United States Government Accountability Office

GAO

Report to Congressional Requesters

July 2009

BIOSAFETY LABORATORIES

BSL-4 Laboratories Improved Perimeter Security Despite Limited Action by CDC

GAO-09-851

July 2009

BIOSAFETY LABORATORIES

BSL-4 Laboratories Improved Perimeter Security Despite Limited Action by CDC

GAO Accountability·Integrity·Reliability

Highlights

Highlights of GAO-09-851, a report to congressional requesters

Why GAO Did This Study

Biosafety laboratories are primarily regulated by either the Department of Health and Human Services (HHS) or the U.S. Department of Agriculture (USDA), depending on whether the substances they handle pose a threat to the health of humans or plants, animals, and related products, respectively. Currently, all operational biosafety level 4 (BSL-4) labs are overseen by HHS's Centers for Disease Control and Prevention (CDC). BSL-4 labs handle the world's most dangerous agents and toxins that cause incurable and deadly diseases. In September 2008, GAO reported that two of the five operational BSL-4 labs had less than a third of the key perimeter security controls GAO assessed and recommended that CDC implement specific perimeter controls for all BSL-4 labs.

GAO was asked to (1) provide an update on what action, if any, CDC took to address the 2008 recommendation; (2) determine whether perimeter security controls at the two deficient BSL-4 labs had improved since the 2008 report; and (3) provide other observations about the BSL-4 labs it assessed.

To meet these objectives, GAO reviewed CDC's statement to Congress as well as other agency and HHS documentation on actions taken or to be taken with respect to the 2008 recommendation, reviewed new security plans for the two deficient BSL-4 labs, and performed another physical security assessment of these two labs. GAO is not making any recommendations.

View GAO-09-851 or key components. For more information, contact Gregory D. Kutz at (202) 512-6722 or kutzg@gao.gov.

What GAO Found

Significant perimeter security differences continue to exist among the nation's five BSL-4 laboratories operational at the time of GAO's assessment. In 2008, GAO reported that three of the five labs had all or nearly all of the 15 key controls GAO evaluated. Two labs, however, demonstrated a significant lack of these controls, such as camera coverage for all exterior lab entrances and vehicle screening. As a result, GAO recommended that CDC work with USDA to require specific perimeter security controls at high-containment facilities. However, to date, CDC has taken limited action on the GAO recommendation.

The two labs GAO found to be deficient made progress on their own despite CDC's limited action. One made a significant number of improvements, thus reducing the likelihood of intrusion. The second made a few changes and formed a committee to consider and prioritize other improvements. The following table shows progress on 9 of the 15 controls GAO initially assessed.

Progress on Perimeter Security Controls at Two BSL-4 Labs as of March 2009

Security controls	Lab C	Lab E
Visitor screening	√	Previously in place
Command and control center	√	Not in place
Camera coverage for all exterior entrances	√	Not in place
Closed-circuit television (CCTV) monitored by command and control center	In progress	Not in place
Active intrusion detection system integrated with CCTV	In progress	Not in place
Visible armed guard presence at all public entrances	Partially addressed	Not in place
Loading docks located outside the footprint of the main building	Partially addressed	Previously in place
Barriers to prevent vehicles from approaching lab	Not in place	√
Blast stand-off area (e.g. buffer zone) between lab and perimeter barriers	Not in place	√

Source: GAO.

Note: √ This symbol signifies control in place after GAO's 2008 report was issued.

Two additional observations about BSL-4 labs concern the significant perimeter security differences among the five labs GAO originally assessed for its 2008 report. First, labs with stronger perimeter controls had additional security requirements mandated by other federal agencies. For example, one lab is a military facility subject to far stricter Department of Defense physical security requirements. Second, CDC inspection officials stated their training and experience has been focused on safety. CDC officials said they are developing a comprehensive strategy for safety and security of labs and will adjust the training and inspection process to match this strategy.

In commenting on findings from this report, CDC and the two labs provided additional information on steps taken in response to GAO's prior recommendation and findings.

