United States Government Accountability Office

GAO

Report to Congressional Committees

September 2008

BIOSAFETY LABORATORIES

Perimeter Security Assessment of the Nation's Five BSL-4 Laboratories

GAO-08-1092

September 2008

BIOSAFETY LABORATORIES

Perimeter Security Assessment of the Nation's Five BSL-4 Laboratories

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-08-1092, a report to congressional committees

Why GAO Did This Study

Biosafety labs under the U.S. Bioterrorism Act are primarily regulated and must be registered with either the Centers for Disease Control and Prevention (CDC) or the U.S. Department of Agriculture (USDA) under the Select Agent Regulations. Currently, all operational biosafety level (BSL) 4 labs are registered with the CDC and thus are regulated by the CDC, not USDA. BSL-4 labs handle the world's most dangerous agents and diseases. In fact, of the four BSL designations, only BSL-4 labs can work with agents for which no cure or treatment exists.

GAO was asked to perform a systematic security assessment of key perimeter security controls at the nation's five operational BSL-4 labs. To meet this objective, GAO performed a physical security assessment of the perimeter of each lab using a security survey it developed. GAO focused primarily on 15 physical security controls, based on GAO expertise and research of commonly accepted physical security principles.

What GAO Recommends

GAO recommends that the Director, 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. HHS agreed that perimeter security is an important deterrent against theft of select agents. However, HHS indicated that the vulnerabilities GAO identified are the result of risk-based planning and that further study is required prior to additional regulation.

To view the full product, including the scope and methodology, click on GAO-08-1092. For more information, contact Gregory D. Kutz at (202) 512-6722 or kutzg@gao.gov.

What GAO Found

Select Agent Regulations do not mandate specific perimeter security controls that need to be in place at each BSL-4 lab, resulting in significant differences in perimeter security between the nation's five labs. While three labs had all or nearly all of the key security controls GAO assessed—features such as perimeter barriers, roving armed guard patrols, and magnetometers in use at lab entrances—two labs demonstrated a significant lack of these controls. Specifically, one lab had all 15 security controls in place, one had 14, and another had 13 of the key controls. However, the remaining two labs had only 4 and 3 key security controls, respectively. The check marks in the table below indicate the presence of specific security features at the labs GAO assessed, illustrating the varying levels of perimeter physical security controls present at the labs for 5 of the 15 security controls GAO assessed.

Selected Results of Perimeter Security Assessment

Security controls	Lab A	Lab B	Lab C	Lab D	Lab E
Command and control center	✓	✓		✓	
Closed-circuit television (CCTV) monitored by the command and control center	✓	✓		✓	
Active intrusion detection system integrated with CCTV		✓		✓	
Camera coverage for all exterior lab building entrances	✓	✓		✓	
Visible armed guard presence at all public entrances to lab	✓	✓			

Source: GAO.

Although the presence of the security controls GAO assessed does not automatically ensure a secure perimeter, having most controls provides increased assurance that a strong perimeter security system is in place and reduces the likelihood of unauthorized intrusion. For example, the two labs with fewer security controls lacked both visible deterrents and a means to respond to intrusion. One lab even had a window that looked directly into the room where BSL-4 agents were handled. In addition to creating the perception of vulnerability, the lack of key security controls at these labs means that security officials have fewer opportunities to stop an intruder or attacker.

The two labs with fewer security controls were approved by the CDC to participate in the Select Agent Program despite their weaknesses. During the course of our review, GAO noted that the three labs with all or nearly all of the key security controls GAO assessed were subject to additional federal security requirements imposed on them by agencies that owned or controlled the labs, not because of the Select Agent Regulations.

