of sufficient quality and diversity for the anomaly detection algorithm to operate with a high level of performance in a wide range of operational environments.[63] This means that the BD21 program must sample the proper environments, design effective placement of sampling triggers, incorporate all relevant interferents—such as diesel fumes and dust particles—and factor in seasonal and climate changes such as pollen, temperature, and humidity when developing the anomaly detection algorithm.

[63]The Technical Maturity Roadmap developed by Johns Hopkins University Applied Physics Laboratory provides the BD21 program with criteria to demonstrate a level of maturity for the Critical Technical Elements expected to be components of the full system and result in readiness level determination for each to support the ADE 2A decision.

According to BD21 program office officials, the sensor technologies used to collect data for training the algorithms are known to produce false alarms. MIT Lincoln Laboratory officials said they prefer subject matter experts evaluate and analyze the sensor data rather than an automated algorithm process. Examples of excluded data are any data collected during equipment maintenance.

One critical and challenging step is accurate organizing and labeling of the large data sets being used to develop the machine learning algorithm. Without proper data organization and labeling, the machine learning tool becomes useless. To organize and label data, BD21 program officials said that sensor data collected will be sent to the DHS cloud, where they are GPS-tagged and timestamped. This step will ensure, for example, that environmental background data collected in one area will not be used to develop the final anomaly detection algorithm in a different operational environment. Figure 9 shows a conceptual model of the anomaly detection algorithm and how it would be used to detect, inform, and report biothreat agent anomalies to decision makers.

Figure 9: How Biological Detection for the 21st Century (BD21) Anomaly Detection Algorithms Are Used



Source: GAO analysis/implementation of Department of Homeland Security data; Adapted from video, Veeramachaneni, Arnaldo et al., *AI2: Training a Big Data Machine to Defend* (https://www.youtube.com/watch?v=b6Hf1O_vpwQ) and put into practice by PatternEx Inc. | GAO-21-292

Field screening device technology limitations. Field screening devices are intended to tentatively identify biological threat material in air samples captured by the collector following the anomaly detection. According to the BD21 preliminary concept of operations, the goal of using field

screening technologies is to shorten detection time and allow for low-consequence actions to be taken to reduce morbidity and mortality.[64] The technologies provided in the BD21 Technical Maturity Roadmap for field screening devices include PCR, nucleic acid sequencing, and immunoassay-based technologies.[65]

The limitations associated with field screening devices (regardless of the field screening technology chosen), stem from the complex sample preparation and analysis conducted in the field that may introduce environmental contaminants such as dust. According to CWMD officials, the sample background—which includes any material present in the environment at the time of screening—poses a major hurdle to field screening device technologies. The background data may be extremely dense, requiring sample clean-up techniques that are not easily conducted in the field without introducing further environmental contaminants. Officials also informed us that the performance (in terms of sensitivity, and specificity) of assays using field screening devices currently may not be comparable to that of their laboratory counterparts. Additionally, given the modifications needed to ensure sterility and portability of the assays, field screening devices add significantly more cost than using just their laboratory-based counterparts.

At the conclusion of the technology demonstrations for BTE, researchers at Johns Hopkins University Applied Physics Laboratory—the independent assessor—recommended that proceeding without a field screening device would be equally beneficial and more cost effective. They also reported that challenges associated with sample preparation and analysis in the field proved impractical, and that there would be little time savings because laboratory confirmatory testing would still be required for high consequence actions.

The BD21 program office's work to develop the concept of operations may further inform how, if at all, field screening will occur. For example, feedback the program office received from public health and first responder stakeholders indicated that there was concern that biological field screening was complicated and that the skill level of first responders

[64]The current BioWatch system relies on laboratory confirmation before certain response actions are taken by public health officials.

[65]Nucleic acid sequencing is the process of determining the sequence of the structural units within DNA - the building blocks of genetic material. Immunoassays are methods for detecting a substance by using an antibody reactive with it.

may impact the quality of the information (false negative and false positive rate). However, until the details of the concept of operations are finalized and the program office can demonstrate results through the technology demonstration, it is too early to determine the effectiveness of any risk mitigation activities the program office may take to overcome limitations of field screening devices.

PCR technology limitations. After presumptive identification of air samples using field screening devices, samples are transported to the laboratory for verification. The lab verification step for the BD21 concept is the same as the verification step for BioWatch. This step uses PCR technology that provides greater confidence by verifying the presence or absence of a biological threat agent. Even though PCR is the most mature technology available for laboratory verification, BD21 program officials recognize that it requires comprehensive biological signature data (from specific segments of genetic material) so the results can accurately report real-world environmental conditions. In other words, PCR laboratory testing requires knowledge of the genetic signature to be verified—such as influenza A or a biological threat agent.

PCR testing would not be able to identify threat agents for which assays (tests) have not been developed, or threat agents that have been altered such that they cannot be identified with existing assays. This may present limitations to realizing one of BD21's desired capabilities, which is to be able to detect new or evolving threats. The anomaly detection capability may be able to indicate the possible presence of a yet-to-be-identified aerosolized threat agent, but additional laboratory verification steps would be needed to determine the identity of the agent, and PCR technology would not be applicable to these scenarios.

There are also instances where the threat agent signatures are indistinguishable from closely related organisms (referred to as near neighbors) because they have the same target genetic elements, which can lead to false positives. We previously reported that this was also an issue for the BioWatch program.[66] Specifically, we reported in 2015 that all of the BioWatch results that prompted an initial response from 2003 through 2014 were associated with PCR assays for two biological threat agents. The majority were associated with the detections of a non-disease-causing relative, or near-neighbor, of one of the agents that occurs naturally in the environment. Program officials said that in the near

[66]GAO-16-99

term, BD21 will still aim to detect the biological threat agents that the current BioWatch system is designed to detect. Should the program decide to expand to additional agents, it will need to identify risk mitigation steps to overcome the limitations of PCR technology.