Contents

Tables

Abbreviations

BSL-4	Biosafety level 4
CCTV	Closed-Circuit Television
CDC	Centers for Disease Control and Prevention
DOD	Department of Defense
HHS	Department of Health and Human Services
IDS	Intrusion Detection System
USDA	U.S. Department of Agriculture
WG	Working Group
WMD	Weapon of Mass Destruction

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

July 7, 2009

The Honorable Susan M. Collins
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Tom Coburn, M.D.
Ranking Member
Permanent Subcommittee on Investigations
Committee on Homeland Security and Governmental Affairs
United States Senate

This report responds to continuing congressional interest in perimeter security at the nation's biosafety[1] level 4 (BSL-4) laboratories, which handle substances that cause incurable and deadly diseases. According to the Commission on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism, a major hurdle for terrorists seeking biological weapons has been the difficulty in acquiring disease-causing microbes and toxins that can be used to harm humans, livestock, or crops.[2] According to the commission, dangerous pathogens can be isolated from natural sources, but it would generally be easier for terrorists to steal or divert well-characterized "hot" strains from a research lab or culture collection. In December 2008, the commission wrote that it believed unless the world community acts decisively and with great urgency, it is more likely than not that a weapon of mass destruction will be used in a terrorist attack somewhere in the world by the end of 2013. The

[1] Biosafety is the discipline addressing the safe handling and containment of infectious microorganisms and hazardous biological materials. The principles of biosafety are containment and risk assessment. Containment includes the practices, equipment, and facility safeguards that protect personnel, the environment, and the public from exposure to substances handled and stored in the lab. Risk assessment is the process that enables the appropriate selection of practices, equipment, and facility safeguards that can prevent lab-associated infections.

[2] Commission on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism, *World at Risk: The Report of the Commission on the Prevention of WMD Proliferation and Terrorism* (Washington, D.C.: Dec. 2008). The creation of the commission, which was established by Pub. L. 110-53, § 1851, 121 Stat. 266, 501 (Aug. 3, 2007), implements a key recommendation of the independent, bipartisan 9/11 Commission to address the grave threat that the proliferation of weapons of mass destruction poses to our country.

commission also stated it believed that terrorists are more likely to be able to obtain and use a biological weapon than a nuclear weapon.

Labs that work with infectious microorganisms or hazardous biological materials are classified into four ascending levels of containment, based on origin, risk of infection, severity of disease, and other factors.[3] BSL-4 labs handle the world's most dangerous substances — those that are exotic in origin and easily transmit life-threatening diseases for which no treatment exists, such as the Ebola and smallpox viruses. Federal law gives regulatory control for pathogens and toxins to either the Department of Health and Human Services (HHS) or the U.S. Department of Agriculture (USDA), depending on whether these substances pose a threat to humans or to plants, animals, and products made from them, respectively.[4] The law requires HHS and USDA to review and publish a list of these substances, called select agents and toxins. All labs handling select agents must be registered with either HHS or USDA. The nation's operational BSL-4 labs are currently all overseen by HHS's Centers for Disease Control and Prevention (CDC), since they work with substances deemed a threat to humans. Regulations for select agents[5] require labs to conduct a site-specific risk assessment and develop a plan to guard against unauthorized access, theft, loss, or release,[6] but they do not mandate specific perimeter security controls be put in place.

[3] HHS, *Biosafety in Microbiological and Biomedical Laboratories*, 5th ed. (Washington, D.C.: 2007).

[4] Pursuant to the Public Health Security and Bioterrorism Preparedness and Response Act of 2002, Pub. L 107–188, § 201, 116 Stat. 594, 637 (codified at 42 U.S.C. § 262a) (Jun. 12, 2002), HHS is required to establish and maintain a list of biological agents and toxins that have the potential to pose a severe threat to public health and safety. Title II, Subtitle B of the Public Health Security and Bioterrorism Preparedness and Response Act is known as the Agricultural Bioterrorism Protection Act of 2002. Section 212, 116 Stat. 594, 647 (codified at 7 U.S.C. § 8401) of this Act requires USDA to establish and maintain a list of biological agents that have the potential to pose a severe threat to animal health and safety, plant health and safety, or to the safety of animal or plant products (select agents). The departments share responsibility for some agents because they potentially threaten both humans and animals (overlap select agents).

[5] 42 C.F.R. Part 73, 7 C.F.R. Part 331, and 9 C.F.R. Part 121.