Contents

Letter 1

Results in Brief 4
Background 5
Results of Security Assessment 6
Conclusions 10
Recommendation for Executive Action 10
Agency Comments and Our Evaluation 11

Appendix I **Perimeter Security Controls** 13

Appendix II **Comments from the Department of Health and Human Services** 16

Appendix III **GAO Contact and Staff Acknowledgments** 20

Tables

Table 1: Results of Perimeter Physical Security Assessment 7
Table 2: Perimeter Physical Security Controls 14

Abbreviations

APHIS	Animal and Plant Health Inspection Service
BSL	biosafety level
CCTV	Closed-circuit television
CDC	Centers for Disease Control and Prevention
DSAT	Division of Select Agents and Toxins
HHS	Department of Health and Human Services
IG	Inspector General
USDA	U.S. Department of Agriculture

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

September 17, 2008

The Honorable John D. Dingell
Chairman
The Honorable Joe Barton
Ranking Member
Committee on Energy and Commerce
House of Representatives

The Honorable Bart Stupak
Chairman
The Honorable John Shimkus
Ranking Member
Subcommittee on Oversight and Investigations
Committee on Energy and Commerce
House of Representatives

Biosafety level (BSL) 4 laboratories (labs) handle the world's most dangerous biological agents and diseases—the Ebola virus, hemorrhagic fevers, and smallpox, for example—in the hope that this work may result in effective medical countermeasures or even a cure. In fact, of the four BSL designations, only BSL-4 labs can work with agents for which no cure or treatment exists. Although BSL-4 labs are required to protect the safety of researchers and the general public, recent security incidents have caused some concern. For example, in October 2007 GAO testified about the lack of oversight and security concerns regarding BSL-3 and BSL-4 labs[1] and identified an hour-long power outage due to lightning strikes, in June 2007, at the Centers for Disease Control and Prevention's (CDC) newest BSL-4 facility. This incident raised questions about safety and security, as well as the backup power system design, and showed that even in the hands of experienced owners and operators, safety and security of high-containment labs can still be compromised. Among other things, the outage shut down the lab's negative air pressure system, one of the important components in place to keep dangerous agents from escaping the containment areas.

[1]GAO, *High-Containment Biosafety Laboratories: Preliminary Observations on the Oversight of the Proliferation of BSL-3 and BSL-4 Laboratories in the United States*, GAO-08-108T (Washington, D.C.: Oct. 4, 2007).

Primary responsibility for regulatory control of select biological agents is divided between the CDC and the U.S. Department of Agriculture (USDA) under Select Agent Regulations—although some labs may have additional security requirements imposed on them by agencies that own or control these labs. While three of the BSL-4 labs are privately owned or operated by academic institutions, the other two are owned and operated by the federal government. As requested by the Department of Health and Human Services (HHS), we are not including the names of the five labs in this report for security reasons. Federal law requires all labs be registered with the CDC's Division of Select Agents and Toxins (DSAT) when handling select agents that pose a severe threat to public health and safety, including BSL-4 agents.[2] Currently, all five operational BSL-4 labs are registered with the CDC's Select Agent Program and therefore are regulated by the CDC, not USDA. This registration process requires each lab to develop a security plan that is based on a site-specific risk assessment.[3] According to regulations, the security plan must be sufficient to safeguard against unauthorized theft, loss, or release of select agents. The DSAT inspection is intended to ensure that the labs meet certain safety and security regulations, which vary according to the BSL ranking of the select agent being handled. However, a recent report by HHS's Office of Inspector General (IG)[4] stated that labs regulated under the DSAT program had weaknesses in such areas as access control and security plan implementation that could have compromised their ability to safeguard select agents from accidental loss or theft.[5]

Performing research on select agents is critical for the development of effective medical countermeasures and, ultimately, the discovery of

[2]Alternatively, if any one of these agents is considered an "overlap agent" that also poses a threat to animal health, it may be registered with USDA's Animal and Plant Health Inspection Service (APHIS), but not both the CDC and APHIS. If the agents pose a risk to only animal and plant health or animal and plant products, they must be registered with APHIS.

[3]A site-specific risk assessment must provide protection based on the risk and intended use of the select agent. It includes four assessments: an agent-specific risk assessment, threat assessment, vulnerability assessment, and graded protection determination.

[4]Department of Health and Human Services, Office of Inspector General, *Summary Report on State, Local, Private, and Commercial Laboratories' Compliance With Select Agent Regulations*, A-04-06-01033 (Washington, D.C.: Jan. 9, 2008).