BD21 Officials Are Taking Steps to Mitigate Acquisition Risks, but DHS's TRA/MRA Guide Does Not Follow Some Best Practices

According to BD21 acquisition documentation, there are concerns over whether a reliable detection system is technologically mature enough to support near real-time detection and preliminary identification of aerosolized biological attacks. We identified three key risk mitigation steps that the BD21 program office is taking during the Analyze/Select phase to help determine critical technology readiness and resource requirements to meet the capabilities outlined and determine if advances in technology can provide significant cost and capability advantages over BioWatch. These steps include (1) a technology demonstration, (2) an alternatives analysis, and (3) technology readiness assessments (TRA).

Technology demonstration. BD21 program officials said technology demonstrations—an important element of the Analyze/Select phase—will help them identify, assess, and mitigate risks before the program commits significant resources to the acquisition effort. These technology demonstrations may help refine requirements and analyze and objectively select the preferred solution alternatives that can meet the approved mission need. For example, during the BTE effort, the results of the technology demonstration showed that adding trigger devices to existing BioWatch collectors would not provide a cost-effective solution based on the available technologies at that time. This allowed DHS to cancel the acquisition early in the life cycle.

As the BD21 program office prepares for the ADE 2A decision (an acquisition decision when DHS approves the best capability alternative to enter the Obtain Phase), program officials report they are conducting a myriad of activities to analyze various solutions for BD21. During the technology demonstration, the BD21 program office will collect information to aid development of the anomaly detection algorithm, evaluate anomaly detection sensors, and inform the development of the concept of operations or how the technologies will be deployed by the jurisdictions. Factors explored during this demonstration include the technology's limits of detection, suitability for specific environments, and information learned from previous studies. As part of the technology demonstration, the program will also be learning the value of trigger devices, which stakeholders have raised concerns about implementing as part of the BD21 preliminary concept of operations.

According to program officials, the first phase of the technology demonstration took place outdoors in 12 jurisdictions across the United States to gather representative background data with which to train the anomaly detection algorithm. Because aerosol particle composition and background levels in indoor environments can differ considerably compared to outdoor environments, future demonstration events will include indoor background characterization to support the development of additional anomaly detection algorithms. Program officials reported the data collected in indoor and outdoor environments will also be used to inform the development and execution of chamber tests to determine if the anomaly detection algorithm can successfully distinguish threat agents from the anticipated background environment. These technology demonstration activities will also help the BD21 program office set expectations for the technology readiness of the critical technology elements required for the next stages of the acquisition.

Alternatives analysis. The BD21 program office commissioned an alternatives analysis to address: 1) what are the alternative anomaly detection capabilities for the detection of airborne biological threat agents in indoor and outdoor environments; and 2) what are the benefits and drawbacks of each alternative capability? As one of several risk mitigation tools, the alternatives analysis is also designed to help the program office identify the metrics for determining technological performance characteristics. As part of the acquisition process, the alternatives analysis was conducted to inform the upcoming acquisition decision event.[67]

A draft report completed in November 2020 stated that the BD21 alternatives analysis solution alternatives and excursions were evaluated to determine their probability of detecting an attack, and Detection-Adjusted Casualties and their false positive rate.[68] The Institute for Defense Analysis study team found that all of the alternatives and excursions have a positive return on investment.[69] The Institute for Defense Analysis study team said that the choice of a preferred

[67]Alternatives constitute the technologies and activities in various combinations and arrangements that are considered in the BD21 alternatives analysis. Excursions are variations within the alternatives, such as continuous collection or collection upon alert.

[68]Detection Adjusted Casualties is the estimate of the expected number of casualties as a function of how many casualties might occur given detection by an alternative versus detection by clinical diagnosis/diagnostics.

[69]We did not independently evaluate the evidence assessed by the DHS contractor, as it was outside the scope of this review.

alternative or excursion depends on tradeoffs among performance characteristics, such as its probability of detecting an attack, as well as the cost and feasibility of the concept of operations. Findings from this analysis include:

- Operational effectiveness. The probability of detection for triggered collection improves with an increased number of deployed anomaly detection units and additional units also increase sensitivity of the anomaly detection individual technologies. Options that involve a triggered alert with continuous collection are comparable to BioWatch (the baseline alternative) in their detection probability in all operational environments. The Institute for Defense Analysis study team said that if a biodetection system is desired outdoors, the system must include continuous collection to achieve a comparable probability of detection to BioWatch. Overall, the study team reported that there is a risk that foreseeable false alert rates would make triggered collection unacceptable to local jurisdictions due to cost and resource requirements.
- Casualties and casualties avoided. The Institute for Defense Analysis said that due to their high probability of detecting, high availability, and possibility of fast response associated with collection triggered by an anomaly detection alert, the options that used a triggered alert with continuous collection always showed the lowest expected casualties. The study team reported that triggered collection options, when deployed outdoors, showed the highest expected casualties due to their low probability of detecting harmful biological agents. On the other hand, deploying triggered collection options indoors may have lower expected casualties than BioWatch because larger attacks that can cause more casualties are easier to detect.

The Institute for Defense Analysis study team reported that all of the results from the alternatives analysis are contingent on the successful development and deployment of the anomaly detection algorithm, which currently exists only as a limited proof-of-concept prototype. Alternatives will also rely on the proposed BD21 network connecting monitors and collectors to a central Command Center, but plans to test these capabilities have not been developed.

Based on the results of these findings, the BD21 program office concluded in November 2020 that pursuing solutions first in indoor environments would have the best chance of closing identified capability gaps and meeting operational requirements in the near-term. The program decided to pursue an incremental acquisition approach to find an

indoor solution using the anomaly detection capability along with continuous collection, and has requested approval of this recommended approach. Program officials also noted that the continuous collection method is likely to help build confidence in the system.