[6] Additional requirements include a written biosafety plan that describes safety and containment procedures and an incident response plan that includes procedures for theft, loss, or release of an agent or toxin; inventory discrepancies; security breaches; natural disasters; violence; and other emergencies.

This report summarizes our findings and recommendation from our report[7] last year on key perimeter security controls at five of the nation's operational[8] BSL-4 labs.[9] In addition, we were asked to provide an update on what efforts, if any, CDC has taken to address our recommendation from that report. Further, this report describes the improvements, if any, that have been made to the perimeter security controls at the two labs found to be deficient. Finally, this report provides other observations about the BSL-4 labs we assessed.

This report is partly based on our previously issued report, which was conducted in accordance with standards prescribed by the President's Council on Integrity and Efficiency. In obtaining an update on whether CDC addressed our recommendation, we obtained and reviewed CDC's statement to congressional committees on actions taken or to be taken by the agency. We also asked that CDC officials apprise us on any other efforts they made to address our recommendation. To determine what improvements the deficient BSL-4 labs made, we asked lab officials to provide us with a list of perimeter security enhancements implemented since our report was issued. After we received the information, we conducted site inspections to verify the improvements and received briefings by lab officials on other planned enhancements. We also evaluated whether the planned and executed improvements fulfilled any of the 15 physical security controls we assessed in our prior report. Although BSL-4 labs may have different levels of inherent risk, we determined that these 15 controls (discussed in more detail in app. I) represent a baseline

[7] GAO, *Biosafety Laboratories: Perimeter Security Assessment of the Nation's Five BSL-4 Laboratories*, GAO-08-1092 (Washington, D.C.: Sept. 17, 2008).

[8] CDC informed us in June 2009 that a sixth BSL-4 lab has become operational. However, we are excluding it from the scope of this report due to its recency in becoming operational.

[9] For the purposes of this report, we defined physical security as the combination of equipment, personnel, and operational procedures used to protect facilities, information, documents, or material against theft, sabotage, diversion, or other criminal acts. Our definition of physical security excludes, and we did not evaluate, intelligence gathering, cyber security, and human capital training and effectiveness. We did not assess the overall security of the labs or the threat of an insider attack, but focused on perimeter security leading up to each building's points of entry. Additionally, we did not test perimeter security controls to determine whether they function as intended. Perimeter security is just one aspect of overall security provisions under the Select Agent Regulations, which includes personnel training and inventory control. Select Agent Regulations also require additional security measures inside the labs themselves, such as locks and other forms of physical control.

for strong perimeter security. We did not test whether the controls the labs did have in place were operating effectively.

We conducted our assessment from January 2009 through March 2009 in accordance with standards prescribed by the Council of the Inspectors General on Integrity and Efficiency. We provided officials from CDC and the two deficient BSL-4 labs with the pertinent sections of a draft of this report. We received written comments from these officials and have incorporated their comments throughout the report, as appropriate.

Security Assessment from Prior Report

Select agent regulations do not mandate that specific perimeter security controls be present at BSL-4 labs, resulting in a significant difference in perimeter security between the nation's five labs. According to the regulations, each lab must implement a security plan that is sufficient to safeguard select agents against unauthorized access, theft, loss, or release. However, there are no specific perimeter security controls that must be in place at every BSL-4 lab. While three labs had all or nearly all of the key security controls we assessed, our September 2008 report demonstrated that two labs had a significant lack of these controls (see table 1 below).

Table 1: Results of Perimeter Physical Security Assessment

No.	Security controls	Lab A	Lab B	Lab C	Lab D	Lab E
1	Outer/tiered perimeter boundary	✓	✓		✓	✓
2	Blast stand-off area (e.g., buffer zone) between lab and perimeter barriers	✓	✓		✓	
3	Barriers to prevent vehicles from approaching lab	✓	✓		✓	
4	Loading docks located outside the footprint of the main building	✓	✓		✓	✓
5	Exterior windows do not provide direct access to the lab	✓	✓	✓	✓	
6	Command and control center	✓	✓		✓	
7	Closed-circuit television (CCTV) monitored by the command and control center	✓	✓		✓	
8	Active intrusion detection system integrated with CCTV		✓		✓	
9	Camera coverage for all exterior lab building entrances	✓	✓		✓	
10	Perimeter lighting of the complex[a]	✓	✓	✓	✓	✓
11	Visible armed guard presence at all public entrances to lab	✓	✓			
12	Roving armed guard patrols of perimeter	✓	✓	✓	✓	
13	X-ray magnetometer machines in operation at building entrances	✓	✓		✓	
14	Vehicle screening	✓	✓			
15	Visitor screening	✓	✓		✓	✓

Source: GAO.