[5]HHS IG regularly conducts reviews of BSL labs. These reviews could possibly include BSL-4 labs; however, the summary reports do not disclose the identity of the labs that were included in the IG's reviews.

vaccines. However, given recent security concerns and the threat of biological terrorism, you are concerned that some BSL-4 labs could be vulnerable to terrorist attack or agent theft. To address these concerns, you requested that we perform a systematic physical security assessment of key perimeter security controls at the five operational BSL-4 labs in the United States.

To meet our objective, we reviewed the site-specific risk assessments and security plans for each BSL-4 lab. We then performed a physical security assessment limited to the perimeter of each lab using a security survey we developed. We focused primarily on 15 physical security controls that contribute to a strong perimeter physical security system based on our expertise and research of commonly accepted physical security principles. 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 for BSL-4 lab perimeter physical security. We discussed the security of each lab with security personnel and lab officials at the conclusion of each site visit. Finally, we interviewed DSAT and Animal and Plant Health Inspection Service officials and reviewed the CDC's BSL-4 lab inspection reports.

For the purposes of this report, we defined physical security as the combination of operational and security equipment, personnel, and 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, cybersecurity, and human capital training and effectiveness. We did not assess the security of the labs themselves or the threat of an insider attack, but focused on perimeter security leading up to the laboratory building 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.

We conducted our assessment from December 2007 through September 2008 in accordance with standards prescribed by the President's Council on Integrity and Efficiency.

Results in Brief

Regulations issued by the CDC do not mandate specific perimeter security controls that need to be in place at each BSL-4 lab, resulting in significant differences 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 minimum specific perimeter security standards 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—features such as perimeter barriers, roving armed guard patrols, and magnetometers in use at lab entrances—two labs demonstrated a significant lack of these controls. Specifically, one lab had all 15 security controls in place, one had 14, and another had 13 of the key controls. However, the remaining two labs had only 4 and 3 key security controls, respectively. Although the presence of the security controls we assessed does not automatically ensure a secure perimeter, having most controls provides increased assurance that a strong perimeter security system is in place and reduces the likelihood of unauthorized intrusion. For example, the two labs with fewer security controls lacked both visible deterrents and a means to respond to intrusion. One lab even had a window that looked directly into the room where BSL-4 agents were handled. In addition to creating the perception of vulnerability, the lack of key security controls at these labs means that security officials have fewer opportunities to stop an intruder or attacker. DSAT approved the security plans by the two labs lacking most key security controls. However, the three labs with all or nearly all of the key security controls we assessed were subject to additional requirements imposed on them by federal agencies other than DSAT. These labs incorporated additional specific security controls in their security plans because of this oversight. For example, one lab maintained a roving armed guard patrol—one of our 15 key controls—because the agency owning the lab required it, not because of DSAT regulation.

To further enhance physical perimeter security at BSL-4 labs regulated by DSAT, we are recommending that the Director, 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. 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 this report, HHS agreed that perimeter security is an important deterrent against theft of select agents. They 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. HHS also provided us with technical comments, which we have incorporated as appropriate.

Background

The Public Health Security and Bioterrorism Preparedness and Response Act of 2002 created the government's Select Agent Regulations,[6] dividing primary responsibility for regulatory control of select biological agents between HHS and USDA.[7] While HHS is responsible for regulating select agents that can potentially pose a severe threat to public health and safety, USDA regulates select agents that can potentially pose a severe threat to animal and plant health or animal and plant products. A number of "overlap agents" can pose both a public health threat and a threat to animals; in these cases, labs must register with either agency, but are not required to register with both. As mentioned above, all five registered BSL-4 labs in the United States are registered with DSAT.