Technology readiness assessments. TRAs are conducted to assess the technical maturity of potential solutions, commonly referred to as critical technologies.[70] The BD21 program office plans to initiate two TRAs to determine whether critical technologies under consideration for the acquisition are appropriately maturing. They will conduct these TRAs at the following phases of development:

- Analyze/Select Phase. The first TRA is an initial assessment planned for the third quarter of 2021 to support the upcoming ADE 2A decision in October 2021.[71] It will be used to ensure that only viable critical technologies can move to the next acquisition phase, such as those technologies determined to be relatively mature or those that demonstrate a clear path to maturity within the schedule and cost constraints of the program.
- Obtain Phase. The second TRA is planned for after DHS moves BD21 into the Obtain Phase, should it decide to do so. This comprehensive TRA is expected to examine each individual critical technology element and report on the maturity level based on an evaluation of the supporting documentation by an independent TRA team. At a minimum, TRAs are initiated by the program office in support of a preliminary design review or critical design review, and again before a

[70]The TRA frequently uses a maturity scale—based on technology readiness levels (TRLs)—that is ordered according to the characteristics of the demonstration or testing environment under which a given technology was tested at defined points in time. The scale consists of nine levels, each one requiring the technology to be demonstrated in incrementally higher levels of fidelity in terms of its form, the level of integration with other parts of the system, and its operating environment until the final level where the actual operation of the technology is in its final form and proven through successful mission operations.

[71]A more formal TRA is performed at the end of the analysis of alternatives/alternative analysis in support of the system engineering review and Acquisition Decision Event (ADE) 2A. TRAs are closely coupled and interdependent with the analysis of alternatives/alternatives analysis and the requirements and concept of operations refinement activities. Together, these interdependent activities form the basis for evaluating the technologies enabling the possible materiel solutions against the capability gaps defined in the mission need statement and capability development plan.

low rate initial production decision for the ADE 2C decision point. A final TRA may be conducted just before the ADE 3 decision point.

DHS's Systems Engineering Life Cycle Guidebook 102-01-103-01 (April 18, 2016) specifies that critical technology elements must be assessed on their maturity to help manage risk, as well as to provide governance authorities the information they need to manage program risks.[72] Although DHS had not conducted TRAs at the time of our review, BD21 officials stated that the department will do so in accordance with the TRA/MRA guide issued by DHS's Office of Science and Engineering in September 2020. DHS issued the TRA/MRA guide to facilitate assessments of critical technologies and to help mitigate risk during an acquisition.

We analyzed DHS's TRA/MRA guide and assessment tool by comparing them against eight selected best practices from GAO's TRA best practices guide. Table 3 shows our analysis on the extent that DHS's TRA/MRA guide followed the eight best practices from GAO's TRA best practices guide.

Table 3: Extent to which Department of Homeland Security's (DHS) Technology Readiness Assessment (TRA)/Manufacturing Readiness Assessment (MRA) Guide Aligns with GAO's TRA Best Practices Guide

Selected GAO Best Practices	Extent that DHS's TRA/MRA Guide met the best practice?	GAO analysis
1. The TRA considers the newness or novelty of technologies and how they plan to be used for selecting critical technologies (CT).	Met	The definition in the DHS TRA/MRA guide includes the newness or novelty of technologies.
2. The TRA considers the operational performance environment and potential cost and schedule drivers as basis for selecting CTs.	Partially met	The definition in the DHS TRA/MRA guide includes the operational performance environment, but does not identify potential cost and schedule drivers as basis for selecting CTs.
3. The TRA considers the relevant environment as basis for selecting CTs.	Met	The DHS TRA/MRA guide defines a relevant environment as basis for selecting CTs.
4. The TRA considers the potential adverse interaction with other systems as basis for selecting CTs.	Partially met	The DHS TRA/MRA guide defines the interaction with other systems, but it does not include "adverse interaction" as basis for selecting CTs.
5. Is conducted by an independent and objective TRA team.	Not met	The DHS TRA/MRA guide does not discuss how to ensure TRA team is independent and objective.

[72]At the time we conducted our analysis, the DHS Systems Engineering Life Cycle Guidebook 102-01-103-01 (April 18, 2016) was the most recent version of that document. DHS recently updated this document. See DHS Systems Engineering Lifecycle Instruction 102-01-103 Revision 01 (February 4, 2021).

Selected GAO Best Practices	Extent that DHS's TRA/MRA Guide met the best practice?	GAO analysis
6. Confirms the CTs based on more specific questions and requirements.	Met	The DHS TRA/MRA guide includes specific questions and requirements as basis for confirming CTs.
7. Follows a reliable, disciplined, and repeatable process to select CTs.	Met	The DHS TRA/MRA guide provides a detailed process, steps, and framework to ensure the TRA process is reliable, disciplined, or repeatable.
8. Has a documented policy or guide for preparing the plan. The refined best practice specifies that a plan should be prepared and include other elements of a plan, such as the purpose, resources, schedule, how dissenting views should be handled, and independence agreements.	Partially met	The DHS TRA/MRA guide says a plan should be prepared and includes some of the elements of a plan (i.e. purpose, resources, and schedule) but it does not specify how dissenting views should be handled, or require independence agreements.

Source: GAO analysis of Department of Homeland Security's (DHS) Technology Readiness Assessment (TRA) / Manufacturing Readiness Assessment Guide (MRA). | GAO-21-292

As indicated, we found that DHS's TRA/MRA guide met four of GAO's TRA best practices, partially met three best practices, and did not meet one best practice. Specifically, and to its credit, DHS's TRA/MRA best practices guide met the GAO TRA best practices that dealt with consideration of the newness or novelty of technologies, consideration of the relevant environment as basis for selecting critical technologies, specific questions to confirm critical technologies, and follows a reliable, disciplined and repeatable process to select critical technologies.

Of the three partially met best practices, we found that one best practice included the operational performance environment in DHS's TRA/MRA guide, but it did not include potential cost and schedule drivers in its definition. Another best practice was defined in DHS's guide on the interaction with other systems as basis for selecting critical technologies, but it did not specify adverse interaction for identifying critical technology elements. Finally, another best practice was identified in terms of the required elements for preparing a plan, such as the purpose, resources and schedule, but it did not specify how dissenting views would be handled, or specify the need for independence agreements.

For the one best practice assessed as not met, we found that DHS's TRA/MRA guide does not discuss how it will ensure the TRA team is independent and objective.