[a]We did not perform our assessment at night, so for this category we relied on the lab security officials to provide this information.

Lab C: Lab C had in place only 3 of the 15 key security controls we assessed. The lab was in an urban environment and publicly accessible, with only limited perimeter barriers. During our assessment, we saw a pedestrian access the building housing the lab through the unguarded loading dock entrance. In addition to lacking any perimeter barriers to prevent unauthorized individuals from approaching the lab, Lab C also lacked an active integrated security system. By not having a command and control center or an integrated security system with real-time camera monitoring, the possibility that security officers could detect an intruder entering the perimeter and respond to such an intrusion is greatly reduced.

Lab E: Lab E was one of the weakest labs we assessed, with 4 out of the 15 key controls in place. It had only limited camera coverage of the outer perimeter of the facility and the only vehicular barrier consisted of an arm gate that swung across the road. Although the guard houses controlling access to the facility were manned, they appeared antiquated and thus did not portray a strong, professional security infrastructure. The security

force charged with protecting the lab was unarmed.[10] Of all the BSL-4 labs we assessed, this was the only lab with an exterior window that could provide direct access to the lab. In lieu of a command and control center, Lab E contracts with an outside company to monitor its alarm in an off-site facility. This potentially impedes response time by emergency responders with an unnecessary layer that would not exist with a command and control center. Since the contracted company is not physically present at the facility, it is not able to ascertain the nature of alarm activation. Furthermore, there is no interfaced security system between alarms and cameras and a lack of real-time monitoring of cameras.

Although the presence of the controls we assessed does not automatically ensure a secure perimeter, having most of these controls in place and operating effectively reduces the likelihood of intrusion. As such, we recommended that the Director of the CDC take action to implement specific perimeter controls for all BSL-4 labs to provide assurance that each lab has a strong perimeter security system in place. As part of this recommendation, we stated that the CDC should work with USDA to coordinate its efforts, given that both agencies have the authority to regulate select agents. In its response to the report, HHS agreed that perimeter security is an important deterrent against theft of select agents. HHS indicated that the difference in perimeter security at the five labs was the result of risk-based planning; however, they did not comment on the specific vulnerabilities we identified and whether these should be addressed. In regard to requiring specific perimeter controls for all BSL-4 labs, HHS stated that it would perform further study and outreach to determine whether additional federal regulations are needed.

CDC Has Taken Limited Action to Require Specific Perimeter Security Controls

Significant perimeter security differences continue to exist among the nation's five BSL-4 labs operational at the time of our most recent assessment. As of May 2009, CDC has taken limited steps to address our recommendation that it should take action to implement specific perimeter security controls for all BSL-4 labs. Since the release of our report in September 2008, CDC stated that the following actions have been taken:

[10] Although the security force was unarmed, there was one armed security supervisor patrolling the facility.

- In late 2007, CDC, along with other federal agencies, established a U.S. Government Trans-Federal Task Force on Optimizing Biosafety and Biocontainment Oversight. The task force was formed to assess the current framework for local and federal oversight of high-containment laboratory research activities and facilities, including the identification and assessment of pertinent laws, regulations, policies, guidelines, and examination of the current state of biosafety oversight systems. The task force held a public consultation meeting in December 2008. According to CDC, the task force will communicate specific recommendations about the nation's lab safety and security issues to the Secretaries of both HHS and USDA.

- CDC and USDA hosted a workshop series in Greenbelt, Maryland, in December 2008 for all of its registered entities and partners. CDC stated that it included several safety and security topics, including discussion of physical security and operational security.