When a lab registers with DSAT to handle a select agent, a site-specific risk assessment must be conducted. Regulations governing the assessment do not specify who must perform it, meaning that the assessment can be performed by officials for the lab itself. Further, labs registering with DSAT are required to develop and implement a written security plan based on the site-specific risk assessment. According to the regulations, the security plan must be sufficient to safeguard against unauthorized theft, loss, or release of select agents and meet all the requirements outlined in the Select Agent Regulations. DSAT authored and utilizes the Select Agents and Toxins Security Information Document to provide possible practices and procedures that entities may use to assist them in developing and implementing their written security plans. Additional requirements include a written biosafety or biocontainment plan that describes the 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. Prior to being issued a certificate of registration, an entity must comply with all security requirements and all other provisions of the Select Agent Regulations. A registration in the CDC's Select Agent Program lasts for 3 years, after

[6]42 C.F.R part 73, 7 C.F.R part 331, 9 C.F.R part 121.

[7]Pub. L. No. 107-188 (June 12, 2002).

which it must be renewed if the entity chooses to retain possession of the select agents.

In addition to the five registered and operational BSL-4 labs, there are more labs currently under construction or in the planning stages. While expansion is taking place within the federal sector as well—there are many new federal facilities currently under construction or planned, which have one or more BSL-4 labs—there are also BSL-4 labs at universities, as part of state response, and in the private sector. These new facilities have not completed the registration process and were not fully operational as BSL-4 labs at the time of our assessment.

Results of Security Assessment

CDC regulations do not mandate that specific perimeter security controls are present at all 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, two labs demonstrated a significant lack of these controls.

The results of our perimeter physical security assessment of the five registered BSL-4 labs are presented in table 1. The check marks in the table indicate the presence of specific security features at the labs we assessed, illustrating the varying levels of perimeter physical security controls present at the labs.

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.

Although the presence of the security controls we assessed does not automatically ensure a secure perimeter, having most controls provides increased assurance that a strong perimeter security system is in place and reduces the likelihood of unauthorized intrusion. As discussed in appendix I, the strongest perimeter security systems use an active, integrated approach to security that takes advantage of multiple layers. For example, an active, integrated system links perimeter intrusion alarms to a CCTV network, allowing security officers to instantly view the location of an alarm. A discussion of each security assessment follows.

Lab A: The physical security controls of Lab A presented a strong visible deterrent from the outside, with 14 of the 15 key security controls in place. Lab A was located in a complex of other buildings that was separated from an urban environment by a perimeter security fence reinforced with airline cable to further strengthen the fence and deter unauthorized access. A roving patrol of armed guards was visible inside and outside the perimeter fence, while other guards manned gated entry inspection points. The gates incorporated technical support for the guards to assist them with the inspection of both private and commercial vehicles. Guards conducted ID

checks at the gates and searched vehicles that did not have the appropriate access decals. Further, all trucks were required to enter a single gate containing an X-ray screening device. Past this outer perimeter, a further man-made barrier existed around the building containing the BSL-4 lab. Although Lab A had most of the security controls we focused on during our assessment, it did not have an active intrusion detection system integrated with the CCTV network covering the facility. This reduced the possibility that security officers could detect and quickly identify an intruder entering the building perimeter.[8]

Lab B: Lab B was the only one of the five BSL-4 labs that had all 15 security controls. The lab was in an urban environment, but located in a complex of other buildings enclosed within an outer fenced perimeter. Roving patrols consisting of both armed security guards and local police walked on the exterior of the perimeter fence. The fence itself was reinforced with airline cable to further strengthen it along areas that bordered roads, serving to further protect against unauthorized intrusion from these public areas. There was a single gated inspection point to enter the complex manned by armed security guards. The inspection point incorporated technical support for the guards to assist them with the inspection of both private and commercial vehicles. Once inside the gate, man-made barriers and a natural (i.e., landscaped) barrier system stood between the gate and the lab itself. More armed guards conducted roving patrols inside the complex and guarded the entrance to the lab itself. Lab B also had a strong active integrated security system. According to lab officials, the system featured an integrated emergency management response whereby appropriate fire and rescue vehicles were automatically dispatched after an alarm.