We recognize DHS's TRA/MRA guide is relatively new and that GAO's TRA best practices guide was recently issued in January 2020. To its credit, DHS has included some of the best practices and other elements from GAO's TRA best practices guide, such as the four high-quality

characteristics for conducting a TRA, and description of formal and knowledge-building TRAs. We believe DHS has an opportunity to strengthen its TRA/MRA guide by incorporating all best practices from our GAO Technology Readiness Assessment Guide: Best Practices for Evaluating the Readiness of Technology for Use in Acquisition Programs and Projects.[73] For example, having a comprehensive guide that includes the best practices in GAO's TRA guide for conducting TRAs will better position DHS decision makers (program managers and governance bodies) to gather important information for making technical and resource allocation decisions that the TRAs provide. This information includes whether a technology is sufficiently mature to move past a decision point to the next acquisition phase, needs additional work, or should be discontinued or reconsidered in favor of more promising technology. In addition, GAO's TRA best practice guide identifies best practices that could augment steps in DHS's process, along with best practices for each step that could help ensure that decision makers have credible, objective, reliable, and useful information. If DHS incorporates all the best practices outlined in GAO's TRA best practice guide into its TRA/MRA guide, the refined best practices could ensure acquisition projects have the best practices for conducting high-quality TRAs, thereby improving the credibility, objectivity, reliability, and usefulness of the information used to make important decisions.

Standards for Internal Control in the Federal Government state that management should use quality information to achieve the entity's objectives.[74] This can be an iterative process by which management uses the entity's objectives and related risks to identify the information requirements needed to achieve the objectives and address the risks. In the context of BD21, the TRA process can help program managers and other stakeholders, including DHS management, understand the maturity of various technology components to help manage risk. As the acquisition and testing progress, and as technology components are combined to create a larger system, the TRAs will continue to help inform risk mitigation decisions.

According to DHS's system engineering guidebook, conducting TRAs before an ADE is one of several important decisions to determine if a program is ready to move into the next acquisition phase. For the BD21

[73]GAO-20-48G.

[74]GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G, (Washington, D.C.: Sep. 10, 2014).

program, conducting TRAs that align with GAO's TRA best practices guide will be important at these events, such as ADE 2B because the program will need to ensure they have credible information about the maturity and readiness of critical technologies, and to ensure there are sufficient resources to execute the program. As the BD21 program moves forward in exploring development of a first-of-its-kind capability in biodetection, conducting TRAs that follow GAO's TRA best practices guide will be important in providing insightful information about the anomaly detection algorithm's technical maturity, particularly as it progresses toward the ADE 2A decision currently scheduled for October 2021. This is essential because of the anomaly detection algorithm's importance to the overall function of the biodetection system and its low maturity, which poses a risk to the overall acquisition, according to a 2020 report by the Institute for Defense Analysis.[75] Officials from DOD's JPEO reported that developing such an algorithm for biodetection is in the very early stages of exploration and it could take years before the capability can be developed.[76] BD21 program officials agreed with that timeframe assessment and said they are in a long research and development effort to get the algorithms correct before moving too far in the acquisition process.

We believe that if the BD21 program conducts high-quality TRAs in accordance with GAO's TRA best practice guide of the critical technologies before ADE 2A decision and subsequent ADE 2B decision (including a TRA of the overall system level interaction with the anomaly detection algorithm), it would be particularly beneficial for the program because of the unprecedented inclusion of the anomaly detection algorithm with limited demonstrated maturity.

Addressing Our Prior Recommendations May Also Help Mitigate Risk in the BD21 Acquisition

Because the BD21 acquisition effort is in an early stage, it is yet to be determined the extent to which the program office will fully leverage lessons learned from prior efforts to replace BioWatch. Our prior work evaluating BioWatch Gen-2 and Gen-3 provide lessons to inform the BD21 acquisition, and DHS agreed to implement our prior recommendations. Specifically, our work identified issues related to requirements development, stakeholder involvement, testing, cybersecurity, and accounting for uncertainty. DHS has made progress in

[75]Institute for Defense Analysis, Biological Detection for the 21st Century (BD21) Alternatives Analysis (AA), Volume 1 (IDA Document NS P-14377) November 2020.

[76]DOD is also working on developing an algorithm for a military biodetection capability and has been collaborating with DHS.

some of these areas but has not fully addressed our prior recommendations, as described below. According to BD21 program officials, the steps they are taking during the BD21 acquisition are designed to address the recommendations, but their work is ongoing.

Requirements development. Our 2012 and 2015 reports on BioWatch described how DHS either did not set technical requirements or set requirements that were too stringent and not based on risk, which led to higher acquisition costs and schedule delays.[77]

BioWatch Gen-2. We reported in 2015 that due to a perceived urgent need, the original BioWatch system was deployed in 2003 without performance requirements, and that in the 12 years since BioWatch's initial deployment, DHS had not developed technical performance requirements against which to measure the system's ability to meet its objective. We reported that requirements would provide targets against which test results can be evaluated in order to assess whether the system will reliably achieve its intended purpose.

At the time we concluded our 2015 review, DHS was already working on an enhancement to the BioWatch system—BTE—and the caution we voiced at that time remains. DHS lacks targets for the current BioWatch 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 also cannot ensure it has complete information to make decisions about the value of proposed upgrades or enhancements.

We recommended that DHS establish technical performance requirements, including limits of detection, necessary for a biodetection system to meet a clearly defined operational objective for the BioWatch program by detecting attacks of defined types and sizes with specified probabilities, and assess the Gen-2 system against these performance requirements to reliably establish its capabilities. This recommendation remains open.

We continue to believe that our recommendation is relevant to DHS's current efforts, as it continues to develop key operational and technical requirements for a biodetection system to meet a clearly defined operational objective. The requirements-setting process is a critical step for BD21, so that performance is not compared to BioWatch, but to the requirements needed to address the key capability gaps DHS identified. Because the BD21 concept is a

[77]GAO-12-810 and GAO-16-99.

system-of-systems the program office will also have to develop system-wide requirements in addition to component-level requirements. Comparing BioWatch's capabilities against these new requirements is also a critical step in determining the extent to which BioWatch can address the existing needs of the biodetection capability and where improvements may be needed.

As described above, the BD21 program is early in its acquisition lifecycle and still developing key documents outlining proposed requirements, therefore it is too early to assess the extent to which DHS will fully implement our recommendation. We believe by implementing the recommendation, DHS can mitigate risks in the BD21 acquisition, and we will continue to monitor DHS's progress while it pursues a replacement for the current BioWatch system.