- In January 2009, in response to Executive Order 13486, a federal working group (WG) was convened to review current laws, regulations, and guidelines in place to prevent theft, misuse, or diversion to unlawful activity of select agents and toxins. The WG is chaired by HHS and the Department of Defense (DOD) and includes representatives from several federal agencies and includes a subgroup that is focused on physical and facility security of biolabs. The WG is expected to issue its final report to the President by July 2009.

Although CDC has taken some modest steps for studying how to improve perimeter security controls for all BSL-4 labs, CDC has not established a detailed plan to implement our recommendation. In addition, we requested documentation (e.g., minutes, interim reports) from the WG to substantiate whether progress was made in addressing our concerns. However, the WG responded to our request stating that they do not expect to make any interim reports, and they refused to provide us the minutes of their meetings. Without a detailed plan from CDC on what corrective actions are planned or information on any progress from the WG, it is impossible to monitor CDC's progress in implementing our recommendation to improve perimeter security controls for all BSL-4 labs. The ability to monitor progress openly and in a transparent manner is especially important because a sixth BSL-4 lab recently became operational, as mentioned above, and CDC expects more BSL-4 labs to be operational in the future.

Two Labs Take Action to Improve Perimeter Security Controls

Although CDC has taken limited action to address our original findings, the two deficient BSL-4 labs have made progress on their own. One BSL-4 lab made a significant number of improvements to increase perimeter security, thus reducing the likelihood of intrusion. The second one made three changes and formed a committee to consider and prioritize other changes.

Lab C

We confirmed the following improvements at Lab C:

- Visitors are screened by security guards and issued visitor badges.
- A command and control center was established.
- Camera coverage includes all exterior lab entrances.
- CCTV is monitored by the command and control center. The cameras currently cover the exterior of the building. Guards can control the cameras by panning, zooming, or tilting.
- One visible guard is present at the main entrance to the lab, but the guard is not armed. A guard mans the entrance 24 hours a day, 7 days a week. Although the guard is unarmed, this improvement does partially address the requirement for guard presence at lab public entrances. Lab officials described installing armed guards as cost prohibitive.
- While the loading dock is still located inside the footprint of the main building, Lab C improved its loading dock security by building a loading dock vehicle gate. Moreover, a pedestrian gate with a sign forbidding entry was built to prevent pedestrians from entering the building through the loading dock; pedestrians were previously allowed to enter the building through the loading dock as a way of taking a short-cut into the building. These new gates prevent individuals from walking into the building, or vehicles driving up to the building, unchallenged.

Lab officials said additional enhancements would be completed by fall 2009. These include an active intrusion detection system that is integrated with CCTV and the addition of 14 new interior cameras with pan, tilt, and zoom capabilities. The new cameras will enhance the interior perimeter security of the lab. The command and control center also will have access to and control of these new cameras. After these improvements are

finished, the lab will have 8 of the 15 controls we tested in place plus 2 others that were partially addressed.

Lab E

We verified three improvements were made at Lab E: heavy concrete planters were added as a vehicle barricade along the roadside adjacent to the building; the window was frosted to block sight lines into the lab from nearby rooftops; and a vehicle barricade is being constructed to block unauthorized access to the parking lot adjacent to the lab, thereby increasing the blast stand-off area. The lab also formed a committee to consider additional perimeter security measures such as widening buffer zones and increasing lighting at the perimeter fence. In all, the lab now has 6 of the 15 controls we assessed in place.

Although lab officials made three improvements and are considering others, the lab's head of research operations at the facility objected to the findings of our 2008 report and has challenged the 15 controls we deemed critical to strong perimeter security. He said that the officials from the lab were not afforded an opportunity to respond to the report and correct "inaccuracies." Specifically, he made the following comments on our previous findings:

- He questioned the basis for our selection of the specific 15 controls we identified as critical to perimeter security, and noted that CDC also expressed similar concerns in its comments on our 2008 report.

- The lab windows do not provide direct access to the lab. He maintained that a number of features prohibited entry by these windows: the lowermost edge of the windows is more than 7 feet 8 inches above ground level; the windows are certified bulletproof glass and are equipped with inside bars; and breaching the integrity of the outer bulletproof glass triggers alarms for the local guard force. Furthermore, he said that having such a window was deemed programmatically important when the laboratory was designed in order to provide light-dark orientation for laboratory workers. Finally, he represented that a group of nationally recognized security experts has opined that the windows are not a security threat, but did not provide evidence of these experts' assessment.