Lab C: Lab C utilized 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 live camera monitoring, the

[8]Officials from Lab A have subsequently informed us that they installed an active intrusion alarm system and integrated it with their CCTV network. However, we did not verify this information.

possibility that security officers could detect an intruder entering the perimeter and respond to such an intrusion is greatly reduced.

Lab D: Although Lab D did not have an armed guard presence outside the lab or vehicle screening,[9] it presented strong physical security controls in all other respects, with 13 of the key 15 controls we assessed. Lab D was located within the interior of a complex of buildings, providing a natural system of layered perimeter barriers that included bollards for vehicle traffic. When combined with the presence of roving armed guard patrols, Lab D projected strong visible deterrents. It also utilized an active integrated security system so that if an alarm was activated, personnel within the command and control center could survey the alarm area though monitors and utilize pan/tilt/zoom cameras to further assess the alarm area. This permits security personnel to better coordinate and determine the appropriate response.

Lab E: Lab E was one of the weakest labs we assessed, with 4 out of the 15 key controls. 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. 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 live monitoring of cameras.

DSAT approved the security plans for the two labs lacking most key security controls, and approved these labs to participate in the Select Agent Program as BSL-4 labs. Conversely, during our assessment, we

[9]At the time of our assessment, Lab D had a vehicle inspection station under construction that would be capable of screening and inspecting vehicles that arrive in the area of the BSL-4 lab building using both guards and technical equipment.

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

noted that the three BSL-4 labs with all or nearly all of our 15 key controls were subject to additional federal security requirements outside the purview of the Select Agent Regulations. For example, the National Institutes of Health both funds research requiring high containment and provides guidance and requirements that are widely used to govern many of the activities in high-containment labs. Other examples of more stringent regulations for BSL-4 labs include those of military labs that also follow far stricter Department of Defense physical security requirements. For example, Lab B had several layers of security, including a perimeter security fence and roving patrol of armed guards, visible inside and outside the perimeter fence. Although these security controls are not necessary for BSL-4 labs registering with DSAT, Lab B utilized these security controls to comply with more stringent federal requirements imposed by the agency owning the facility and incorporated these controls into its security plan. Security officials at the two labs with fewer security controls (Labs C and E) told us that management and administration had little incentive to improve security because they already met DSAT requirements. Some security officials also suggested that budgetary restrictions limited attempts to make security improvements.

Conclusions

Although numerous factors influence the security of a facility, two of the BSL-4 labs we assessed were lacking key perimeter security controls even though they met DSAT requirements. Our observation that the three labs with strong perimeter security all were subject to additional federal oversight outside of the DSAT program leads us to conclude that minimum specific perimeter security standards would provide assurance that all BSL-4 labs are held to the same security standard. Given that many new BSL-4 labs are under construction and will come online over the next few years, it is important for DSAT to ensure that there is no “weak link” in security among the nation’s BSL-4 labs.

Recommendation for Executive Action

To further enhance physical perimeter security at BSL-4 labs regulated by DSAT, we are recommending that the Director, CDC, take action to implement specific perimeter security controls for all BSL-4 labs to provide assurance that each lab has a strong perimeter security system in place. The CDC should work with USDA to coordinate its efforts, given that both agencies have the authority to regulate select agents.

Agency Comments and Our Evaluation

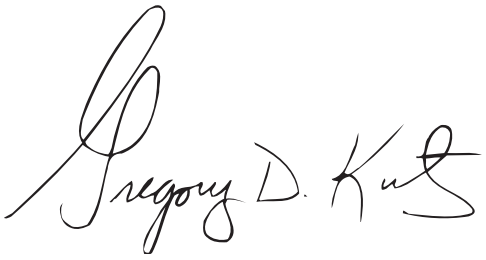
We received written comments on a draft of this report from the Assistant Secretary for Legislation of HHS. HHS agreed that perimeter security is an important deterrent against theft of select agents. They indicated that the difference in perimeter security at the five labs was the result of risk-based planning; however, they did not comment on the specific vulnerabilities we identified (e.g., an unsecured loading dock at one building housing a BSL-4 lab) and whether these should be addressed. In regard to requiring specific perimeter controls at all BSL-4 labs, HHS stated that it would coordinate with APHIS to seek input from physical security experts and the scientific community; the regulated community; professional associations; State, local, and tribal officials; and the general public as to the need and advisability of requiring, by Federal regulation, specific perimeter controls at each registered entity having a BSL-4 lab. They explained that specific security controls are not in place because Select Agent Regulations are focused on performance objectives rather than specific methods of compliance. We are encouraged that HHS plans to study this matter further, and suggest that, as part of this study, HHS reconsider whether the lack of many specific perimeter security controls at two of the nation's five BSL-4 labs is acceptable.