BioWatch Gen-3. In 2012, we reported on DHS's efforts to replace the Gen-2 BioWatch system with an autonomous detection system called Gen-3. According to BioWatch program officials at the time, the original sensitivity requirement—a key performance parameter outlined in the Operational Requirements Document—was set based on interest in pushing the limits of potential technological achievement rather than in response to a desired public health protection outcome. The system sensitivity demonstrated by the candidate technology tested for Gen-3 during characterization testing was orders of magnitude lower than the original requirement.

BioWatch program officials told us at the time of our 2012 review that the original sensitivity requirement was based on what DHS thought the technology could theoretically achieve, and was not informed by a scientific and risk-informed assessment of what level of sensitivity would be needed, from an operational perspective, to fulfill the Gen-3 purpose of mitigating consequences in the event of a biological attack. Because DHS did not ground the sensitivity requirement in Gen-3 program goals, when the candidate technologies were unable to meet the requirement, DHS encountered delays and uncertainty about how to move forward. Officials said that this led to a requirement that may have been too stringent, resulting in higher costs and schedule delays without a demonstrated mission imperative. Further, the revised Gen-3 sensitivity requirement was based on ideas about the performance characteristics of the Gen-2 system, which has not been linked to a clear operational objective; therefore, because the revised sensitivity requirement for Gen-3 was based on Gen-2, it was not grounded in an operational objective, either.

BD21 is exploring the performance envelope of current biological sensor technologies which will inform development of the Operational

Requirements Document. We recognize that the BD21 program office is early in the acquisition lifecycle and understand the importance of setting realistic requirements that do not far outpace the maturity of the technology. As part of our 2015 review that evaluated Gen-3 testing, we reported that any future acquisition, upgrade, or enhancement to BioWatch Gen-2 could help prevent delays and uncertainty in the acquisition by having initial requirements based more closely on mission need and operational objectives. By implementing the recommendations from our 2015 report, DHS has an opportunity to mitigate risk in the BD21 acquisition by applying lessons from other acquisition efforts to replace BioWatch and collect the scientific and risk-informed information it will need to develop requirements for BD21.

Stakeholder involvement. In 2012, we also reported that the process used to set the original sensitivity requirement for Gen-3 did not reflect stakeholder consensus about how to balance mission needs with technological capabilities. Specifically, the BioWatch program did not prepare a Concept of Operations before ADE 2A. According to DHS acquisitions guidance, in developing a Concept of Operations, stakeholders engage in a consensus-building process regarding how to balance technological capabilities with mission needs in order to gain consensus on the use, capabilities, and benefits of a system. We found at the time that because DHS did not prepare a Concept of Operations before establishing operational requirements for Gen-3, the sensitivity requirement did not reflect broad stakeholder engagement in balancing schedule, cost, and risk realities with achieving a specified mission outcome, for example, a specific level of population protection. After the Gen-3 acquisition was canceled, DHS recognized the need to better communicate with stakeholders about using a flexible testing approach to refine requirements to avoid any misperception that the requirements would be adjusted to accommodate the vendor's capabilities.

The BD21 program office has conducted several outreach efforts with stakeholders, including workshops with first responders and public health officials and will be analyzing results of a stakeholder survey to stakeholders conducted in 2020. BD21 Program office officials said they are using this information to develop the concept of operations document and operational requirements document prior to ADE 2A decision.[78] It is too early to determine the extent to which these documents will reflect

[78]The BD21 concept of operations was finalized in March 2021. We will assess this as part of our ongoing recommendation monitoring activities.

stakeholder consensus, but the engagement described to date is an improvement on past efforts. As part of our efforts to monitor DHS's implementation of our prior recommendations, we will continue to assess DHS's actions to incorporate stakeholder feedback in developing acquisition documentation.

Early developmental testing for resilience. In 2015, we reported that the actions and decisions DHS made regarding the acquisition and testing of Gen-3 partially aligned with best practices GAO previously identified for developmental testing of threat detection systems.[79] For example, best practices indicate that resilience testing, or testing for vulnerabilities, can help uncover problems early. While DHS took steps to help build resilience into the Gen-3 testing, we found in 2015 that future testing for a biodetection capability could be improved by using more rigorous methods to help predict performance in different operational environments.

Our 2015 findings also highlighted the best practice of taking a systems engineering view of the system prior to entering into any developmental test. This includes understanding the boundaries of what it is being tested prior to developmental testing. For example, in the context of BD21, will test plans include just the testing of assays or analytical components or will they describe a plan to test the whole end-to-end system (i.e., anomaly detection, collection, field analysis, and laboratory confirmation)? Further, will that plan be documented in the test and evaluation master plan? As our past work has noted, taking a systems engineering view is critical, since different system boundaries impose different testing methods and constraints.

[79]GAO-16-99 and GAO, *Combating Nuclear Smuggling: DHS Research and Development on Radiation Detection Technology Could Be Strengthened*, GAO-15-263 (Washington, D.C.: March 6, 2015). The March 2015 report provided the complete list of best practices for developmental testing of threat detection systems. The practices are (1) Ensure that accountability and engagement in developmental testing are commensurate with the amount of risk accepted, (2) Include representatives from the user community in design and developmental testing teams to ensure acceptance of the system by the user community, (3) Take a proper systems engineering view of the system prior to entering into any developmental test, (4) Use statistical experimental design methodology to establish a solid foundation for developmental testing, (5) Measure and characterize system performance with established procedures, methods, and metrics, (6) Test to build in resilience, especially in the development stages, (7) Use developmental tests to refine requirements, and (8) Engage in a continuous cycle of improvement by conducting developmental testing, conducting operational testing, and incorporating lessons learned.

We recognize that demonstrating the BD21 system's end-to-end ability to detect live agents in an operational environment is not possible because threat agents cannot be released into the air in such environments. Like the testing for BioWatch, BD21 tests will need to rely on simulants, which may be inactivated, or killed, forms of the same agents that the system is designed to detect. Nevertheless, end-to-end testing that creates the most realistic environment possible will be important, because components may perform differently when combined than when tested separately. This end-to-end testing will also be crucial, as BD21's present design is referred to as a system-of-systems.

