XXX Site threat/risk assessment:

Conducted: 02/2013
Revised: 03/2013

XXX Technologies, Inc. is a pharmaceutical company specializing in developing therapeutic solutions for some of the most lethal disease-causing pathogens - smallpox, Ebola, dengue, Lassa fever and other dangerous viruses. XXX is located at 4575 SW Research Way, in XX XX.

The XX, XX laboratory facility currently employs **65** full time personnel. The New York financial office currently employs **9** full time personnel. In XX, XXX currently leases **18,127** square feet of space, in a building occupied by multiple tenants. XXX in XX added an additional **16,000** square feet of office and lab space in 2012, with construction pending. XXX has developed a security master plan and policies and procedures for the overall protection of personnel, information, data, consultants, and subcontractors associated with XXX programs. **Reference Appendices A-FF**

Assessment Conducted By: Victor N. Allen

The site risk assessment was conducted by Victor N. Allen – XXX Director of Security. This assessment was updated on 25 March 2013. My back ground includes over 11 years in law enforcement and more than 13 years of security operations management.

References:

Natural Disaster threat information in this document was obtained using the following resources; XX Extension Services site covering Natural Disaster Preparedness, The XX Department of Geology and Mineral Industries, and a reference guide by NAME Author of over a dozen books on XX History and the author of XX's Natural Greatest Natural Disasters in which he talks about earthquakes, forest fires and tsunamis among other natural disasters that have occurred in XX over its entire settled history.

Crime Information was obtained using information from the XX Police Department-Monthly and Quarterly Crime Analysis Reports.

Other information included in this report are a result of regular site inspections, and security strategy planning sessions with XXX senior management and various vendors of physical security services in XX (SAC). I follow some general standards and guidelines found in the ANSI/ASIS Standards and Guidelines, as well as information as a result of "CAP Index®" reviews for our site.

Purpose

The purpose of the site risk assessment is to provide a local approach in line with and in support of a national approach to prevention, mitigation, and response to various threats and emergencies that may affect XXX.

The main threats to XXX's XX facility involve physical, electronic, and human risk elements. The Master Security Plan and Crisis Management Team Responsibilities Guide which are housed on the XXX R: drive and are accessible to all management team members provide an overview of

XXX, XX, OR
Tel: Fax: XXX.com

responsibilities for handling threats and risk (updated 02/2013). Threats, risks or emergencies that may result in the implementation of these procedures include; criminal threats; terrorist threats; industrial espionage; natural disasters; and potential loss of critical infrastructure. This includes the security interests of people, equipment, information, and property.

Since threats vary and emergencies may be sudden and without warning, XXX's policies and procedures are designed to be clear and simple in order to accommodate contingencies of various types and magnitudes.

Criminal Threat

Criminal risks at XXX, both internally and externally, are moderate, and include potential larceny-theft to include burglary. XXX receives regular crime data from the XX Police Department. The most recent report for February 2013 shows "Larceny" has the highest number of offense committed in the city. XXX's expXXre to Larceny would generally occur internally, though external thefts/burglaries in XX have shown a slight decrease in the past year, particularly in the area of burglaries to businesses in the Technology in the city.

XXX continues to address this and other potential after hours forced entry threats by installing an alarm system that includes motion detection sensors, individual door access sensors and 13 CCTV cameras that provide coverage of all entrances and exits to the facility. The alarm system is monitored 24/7/365 and the service provides police response as well as simultaneous alerts to designated XXX personnel. XXX added 1 additional HD-CCTV cameras to the exterior of the facility in December of 2012, which provides a view of activity that could adversely affect XXX. This additional camera is directed at XXX's 2nd back up power generator that is fully fenced and contains signage appropriate to advise passersby.

Due to the location of the property and multi-tenant occupancy, the building and surrounding property where XXX resides have no exterior fencing and will remain an open campus concept. There is a contingency plan that awaits landlord and multi-tenant support to add cameras that specifically monitor incoming and outgoing traffic to all facility parking areas. Additional exterior building lighting is currently being added.

Terrorists Threats

XXX will follow the Department of Homeland Security (DHS) National Terror Advisory System (NTAS) guidelines for handling terror alerts:

When a threat develops that could impact XXX we will advise all affected personnel. We will provide whatever information we can so they know how to protect themselves, their families and their communities. Under the new two tiered system by the DHS, XXX will coordinate with local authorities to issue formal detailed alerts regarding information about a specific or credible threat.

XXX will also deploy the guidance provided in its Threat/Emergency Response procedure and the Crisis Management Team Response Guide to help organize its efforts in response to these types of threats.