HHS also requested that we provide references for the research that identified our 15 security controls as being appropriate for the assessment of the perimeter security of BSL-4 labs, identify the security experts that we consulted, and indicate whether these 15 security controls had been peer reviewed. We have notified HHS that we will work with them to understand the controls in more detail. As discussed in our report, we developed the 15 security controls based on our expertise in performing security assessments and our research of commonly accepted physical security principles. These principles are reflected in the security survey tool we used to evaluate each of the five BSL-4 labs. We have used this survey tool for similar security assessments in the past. Although we acknowledge that the 15 security controls we selected are not the only measures that can be in place to provide 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. Many of these controls—such preventing direct access to a lab via windows, or ensuring visitors are screened prior to entering a building containing a BSL-4 lab—are common-sense security measures.

HHS also provided us with technical comments, which we incorporated as appropriate. HHS's comment letter is reprinted in appendix II.

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 the CDC, and other interested parties. The report will also be available at no charge on the GAO Web site at http://www.gao.gov.

If you or your staff have any questions concerning 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 III.



Gregory D. Kutz
Managing Director
Forensic Audits and Special Investigations

Appendix I: Perimeter Security Controls

To perform our perimeter security assessment of biosafety level (BSL) 4 labs, we identified 15 key perimeter security controls, based on our expertise and research of commonly accepted physical security principles, that contribute to a strong perimeter security system. A strong perimeter security system utilizes 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 2 shows 15 physical security controls we focused on during our assessment work.

Table 2: 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, similarly 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.
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 ID check and vehicle inspection, to deny unauthorized individuals access and potentially detect a threat.

No.	Perimeter physical security control	Rationale
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: Comments from the Department of Health and Human Services

DEPARTMENT OF HEALTH & HUMAN SERVICES OFFICE OF THE SECRETARY

Assistant Secretary for Legislation
Washington, DC 20201

SEP 05 2008

Gregory D. Kutz
Managing Director
Forensic Audits and Special Investigation
Government Accountability Office
441 G Street NW
Washington, DC 20548

Dear Mr. Kutz:

Enclosed are the Department's comments on the U.S. Government Accountability Office's (GAO) draft report entitled: "Biosafety labs: Perimeter Security Assessments of the Nation's Five BSL-4 Laboratories" (GAO-08-1092).

The Department appreciates the opportunity to review and comment on this report before its publication.

Sincerely,

Jennifer R. Luong for
Vincent J. Ventimiglia, Jr.
Assistant Secretary for Legislation

Attachment

COMMENTS OF THE DEPPARTMENT OF HEALTH AND HUMAN SERVICES (HHS) ON THE U.S. GOVERNMENT ACCOUNTABILITY OFFICE'S (GAO) DRAFT REPORT ENTITLED, "BIOSAFETY LABS: PERIMETER SECURITY ASSESSMENTS OF THE NATION'S FIVE BSL-4 LABORATORIES" (GAO-08-1092)

The Centers for Disease Control and Prevention (CDC) appreciates the opportunity to review and comment on the Government Accountability Office's (GAO) Draft Report: "Biosafety Labs: Perimeter Security Assessments of the Nation's Five BSL-4 Laboratories" (GAO-08-1092). Thank you for your review of this important issue.

GENERAL COMMENTS

Perimeter Security Just One Component of Overall Select Agent Security

As noted in your January 22, 2008 letter notifying CDC of this investigation, GAO conducted a limited security assessment of the nation's Biosafety Level (BSL) 4 laboratories that focused on each facility's outer perimeter security features, command and control center, and responsible personnel.