In our 2015 report, we recommended that DHS use the best practices outlined in the report to inform test and evaluation actions for any future upgrades or changes to technology for BioWatch. DHS has made multiple improvements to its acquisition and test and evaluation guidance since the Gen-3 system was tested, which largely reflect the best practices. However, because the BD21 acquisition is so early in the acquisition lifecycle, this recommendation remains open until we can assess whether DHS is applying the lessons learned for its testing events.

Cybersecurity risks. Accounting for cybersecurity risks in the planning and testing will be important for BD21, due to its reliance on the use of algorithms and networked communication. For example, DHS will need to secure the networked communication system against interference, such as from hackers. In 2015, we reported that during the Gen-3 acquisition, DHS officials specifically planned for testing of network security as described in the test and evaluation master plan. DHS officials stated that an unsecure system would be vulnerable to hackers' planting results or shutting systems down. In 2012, we reported that the 2011 Operational Assessment for Gen-3 stated that failure to demonstrate network security may seriously inhibit user confidence in the system.

BD21 officials reported to us that cybersecurity needs for the acquisition have been discussed since the April 2020 acquisition review board meeting. Since then, they said a cybersecurity resilience working group has been established and a draft threat assessment of cyber threats has been completed. BD21 officials characterized the discussion of cybersecurity threats as an emerging discussion between the program and DHS is deciding if BD21 should be an IT or non-IT acquisition program. BD21 officials said that the control module demonstration for BD21 will inform how data are managed and shared with stakeholders, and that the program will have to evaluate the platforms and interfaces the stakeholders might use to communicate information. It is too early to

determine the extent to which the test plans will reflect the testing needed to ensure BD21's cybersecurity, but leveraging past experience and available guidance can help ensure a secure system.

Accounting for uncertainty. As part of our 2015 review evaluating the capabilities of the current BioWatch Gen-2 system, we found that in the absence of technical performance requirements, DHS officials said their assertion that the system can detect catastrophic attacks was supported by modeling and simulation studies. However, 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 had provided a full accounting of statistical and other uncertainties—meaning decision makers had no means of understanding the precision or confidence in what is known about system capabilities.[80] In 2015, we recommended DHS produce a full accounting of statistical and other uncertainties and limitations in what is known about Gen-2's capabilities. DHS concurred and described steps to address the recommendation, but this recommendation remains open. We will continue to monitor DHS's progress while it pursues a replacement for the current BioWatch system.

Because of the limitations with Gen-2 we identified in our 2015 work, decision makers may not have sufficient information to ensure future investments in biodetection are actually addressing a capability gap not met by the current system. This information is vital to making informed decisions about the value of proposed upgrades, like BD21. We believe that our 2015 recommendation is relevant to DHS's current efforts, as it conducts demonstrations and tests of technologies to replace the BioWatch system.

Conclusions

The BD21 acquisition program is the latest in a series of DHS efforts designed to improve its ability to provide early warning and detection of an aerosolized biological attack. The BD21 concept incorporates state-of-the-art technologies alongside established capabilities to create an innovative approach to biodetection, and the BD21 acquisition builds on previous and ongoing investments in biodetection. For example, DHS's decision to focus on an anomaly detection capability builds on the results of two previous acquisition efforts that did not provide a cost effective

[80]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.

solution. BD21 is an incremental approach that builds on the results of the cancelled BTE effort aimed at addressing gaps BTE could not address. However, as the BD21 program office continues to develop key required acquisition documents for the BD21 acquisition, clarification is needed on how the program plans to address the situational awareness capability gap it identified. Specifically, current program documentation is not clear on how this effort to develop a situational awareness capability is different from, tied to, or may leverage an ongoing DHS biosurveillance effort that provides a common operating picture for DHS and its partners. Providing clarification on the specific functionality and sources of information will help give BD21 stakeholders the information they need to understand what data they are expected to provide and how BD21 will operate within their jurisdictions, as well as identify the technology elements necessary to address this identified gap. This clarification will also help ensure efforts are not unnecessarily duplicative within DHS or elsewhere.

The BD21 concept involves incorporating critical technologies that have not been combined and used previously for use in biodetection in urban, civilian environments, and we identified several inherent limitations and new challenges the BD21 program acquisition faces in developing anomaly detection algorithms. To help mitigate risk in the acquisition associated with its approach, the program office conducted an alternatives analysis and is testing the basic proof of concept of the anomaly detection algorithm in a technology demonstration. Although the program described future efforts to conduct technology readiness assessments of the critical technology elements under consideration, we found DHS's TRA/MRA guidance on conducting such assessments did not fully incorporate best practices we previously identified. Specifically, we recently issued a best practice guide for technology readiness assessments that identifies the best practices and associated high-quality characteristics of a TRA. Incorporating the refined best practices from our GAO TRA best practices guide into DHS's guidance, and applying them in the BD21 acquisition, can help ensure DHS has sufficient information on the maturity of technology elements, as well as systems-level information, to determine if the solutions under consideration are sufficiently mature.

Finally, our prior body of work evaluating the capabilities of the current BioWatch system, efforts to upgrade the existing system, and role these types of environmental detection systems play within the broader biodefense enterprise offers insight into additional risk mitigation steps DHS should consider during the BD21 acquisition. For example, we have several open recommendations to help ensure sufficient information is

known about the current BioWatch system, including to compare what is known about the current system against technical performance requirements for a biodetection system to meet a clearly defined operational objective. Addressing our prior recommendations can help ensure biosurveillance-related funding is directed to programs that can demonstrate their intended capabilities or make informed cost-benefit decisions about possible upgrades and enhancements to the system. Emerging events also underscore the need to assess the benefit of environmental detection systems aimed at providing early warning of possible aerosolized attacks as a risk mitigation activity, because of their relatively limited scope. Evaluating how these systems fit within the broader biodefense enterprise that must address a vast array of evolving biological threats, including naturally occurring infectious diseases, is part of the ongoing implementation of the National Biodefense Strategy, which we have previously reported requires continued oversight.