- Armed guards are present on the campus. He stated that a table in our 2008 report indicates that armed guards are not present on the campus, although a footnote on a subsequent page acknowledges that an armed security supervisor patrols the facility.

- A vehicle barrier does surround the perimeter of that portion of the laboratory building housing select agents, including the BSL-4 laboratory. He said it was recommended and approved by the Federal Bureau of Investigation during consultations on the safety of the building and installed in 1999 prior to initiation of research in this facility.

We continue to believe that our assessment of perimeter controls at Lab E is accurate. Specifically, we disagree with Lab E's position as follows:

- As stated in the report, we developed the 15 security controls based on our expertise in performing security assessments and our research of commonly accepted physical security principles. Although we acknowledge that the 15 security controls we selected are not the only measures that can be in place to provide effective perimeter security, we determined that these controls (discussed in more detail in app. I) represent a baseline for BSL-4 lab perimeter physical security and contribute to a strong perimeter security system. Having a baseline provides fair representation as to what key perimeter security controls do or do not exist at these facilities. The controls represent commonly accepted physical security principles. A lack of such controls represents a potential security vulnerability. For example, as mentioned above, at the time of our original assessment Lab E had only limited camera coverage of the outer perimeter of the facility. Camera coverage of a building's exterior provides a means to detect and quickly identify potential intruders.

- As mentioned above, Lab E was the only lab with an exterior window that could provide direct access to the lab. This window allowed for direct "visual" access into the lab area from an adjacent rooftop. Lab E in essence acknowledged this when it informed us in a letter that it "Frosted the BSL-4 laboratory windows to block sight lines from adjacent rooftops." While we credit Lab E for obscuring visual access to the lab by frosting this window, the window continues to pose a security vulnerability because it is not blast proof.

- Armed guards are not present on the campus. As mentioned above, Lab E's head of research operations pointed out that our 2008 report acknowledged that an armed security supervisor patrols the facility. However, employing one armed security supervisor does not support the plural definition of "guards." The supervisor also is not generally at the entrances to the facility. He normally responds to incidents and would not generally be in a position to confront an intruder at the

point of attack. Furthermore, placing armed guards at entrances also functions as a deterrent.

- The vehicle barrier did not surround the full perimeter of the BSL-4 lab building as it adjoined another lab building at the time of our original assessment. The facility has since placed additional barriers as noted in this report to give full coverage, thus validating our original assessment. Furthermore, part of the barrier in the area between a small parking lot and the BSL-4 lab building did not provide an adequate blast stand-off area. The lab, as noted in this report, has since erected barriers to this parking lot to allow only deliveries into the area.

The following table summarizes the progress the two labs have made on 9 of the 15 controls we initially assessed:

Table 2: Progress on Perimeter Security Controls at Labs C and E as of March 2009

Security controls	Lab C	Lab E
Visitor screening	√	Previously in place
Command and control center	√	Not in place
Camera coverage for all exterior entrances	√	Not in place
CCTV monitored by command and control center	In progress	Not in place
Active intrusion detection system integrated with CCTV	In progress	Not in place
Visible armed guard presence at all public entrances	Partially addressed	Not in place
Loading docks located outside the footprint of the main building	Partially addressed	Previously in place
Barriers to prevent vehicles from approaching lab	Not in place	√
Blast stand-off area (e.g., buffer zone) between lab and perimeter barriers	Not in place	√

Source: GAO.

Note: √ This symbol signifies control in place after our 2008 report was issued.

Additional Observations on Federal Oversight of BSL-4 Labs

During the course of our work, we made two additional observations that concern perimeter security differences among the nation's five BSL-4 labs that were operational at the time of our assessment:

- All five BSL-4 labs operating in 2008 had a security plan in place when we assessed them. Yet significant perimeter security differences exist among these high-containment labs. A reason for the discrepancies can be found in the additional federal security requirements the three labs with strong perimeter security controls in place had to follow beyond the select agent regulations. For example, Lab B is a military facility

subject to far stricter DOD physical security requirements. It had a perimeter security fence and roving patrol guards visible inside and outside this fence. Labs A and D also must meet additional mandates from the federal agencies that oversee them. A lack of minimum perimeter security requirements contributes to sharp differences among BSL-4 labs as well.

