Office of Infrastructure Protection's Biosecurity Assessments and Activities

prepared for:

The 2nd Annual Select Agent and Toxin Conference

August 2009

Homeland Security

FOR OFFICIAL USE ONLY

Vulnerability Assessment Authorities

- Homeland Security Presidential Directive-7 (HSPD-7) and the National Infrastructure Protection Plan (NIPP) require DHS to identify, prioritize, and coordinate the protection of critical infrastructure and key resources (CIKR).
  - DHS is responsible for ensuring that comprehensive vulnerability assessments are performed for nationally critical CIKR, and conducting or supporting vulnerability assessments that address the specific needs of the NIPP's comprehensive approach to CIKR protection.
- The Senate Appropriations Committee Report to the Consolidated Security, Disaster Assistance, and Continuing Appropriations Act, 2009 (P.L. 110-329) directs DHS to report to the Committee by March 20, 2009, on the progress made to expand vulnerability assessment capacity.

Homeland Security

Site Assistance Visits

- Collaborative process for conducting information-gathering visits and providing security recommendations at high-risk sites.
- Conducted by DHS in coordination and collaboration with other Federal, State, and local government entities, and CIKR owners and operators.
- Increases owner/operator awareness of vulnerabilities and provide options for enhancing protective measures to reduce vulnerabilities.
- Provides detailed reports to private sector partners – used to make security enhancements.
- Information informs sector-based Characteristics and Common Vulnerabilities (CV), Potential Indicators of Terrorist Activity (PI) and Protective Measures (PM) reports.
- Conducted eight SAVs on BSL 3 and 4 laboratories.

Buffer Zone Protection Program

- DHS-administered grant program to help local law enforcement and CIKR owner/operators increase security within site "buffer zones," the area outside of a facility that can be used by an adversary to conduct surveillance or launch an attack.

- Provides a coordinated process to identify and assess vulnerabilities, conduct security planning, implement preparedness activities, coordinate protective measures, and obtain mitigation equipment needed to enhance security.

- Annual grant program provides $50 million to approximately 200 facilities of national significance.

- Since FY04, approximately $300 million in BZPP grants distributed to State and local law enforcement to purchase authorized equipment to enhance protection capabilities in the buffer zone of the identified facility.

- Completed 25 BZPP assessments on BSL 3 and 4 laboratories and provided over $4.3 million of grant funds to local law enforcement agencies.

Homeland Security

Vulnerability Assessment Teams

- Federal Team Lead (FTL) / Protective Security Advisor (PSA):
  - Provides leadership, instruction, and direction to the team;
  - Monitors the quantitative and qualitative results;
  - Focuses on internal and external requirements; and
  - Coordinates documentation.

- **CBRNE Specialists (optional)**
  - Conducts analysis and mitigation based on a balanced assessment;
  - Works closely with sites to identify and understand explosion hazards; and
  - Conducts 3-D Blast and Plume Modeling.

- Physical Security / Assault Planning Specialists:
  - Identifies weaknesses and vulnerabilities;
  - Incorporates a risk-based approach; and
  - Develops Buffer Zone Plans.

- Infrastructure Interdependencies and Systems Analysts:
  - Designs risk analysis for engineering systems.
  - Provides subject matter expertise:
    - Infrastructure interdependencies;
    - Operation processes; and
    - Computer-based systems and reliability modeling.

Partnership with National Guard Bureau

- DHS and DoD signed a Memorandum of Agreement (MOA) to leverage the capabilities of the National Guard (NG) and the West Virginia National Guard Joint Interagency Training and Education Center (JITEC) to conduct vulnerability assessments.

- Ten teams from 9 states involved in the program.
  - NV, OR, WA, TX, GA, VA, MI, MN and WV.

- DHS/NG teams have conducted over 200 vulnerability assessments since FY08.
  - GA team conducted August 2008 CDC SAV.
  - TX and VA teams conducted December 2008 SFBR SAV.

- Potential increase of 10 additional teams in FY09.

Infrastructure Protection Report Series (IPRS)

- Increase awareness and improve understanding of infrastructure protection

Characteristics and Common Vulnerabilities

- **Common Characteristics**
- **Consequences of Events**
- **Common Vulnerabilities**

Potential Indicators of Terrorist Activity

- **Surveillance Indicators**
- **Surveillance Objectives**
- **Transactional and Behavioral Indicators**

Protective Measures

- **General Protective Measures Options**
- **Specific Protective Measures Options per HSAS Level**

- Combined Protective Paper and two-page summer report on BSL-4 laboratories.