Recommendations for Executive Action

We are making three recommendations to the Secretary of Homeland Security:

The Secretary of Homeland Security should ensure the BD21 program office clarifies in its acquisition documentation before the ADE 2A decision point the intention of the situational awareness and common operating picture capability identified as a gap, including the specific functionality, sources of information, and distinction from existing common operating picture functions at DHS. (Recommendation 1)

The Secretary of Homeland Security should ensure DHS fully incorporate the best practices outlined in GAO's TRA best practice guide in DHS's TRA/MRA guide to ensure that its acquisition projects have the best practices for conducting high-quality TRAs. (Recommendation 2)

The Secretary of Homeland Security should ensure the BD21 program conducts high-quality TRAs of all critical technologies for BD21 before the ADE 2A decision and before the ADE 2B decision (including a TRA of the overall system level interaction with the anomaly detection algorithm), in accordance with GAO's TRA best practice guide. (Recommendation 3)

Agency Comments and Our Evaluation

We provided a draft of this report to DHS and DOD for review and comment. We incorporated technical comments from DHS, as appropriate. Additionally, in its written comments, which are reproduced in appendix I, DHS concurred with our three recommendations and provided additional information on the steps the agency has taken or plans to take to address our recommendations.

DHS concurred with our first recommendation to clarify its acquisition documentation prior to ADE 2A regarding the establishment of a situational awareness capability for BD21, including identifying the specific functionality, sources of information, and distinction from existing common operating picture functions. DHS stated that the operational requirements document, which will be prepared in advance of ADE 2A will capture what the BD21 system needs to accomplish from an operational standpoint to meet the stated mission need. DHS said that further clarification and translating of those requirements will happen after ADE 2A. DHS described plans to clarify acquisition documents by capturing BD21 system situational awareness and normal operation picture capability functionality, sources of information, and distinction from the existing standard operating picture functions at DHS. DHS estimated it will complete these initiatives by April 29, 2022. We believe DHS's described actions align with the intent of our recommendation, and having as much detail and transparency in describing BD21's operational requirements will help ensure situational awareness capabilities do not overlap.

DHS concurred with our second recommendation to incorporate TRA best practices from GAO's guide into its TRA/MRA guide to ensure that its acquisition projects have the framework and best practices for conducting high-quality TRAs. Specifically, DHS stated that its guide, promulgated by Science and Technology's Office of Science and Engineering on November 4, 2020, incorporates lessons learned from the Department of Defense, National Aeronautics and Space Administration, Veterans Affairs, Federal Aviation Administration, and GAO to enable a credible and consistent Technology and Manufacturing Readiness Assessments as a means of assessing technology and manufacturing maturity. DHS considers this recommendation implemented.

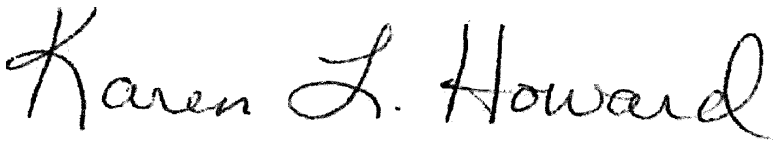
While DHS considers this recommendation as already implemented, we disagree. DHS submitted a copy of its TRA/MRA guide on April 29, 2021, and said the GAO best practices were incorporated into its guide. We evaluated the updated guide against GAO's TRA best practices and found that while DHS's TRA/MRA guide does incorporate some of the best practices from GAO's TRA best practices guide, it does not fully implement all of the best practices that we identify as important. For example, DHS's TRA/MRA guide does not discuss how it will ensure the TRA team is independent and objective. Further, while DHS's guide states a plan should be prepared and included some elements of a TRA plan (i.e. purpose, resources, and schedule), it does not specify how dissenting views should be handled, or require independence

agreements. We believe fully incorporating all the best practices we identified will help DHS ensure higher-quality TRAs. Therefore, we do not consider this recommendation to be fully implemented. We have updated the discussion of the TRA/MRA guide in this report to reflect these recent changes and consider this recommendation open.

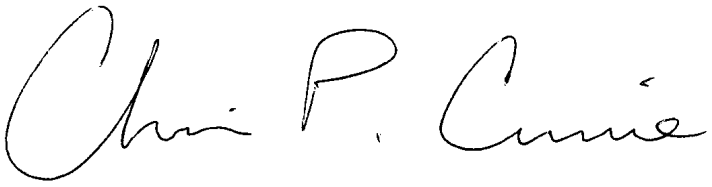
DHS concurred with our third recommendation to conduct high-quality TRAs of all critical technologies for BD21 before ADE 2A decision and before the ADE 2B. DHS said that the Johns Hopkins University Applied Physics Laboratory in conjunction with DHS Science & Technology will conduct a TRA prior to ADE 2A. Further it said the program will also conduct another TRA on system developer-proposed solutions as part of the Preliminary Design Review prior to ADE 2B. DHS anticipates these activities will take place in the first quarter of FY 2022 and the first quarter of FY 2023, respectively. We believe DHS's plan for Johns Hopkins University in conjunction with DHS Science & Technology to conduct high-quality TRAs prior to acquisition decision events align with our recommendation, provided it conducts assessments that follow all the best practices we identified. We will continue to monitor DHS's activities in addressing this recommendation.

We are sending copies of this report to the appropriate congressional committees, the Secretary of the Department of Defense, and the Secretary of the Department of Homeland Security. In addition, the report is available at no charge on the GAO website at https://www.gao.gov.

If you or your staff have any questions about this report, please contact Karen Howard at (202) 512-6888 or howardk@gao.gov, or 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 report. GAO staff who made key contributions to this report are listed in appendix II.