While CDC agrees that perimeter security is an important deterrent against theft of select agents[1], the Select Agent Regulations (42 CFR Part 73, 7 CFR Part 331, 9 CFR Part 121) require that entities registered for possession, use, and transfer of select agents take a comprehensive approach to securing select agents. Biosecurity experts describe the basic components of biosecurity as physical security, personnel security, information security, transport security, and material control and accountability.[2] The security provisions of the *Select Agent Regulations* reflect this comprehensive approach to securing agents. The regulations contain more than 20 requirements that entities must implement to protect agents from theft, loss, or release. The provisions include:

- Limiting access to buildings with select agents (e.g., guard station at the building entrance, locks on doors, card access system, biometric system, or intrusion detection system);
- Limiting access to laboratory rooms with select agents (e.g., locks on doors, card access system, biometric system, or intrusion detection system);
- Limiting access to select agents inside the room (e.g., locks on laboratory equipment (incubators, refrigerators, and freezers), locked boxes inside laboratory equipment (incubators, refrigerators, and freezers), biometric system, card access system, and intrusion detection system);
- Monitoring access to areas where select agents are used or stored (e.g., electronic logs of access, manual sign in logs, and video camera surveillance);
- Maintaining accurate, current inventory records for all select agents held in long-term storage; and
- Providing information and annual training to each individual who will have access to select agents.

[1] "Select agents" are biological agents (viruses, bacteria, fungi, prions, etc.) and toxins that have the potential to pose a severe threat to public health and safety, to animal or plant health or to animal and plant products. The agents and toxins are defined by lists that appear in sections §73.3 and §73.4 of the HHS/CDC *Select Agent Regulations* (42 CFR Part 73) and section §121.3, §121.4, and §331.3 of the USDA/APHIS *Select Agent Regulations* (7 CFR Part 331 and 9 CFR Part 121).

[2] Sandia National Laboratories. *Laboratory Biosecurity Handbook.* Albuquerque, NM: Sandia National Laboratories; 2007. Available at: http://www.biosecurity.sandia.gov/home.html.

1

COMMENTS OF THE DEPPARTMENT OF HEALTH AND HUMAN SERVICES (HHS) ON THE U.S. GOVERNMENT ACCOUNTABILITY OFFICE'S (GAO) DRAFT REPORT ENTITLED, "BIOSAFETY LABS: PERIMETER SECURITY ASSESSMENTS OF THE NATION'S FIVE BSL-4 LABORATORIES" (GAO-08-1092)

CDC notes that GAO did not assess the security of the laboratories themselves or the threat of an insider attack. The GAO limited security assessment focused only on the perimeter security leading up to the laboratory building points of entry. CDC recommends that the final report include additional clarification of how perimeter security fits into overall select agent security.

Overall Security Measures are Based on Specific Conditions at Each Laboratory

The GAO draft report is correct that there are significant differences in perimeter security among the five entities that maintain BSL-4 laboratories. However, this is because there are significant differences in the risk present at each of the five registered entities, which vary not only by physical plant and location, but by the agents possessed and how those agents are used and stored.

The report is also correct that the Select Agent Regulations are not prescriptive, "one size fits all" requirements but are performance standards. Presidential Executive Order 12866, as amended, requires that "each agency shall identify and assess alternative forms of regulation and shall, to the extent feasible, specify performance objectives, rather than specifying the behavior or manner of compliance that regulated entities must adopt." E.O. 12866, as amended, section 1(b)(8).

Wide Range of Expertise Used to Develop Select Agent Security Guidance

The Select Agent Regulations are implemented jointly by the Department of Health and Human Services (HHS)/CDC and the U.S. Department of Agriculture (USDA)/Animal and Plant Health Inspection Service (APHIS). As noted earlier, the Select Agent Regulations require a comprehensive approach to select agent security, focusing on security measures beyond just perimeter security. This holistic approach to select agent security has been developed by CDC and APHIS through a comprehensive and deliberative process, involving critical stakeholders and experts in the law enforcement, security, and laboratory communities.