XXX, XX, OR
Tel: Fax: XXX.com

Industrial Espionage

Initially, XXX takes precautions to avert Industrial Espionage crime by conducting detailed and thorough background investigations and repeating that background investigation every 5 years. All XXX background checks are "Executive" level. Everyone (employees, contractors, vendors) receive the same background check, which covers 10 years for employment and driver's license/Department of Motor Vehicles checks. XXX uses the E-Verify system operated jointly by the Department of Homeland Security and the Social Security Administration to confirm employment eligibility for all new hires. Criminal history checks are conducted for employment addresses and education addresses submitted to XXX covering 7 years. Verification is conducted on each individual's past three addresses as provided by the SSN search. Once counties are identified for the candidate's education, employment, and residence address history, HR Plus (XXX's designated service provider) submits the county searches and receives a minimum of 7 years of history check. Citizenship and DOB are covered in the I-9 done upon hire.

Additionally, XXX will use annual and biennial Cap Index®, Crime Cast® report to provide threat risk analysis. These reports will include proximity reports that assist us with identifying potential threats in our surrounding area that may have an impact to our business operations, Citywide Maps® detailing risk of crime in a geographic area, and Industry Benchmarks® that identify crime risk for specific industries. XXX currently receives regular crime updates from local law enforcement.

Information Technology Security risk of industrial espionage is addressed using automated systems that monitor various aspects of the information systems security implementations include intrusion detection and prevention, managed antivirus software, environmental monitoring and system/network monitoring. All automated systems notify the appropriate personnel when problems arise so they can be addressed immediately.

Natural Disaster

Natural disasters in XX include; earthquakes, forest fires and tsunamis. Power outages as a result of any of these disasters are common. XXX has backup generators to address power outages and will follow the Master Security Plan and Crisis Management Team Responsibilities Reference Guide as guidance tools. The Cap Index® REDFLAG® Risk ExpXXre Analysis will be used in advance of an event to evaluate XXX's relative risks and vulnerabilities to these and other natural threats.

Potential Loss of Critical Infrastructure

XXX's critical infrastructure is potentially vulnerable to cyber-attack. However, XXX deploys automated systems that monitor various aspects of the information systems security implementations include intrusion detection and prevention, managed antivirus software, environmental monitoring and system/network monitoring. All automated systems notify the appropriate personnel when problems arise so they can be addressed immediately.

XXX has implemented steps to further secure its physical facilities by bring the building access control system in-house. XXX has installed CCTV cameras covering all exits and entrances to the facility that are monitored and has DVR recordings that are maintained for at least 30 days by the director of security. XXX has plans to increase lighting on the exterior and perimeter of the building

XXX, XX, OR
Tel: Fax: XXX.com

and to place fixed and point tilt zoom cameras around the perimeter of the building. XXX has 24/7 building alarm monitoring and response and motion sensor detection and system security.

Incident Response

In response to recent events regarding drum seals with XXX/BARDA product in transport. XXX has reached out to all CMO's to assess, review and provide training for handling, and managing an incident or event of significance. A complete report of the incident has been provided to BARDA and XXX has also responded to additional conditions that BARDA requested to be addressed for all XXX/BARDA products going forward. These reports have been thoroughly reviewed by XXX and BARDA and have been processed and approved as appropriate steps taken to mitigate future risks.

Summary/Recommendations

XXX will continue to monitor local crime statistics through liaison with local law enforcement, and by maintaining additional information from Infragard. XXX maintains Cap Index® Crime Reports® as risk analysis tools, and will continue to provide physical and information security alerts using ASIS security management daily briefs. XXX maintains a knowledgeable and experienced security director to review, develop, implement and train all personnel on new security policies and procedures.

XXX's annual security training includes organizational change presented by our Chief Scientific Officer and laboratory specific safety training provided by the Director of Security. XXX's Crisis Committee Team meets quarterly to discuss and plan for risk which includes table top exercises to strengthen our ability to respond to events. XXX maintains a dynamic approach to effective security management and will assess risk on an ongoing basis using the listed tools to assure that we maintain the highest levels of protection for all of our assets.

Current Risk Mitigation Plan items for 2013;

- Review access policy and number of entrances available
- Review access to main office and require visual inspection of ID for all non –XXX visitors
- Review Alarm Policy and consider individual alarm access codes
- Review Lab security and consider tighter security around lab and or freezer access
- Consider Communications restrictions for media events to designated personnel

XXX, XX, OR
Tel: Fax: XXX.com