Karen L. Howard
Director, Science, Technology Assessments, and Analytics



Chris P. Currie
Director, Homeland, Security, and Justice

List of Requesters

The Honorable Gary C. Peters
Chairman
The Honorable Rob Portman
Ranking Member
Permanent Subcommittee on Investigations
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Frank Pallone, Jr.
Chairman
The Honorable Cathy McMorris Rodgers
Republican Leader
Committee on Energy and Commerce
House of Representatives

The Honorable Bennie Thompson
Chairman
Committee on Homeland Security
House of Representatives

The Honorable Eddie Bernice Johnson
Chairwoman
The Honorable Frank Lucas
Ranking Member
Committee on Science, Space, and Technology
House of Representatives

The Honorable Bill Foster
Chairman
Subcommittee on Investigations and Oversight
Committee on Science, Space, and Technology
House of Representatives

The Honorable Diana DeGette
Chair
The Honorable H. Morgan Griffith
Republican Leader
Subcommittee on Oversight and Investigations
Committee on Energy and Commerce
House of Representatives

The Honorable Ron Johnson
United States Senate

The Honorable Brett Guthrie
House of Representatives

The Honorable Ralph Norman
House of Representatives

The Honorable Mike Rogers
House of Representatives

The Honorable Mikie Sherrill
House of Representatives

Appendix I: Comments from the Department of Homeland Security

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

May 3, 2021

Karen L. Howard
Director, Science, Technology
Assessments, and Analytics
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Chris Currie
Director, Homeland Security and Justice
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: Management Response to Draft Report GAO-21-292, "DHS Exploring New Methods to Replace BioWatch and Could Benefit from Additional Guidance"

Dear Ms. Howard and Mr. Currie:

Thank you for the opportunity to comment on this draft report. The U.S. Department of Homeland Security (DHS or the Department) appreciates the U.S. Government Accountability Office's (GAO) work in planning and conducting its review and issuing this report.

The Department is pleased to note GAO's recognition of Biological Detection for the TwentyFirst Century (BD21) as an acquisition program that is intended address BioWatch limitations by enhancing early detection of aerosolized biological attacks in such a way that increases opportunities to implement measures to reduce illness and loss of life. It is important to also note that on March 25, 2021, the Executive Director of the DHS Joint Requirements Council validated the BD21 Concept of Operations (CONOPS), which contrasts current operations and practices with future methods of operating under potential future threats and conditions, using potential capability solutions. Furthermore, this validation of the CONOPS supports the Countering Weapons of Mass Destruction Office's (CWMD) development of the BD21 Operational Requirements Document (ORD). Through this and other efforts, the Department remains committed to employing

best practices and conducting technology readiness assessments (TRAs) throughout the acquisition lifecycle to pursue a next-generation capability to detect airborne biological threat agents.

The draft report contained three recommendations with which the Department concurs. Attached find our detailed response to each recommendation. The Department previously submitted technical comments addressing several accuracy, sensitivity, and contextual issues under a separate cover for GAO's consideration.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Sincerely,

JIM H CRUMPACKER

Digitally signed by JIM H CRUMPACKER
Date: 2021.05.03 15:54:34 -04'00'

JIM H. CRUMPACKER, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

Attachment

2

Attachment: Management Response to Recommendations Contained in GAO-21-292

GAO recommended that the Secretary of Homeland Security ensure that:

Recommendation 1: The BD21 program office clarifies in its acquisition documentation before the ADE [Acquisition Decision Event] 2A decision point, the intention of the situational awareness and common operating picture capability identified as a gap, including the specific functionality, sources of information, and distinction from existing common operating picture functions at DHS.

Response: Concur. The BD21 program office is currently in the "Analyze/Select" phase of the acquisition lifecycle and is conducting program planning activities. A key document delivered prior to ADE 2A, currently on track for the first quarter of fiscal year (FY) 2022, is the ORD, which will capture what the BD21 system needs to accomplish from an operational standpoint to meet the stated mission need. Once the BD21 program has an approved ORD and has successfully passed the ADE 2A milestone to proceed into the "Obtain" phase of the acquisition lifecycle, functional analysis of the operational requirements will occur. At that point, the BD21 program office will capture in acquisition documentation the: (1) BD21 system situational awareness and normal operational picture capability functionality; (2) sources of information; and (3) distinction from existing standard operating picture functions at DHS. Estimated Completion Date (ECD): April 29, 2022.

Recommendation 2: DHS incorporates the best practices outlined in GAO's TRA best practice guide in DHS's updated TRA guide to ensure that its acquisition projects have the framework and best practices for conducting high-quality TRAs.

Response: Concur. CWMD agrees with the use of GAO's TRA best practices and notes that DHS has already incorporated them into the September 2020 DHS Technology Readiness Assessment/Manufacturing Readiness Assessment (TRA/MRA) Guide, promulgated by Science and Technology's Office of Science and Engineering on November 4, 2020. This final DHS TRA/MRA Guide incorporates lessons learned from the: (1) Department of Defense; (2) National Aeronautics and Space Administration; (3) Veterans Affairs; (4) Federal Aviation Administration; and (5) GAO to enable credible and consistent Technology and Manufacturing Readiness Assessments as a means of assessing technology and manufacturing maturity. On April 29, 2021, a copy of the TRA/MRA Guide was provide to GAO under separate cover.

DHS requests that the GAO consider this recommendation closed, as implemented.

3

Recommendation 3: The BD21 program conducts high-quality TRAs of all critical technologies for BD21 before the ADE 2A decision point, and before the ADE 2B decision point (including a TRA of the overall system level interaction with the anomaly detection algorithm), in accordance with the best practices in GAO's TRA best practice guide.

Response: Concur. The BD21 program commissioned the Johns Hopkins University Applied Physics Laboratory to conduct a formal TRA of representative system critical technology elements supporting the S&T Assessment required before going into the ADE 2A decision in the first quarter of FY 2022. The program will also conduct another TRA on system developer-proposed solutions as part of the Preliminary Design Review prior to the ADE 2B decision in the first quarter of FY 2023. The BD21 program ensures that all TRAs are carried out according the best practices in GAO's TRA best practice guide. ECD: November 30, 2022.

4

Appendix II: GAO Contacts and Staff Acknowledgments

GAO Contacts

Karen L. Howard at (202) 512-6888, howardk@gao.gov

Chris P. Currie at (404) 679-1875, curriec@gao.gov

Staff Acknowledgments

In addition to the contacts named above, Sushil Sharma (Assistant Director), Chris Ferencik (Assistant Director), John Ortiz (Analyst-in-Charge), Katrina Taylor (Analyst-in-Charge), Nora Adkins, Brian Bothwell, Tracey King, Cindy Korir-Morrison, Susanna Kuebler, Anika McMillon, Alexis Olson, and Benjamin Shouse made key contributions to the report.