Homeland Security

Common Vulnerabilities

- No security director as an executive staff member (sole function).
- No established security protocols in response to unusual incidences.
- No screening of packages or vehicles entering facility.
- Inadequate relationship between first responders in consideration to exigent circumstances requiring emergency response to facility.
- Insider threat to facility operations.
- Potential for stealing or diverting agents during shipping and transfers.
- Inconsistent background checks on employees that do not have “entry” access to BSL laboratory.
- No annual or semi-annual updates of background checks for laboratory personnel.
- Co-location of laboratory with other facilities-full access to facility can be gained.
- Inconsistent security procedures across facilities.
- Perimeter security inadequate or in need of repair/replacement.
- No procedure for “non-existing” badge challenges.

Homeland Security

Recommended Protective Measures

- Designate security director to develop, implement, and coordinate security related activities.
- Develop a comprehensive security and emergency response plan.
- Establish liaison and regular communication with local law enforcement and emergency response officials.
- Conduct background checks on all employees and establish procedures for reporting change of life information (bankruptcies, divorce, marriage, etc).
- Incorporate security awareness and response procedures into new employee training.
- Install intrusion detection systems in sensitive areas.
- Provide adequate locks, gates, doors, and other barriers for designated secure areas.
- Install barriers at HVAC systems, hatches, and power substations.
- Implement adequate policies and procedures for cyber and control systems security.
- Immediately cancel all access to terminated staff (employees and contractors).
- Develop and maintain emergency response plans, notifications process, and calling procedures.

Executive Order

- **E.O. 13486 "Strengthening Laboratory Biosecurity in the United States"**
  - Issued on January 9, 2009 after WMD Commission Report.
- **Established a Working Group**
  - To ensure that facilities that possess biological select agents and toxins have appropriate security and personnel assurance practices to protect against theft, misuse, or diversion to unlawful activity.
- **Working Group tasked to provide a Report to President within 180 days**
  - Report will include a summary of existing laws; recommendations for new legislation; options for establishing oversight mechanisms; and a comparison of the range of existing security programs compared to security programs in other fields and industries.
- **Created interagency sub-working groups**
  - Review and analyze current regulations, policies, procedures, and other documents
  - Identify gaps in current regulations, policies, procedures, and practices
  - Recommend ways to strengthen biosecurity

Homeland Security

DHS Full/Sub-Working Groups Participation

- **Full Working Group Representation**
  - Representatives from DHS/Office of Health Affairs represent DHS at the senior-level
  - Dr. Tillman Jolly (Assistant Chief Medical Officer)
- **Physical Security Sub-Working Group**
  - DHS Office of Infrastructure Protection co-chairs with Department of Defense
  - DHS Office of Infrastructure Protection/ISC
  - DHS Office of Security
  - DHS Chief Security Officer-Plumb Island
- **Transportation Security Sub-Working Group**
  - DHS Transportation Security Administration
  - DHS Office of Infrastructure Protection

Homeland Security

DHS Sub-Working Groups Participation (con't)

- **Select Agent Rule Sub-Working Group**
  - DHS Office of Infrastructure Protection's Homeland Infrastructure Threat and Risk Analysis Center (HITRAC)
  - DHS Office of Health Affairs
- **Personnel Security/Reliability Sub-Working Group**
  - DHS Office of Infrastructure Protection's Infrastructure Security Compliance Division
  - DHS Office of Security

Future Initiatives

- **Memorandum of Agreement**
  - In efforts to further the BSL security initiatives, IP executed a Memorandum of Understanding (MOU) with CDC, US Department of Agriculture's Animal and Plant Health Inspection Service (APHIS), and FBI concerning the sharing of select agent facility location and toxin information.
  - IP's Infrastructure Information Collection Division (IICD) received the facility lists from CDC and APHIS and developed a way forward for obtaining the data in database format.
  - IP will continue to work with CDC and APHIS to obtain data clarification and analyze information in a risk-base manner.
- **S&T and IP Coordination**
  - IP Security Specialists have provided subject mater expertise (SME) to S&T site visits to offer security assistance in the form of a Site Assistance Visit.
  - IP has provide program overviews during two S&T visits since January 2009. IP continues to support this effort and provide SME support to S&T.