- CDC inspection officials stated their training and experience had been mainly in the area of safety. They also noted that their philosophy is a layered approach to security and safety. According to CDC officials, they are developing a comprehensive strategy for safety and security of biosafety labs and will adjust the training and inspection process accordingly to match this comprehensive strategy.

Agency and Third-Party Comments and Our Evaluation

We briefed CDC on the results of our work, and received comments from CDC by e-mail. In its response, CDC stated that it agrees that perimeter security is an important deterrent against theft of select agents and should be considered as one component of overall security at select laboratories. CDC stated that a comprehensive approach to securing select agents should be taken, and should include basic components such as physical security, personnel security, information security, transport security, and material control and accountability. CDC stated that its Select Agent Regulations reflect this comprehensive approach to securing agents and provide performance standards that entities must implement to protect agents from theft, loss, or release.

CDC also stated that multiple groups are assessing the issue of laboratory security and developing related recommendations. CDC stated that it will consider our prior recommendation and the reports from the multiple groups together before developing a detailed plan to address security at select agent laboratories. As part of this commitment, CDC stated that it is in the process of hiring a Security Officer to ensure that CDC has a continuing focus on security at the laboratories. According to CDC, the Security Officer will work with USDA to consider the recommendations from us and others in developing the plan to enhance security at select agent laboratories. In addition, CDC stated that it, in coordination with USDA, will seek input as to the need and advisability of requiring by federal regulation specific perimeter controls at each registered entity having a BSL-4 laboratory. CDC will initiate this process once all of the recommendations from the aforementioned groups have been received. CDC's stated intent to study our prior recommendation in improving laboratory security is an important response to the security issues that have been identified.

We also provided officials from Lab C and Lab E with the pertinent sections of a draft of this report that covered the results of our most recent perimeter security assessment of their labs, to which they responded with comments. Lab C officials provided additional details about several changes they made or plan to make to the lab's perimeter security controls, including changes to its CCTV, camera coverage, loading dock, barriers, and blast stand-off area. For example, Lab C officials said they are extending the sidewalks and installing landscaping features around the lab building to increase the size of the blast stand-off area. According to officials from Lab E, they plan to submit a grant application for additional perimeter security improvements, including an intrusion detection system at the perimeter fence and expanded CCTV coverage of key perimeter areas. We did not verify the perimeter security enhancements from Lab C and Lab E because these changes were made or planned subsequent to our most recent assessment. Officials from these labs also provided technical comments on the draft language from our report that we have incorporated throughout the report, as appropriate.

As agreed with your office, unless you announce the contents of this report earlier, we will not distribute it until 30 days after its issue date. At that time, we will send copies of this report to the Secretary of Health and Human Services, the Director of CDC, and other interested parties. In addition, the report will be available at no charge on GAO's Web site at http://www.gao.gov. If you or your staff have any questions regarding this report, please contact me at (202) 512-6722 or kutzg@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 major contributions to this report are listed in appendix II.

Gregory D. Kutz
Managing Director
Forensic Audits and Special Investigations

Appendix I: Perimeter Security Controls

To perform our perimeter security assessment of biosafety level 4 (BSL-4) labs, we identified 15 key perimeter security controls. We based their selection on our expertise and research of commonly accepted physical security principles that contribute to a strong perimeter security system. A strong perimeter security system uses layers of security to deter, detect, delay, and deny intruders:

- **Deter.** Physical security controls that deter an intruder are intended to reduce the intruder's perception that an attack will be successful—an armed guard posted in front of a lab, for example.
- **Detect.** Controls that detect an intruder could include video cameras and alarm systems. They could also include roving guard patrols.
- **Delay.** Controls that delay an intruder increase the opportunity for a successful security response. These controls include barriers such as perimeter fences.
- **Deny.** Controls that can deny an intruder include visitor screening that only permits authorized individuals to access the building housing the lab. Furthermore, a lack of windows or other obvious means of accessing a lab is an effective denial mechanism.