In March 2006, CDC, in coordination with APHIS, hosted a meeting of physical security experts as a first step in the development of guidance that would assist entities in complying with the physical security requirements of the Select Agent Regulations. The meeting included representatives from the regulated entities, associations that represent laboratories, the Department of Justice, the Federal Bureau of Investigation, Department of Homeland Security, HHS/Office of Emergency Operations and Security Programs, CDC, the National Institutes of Health, the Department of Defense, and the USDA. As a result of the input from this meeting, CDC and APHIS released a Security Information Document and Security Plan Template to assist registered entities in complying with the physical security requirements of the Select Agent Regulations. These guidance documents are available at: http://www.selectagents.gov/complianceAssistance.htm.

Criteria Used to Select the 15 Security Controls Assessed by GAO

In this investigation, GAO used 15 security controls to assess the perimeter security of the five BSL-4 laboratories; however, CDC is not aware of research identifying these specific 15 security controls as appropriate for the assessment. GAO states that these security controls were selected for assessment based on "GAO expertise and research of commonly accepted physical security principles." So that the report's findings can be considered in the appropriate context, CDC encourages GAO, in the final report,

2

COMMENTS OF THE DEPPARTMENT OF HEALTH AND HUMAN SERVICES (HHS) ON THE U.S. GOVERNMENT ACCOUNTABILITY OFFICE'S (GAO) DRAFT REPORT ENTITLED, "BIOSAFETY LABS: PERIMETER SECURITY ASSESSMENTS OF THE NATION'S FIVE BSL-4 LABORATORIES" (GAO-08-1092)

to provide references for the research that identified these 15 security controls as being appropriate for the assessment of the perimeter security of BSL-4 laboratories, identify the security experts that had been consulted in developing the list of security controls to use for the assessment, and to indicate whether the use of this set of security controls for perimeter security assessments has ever been peer-reviewed.

Agency Response to GAO's Recommendation:

In the draft report, GAO recommends that, "the Director, CDC, take action to implement specific perimeter security controls for all BSL-4 labs to provide assurance that each lab has a strong perimeter security system in place. CDC should work with USDA to coordinate its efforts, given that both agencies have the authority to regulate select agents." (CDC notes that the recommendation language differed slightly in the opening letter and in the text of the report; the quotation above is from the text of the report.) CDC appreciates GAO's commitment to improving security at laboratories across the nation and agrees that perimeter security is an important component of overall select agent security.

Based on the findings and recommendation in the draft report, CDC will, in coordination with APHIS, seek input from physical security and scientific community, the regulated community, professional associations, State, local, and tribal officials, and the general public as to the need and advisability of requiring by Federal regulation specific perimeter control(s) at each registered entity having a BSL-4 laboratory. Using the GAO's list of four goals of a strong perimeter security system and 15 perimeter physical security elements as a starting point, we will seek input as to the:

- Specific perimeter controls that would be appropriate for a facility which includes a BSL-4 laboratory;
- Estimated initial and long-term cost for select agent registered entities to implement those controls; and
- Impact, if any, upon the availability of select agents for research, education, and other legitimate purposes.

This will allow CDC and APHIS to synthesize and benefit from the advice and expertise of security experts and the regulated community in considering which physical security enhancements are most appropriate for improvement of overall select agent security. The CDC also will seek advice on this matter from other Federal Departments and Agencies. The CDC is committed to enhancing security at our nation's BSL-4 laboratories based on risk and sound science, while balancing security enhancements against any impact on the important research being conducted by these laboratories.

Our technical comments on the draft report are provided in the attachment. We appreciate your consideration of the comments contained in this memo and the technical comments as you develop the final report. We are happy to discuss any of these comments with you.

3

Appendix III: 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; Verginie Amirkhanian; Randall Cole; John Cooney; Elizabeth Isom; Barbara Lewis; Jeffrey McDermott; and Andrew McIntosh.

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, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "E-mail Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, DC 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

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