Some security controls serve multiple purposes. For example, a perimeter fence is a basic security feature that can deter, delay, and deny intruders. However, a perimeter fence on its own will not stop a determined intruder. This is why, in practice, layers of security must be integrated in order to provide the strongest protection. Thus, a perimeter fence should be combined with an intrusion detection system that would alert security officials if the perimeter has been breached. A strong system would then tie the intrusion detection alarm to the closed-circuit television (CCTV) network, allowing security officers to immediately identify intruders. A central command center is a key element for an integrated, active system. It allows security officers to monitor alarm and camera activity—and plan the security response—from a single location. Table 3 shows 15 physical security controls we focused on during our assessment work.

Table 3: Perimeter Physical Security Controls

No.	Perimeter physical security control	Rationale
1	Outer/tiered perimeter boundary	There should be a perimeter boundary outside the lab to prevent unauthorized access. Examples include a reinforced perimeter security fence or natural barrier system that uses landscaping techniques to impede access to buildings. Outer/tiered perimeter also includes other structures that screen visibility of the lab.
2	Blast stand-off area (e.g., buffer zone) between lab and perimeter barriers	To minimize effects of explosive damage if a bomb were to be detonated outside the lab, the perimeter line should be located as far as practical from the building exterior.
3	Barriers to prevent vehicles from approaching lab	A physical barrier consisting of natural or man-made controls, such as bollards, designed to keep vehicles from ramming or setting off explosives that could cause damage to the building housing the BSL-4 lab.
4	Loading docks located outside the footprint of the main building	Because they are areas where delivery vehicles can park, loading docks are vulnerable areas and should be kept outside the footprint of the main building.
5	Exterior windows do not provide direct access to the lab	Windows are typically the most vulnerable portion of any building; therefore, there should be no exterior windows that provide direct access to the lab.
6	Command and control center	A command and control center is crucial to the administration and maintenance of an active, integrated physical security system. The control center monitors the employees, general public, and environment of the lab building and other parts of the complex and serves as the single, central contact area in the event of an emergency.
7	CCTV monitored by the command and control center	A video system that gives a signal from a camera to video monitoring stations at a designated location. The cameras give the control center the capability of monitoring activity within and outside the complex.
8	Active intrusion detection system (IDS) integrated with CCTV	An IDS is used to detect an intruder crossing the boundary of a protected area, including through the building's vulnerable perimeter barriers. Integration with CCTV is integral to the IDS's ability to alert security staff to potential incidents that require monitoring.
9	Camera coverage for all exterior lab building entrances	Cameras that cover the exterior building entrances provide a means to detect and quickly identify potential intruders.
10	Perimeter lighting of the complex	Security lighting of the site, similar to boundary lighting, provides both a real and psychological deterrent, and allows security personnel to maintain visual-assessment capability during darkness. It is cost-effective in that it might reduce the need for security forces.
11	Visible armed guard presence at all public entrances to lab	All public entrances require security monitoring. This presence helps to prevent or impede attempts of unauthorized access to the complex.

No.	Perimeter physical security control	Rationale
12	Roving armed guard patrols of perimeter	The presence of roving armed guard patrols helps to prevent or impede attempts of unauthorized access and includes inspecting vital entrance areas and external barriers.
13	X-ray magnetometer machines in operation at building entrances	These machines provide a means of screening persons, items, and materials that may possess or contain weapons, contraband, or hazardous substances prior to authorizing entry or delivery into a facility.
14	Vehicle screening	Screening vehicles that enter the perimeter of the lab includes an identification check and vehicle inspection, in order to deny unauthorized individuals access and potentially detect a threat.
15	Visitor screening	Screening visitors to the lab reduces the possibility that unauthorized individuals will gain access. Visitor screening includes identifying, screening, or recording visitors through methods such as camera coverage or visitor logs so that their entry to the lab is recorded.

Source: GAO.

Appendix II: GAO Contact and Staff Acknowledgments

GAO Contact

Gregory D. Kutz, (202) 512-6722 or kutzg@gao.gov.

Acknowledgments

In addition to the contact named above, the following individuals made contributions to this report: Andy O'Connell, Assistant Director; Matt Valenta, Assistant Director; Christopher W. Backley; Randall Cole; John Cooney; Craig Fischer; Vicki McClure; Anthony Paras; and Verginie Tarpinian.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548