COUNTER TERRORISM
NEW YORK STATE DIVISION OF HOMELAND SECURITY AND EMERGENCY SERVICES

Andrew M. Cuomo
Governor
Jerome M. Hauer, Ph.D, MHS
Commissioner

CRITICAL INFRASTRUCTURE PROTECTION AND RESILIENCE QUARTERLY NEWSLETTER

ISSUE #7 October 2014

DHSES Receives Distinguished 2014 Excellence in Public Service Award

Earlier this year, DHSES released the 2014-2016 State Homeland Security Strategy. The Strategy is a critical document which guides State and local homeland security planning and investments. It builds upon the lessons learned from Superstorm Sandy, Hurricane Irene, Tropical Storm Lee, and other major disasters, and it represents an evolution from traditional "all hazards" preparedness to preparing for catastrophic or worst case scenarios. This important document can be found here. DHSES and the members of the State Homeland Security Strategy development team have received recognition from the New York State Academy for Public Administration. The Excellence in Public Service Award is a highly coveted award as only a few public agencies receive such recognition each year. More information about the State Academy for Public Administration can be found here.

National Cyber Security Awareness Month

October 2014 marks the 11th Annual National Cyber Security Awareness Month.

National Cyber Security Awareness Month (NCSAM) is a nationally recognized effort sponsored by the U.S. Department of Homeland Security in cooperation with the National Cyber Security Alliance and Multi-State Information Sharing and Analysis Center to raise cyber security awareness across the country and to empower citizens, businesses, government and schools to improve their cyber security preparedness.

Taking part in NCSAM is possible in a variety of ways. Everything from adding a NCSAM signature to your emails to utilizing the #NCSAM hashtag can help spread awareness to your colleagues and fellow citizens. The New York State Office of Information Technology Services provides a variety of resources for this initiative including posters, downloadable materials, and useful links. All of these can be found on their NCSAM website located here.

ALSO IN THIS ISSUE...

America's Safe Schools Week

October 19-25, 2014 is America's Safe Schools Week, which is sponsored by the National School Safety Center, state governors and school superintendents. The goal of this campaign is to motivate key education and law enforcement policymakers, as well as students, parents and community residents, to vigorously advocate school safety. School safety includes keeping campuses free of crime and violence, improving discipline, and increasing student attendance. School that are safe and free of violence, weapons and drugs are necessary to ensure the well-being of all children and the quality of their education.

In preparation of America's Safe Schools Week the New York State Safe Schools Initiative is hosting a School Safety Planning webinar on October 16th. The New York State Safe Schools Initiative helps schools across the State implement effective school safety strategies and plans to enhance emergency preparedness. More information about the webinar as well as links to a variety of resources for first responders, schools, and parents can be found here.

November is Critical Infrastructure Security and Resilience (CISR) Month

This November we recognize the efforts of our State, Federal, and Local partners as well as our private sector partners and the work they do every day ensuring the security of New York State's Critical Infrastructure. We ask all of our partners to start planning how your organization will contribute to building awareness and understanding of the importance of Critical Infrastructure to America's national security and economic prosperity, as well as reaffirming the commitment to keep our Critical Infrastructure and our communities safe and secure. With this in mind, we would like to highlight partner success stories in security and resilience. Please feel free to share your own stories with us at CIP@dhses.ny.gov. Your Best Practice/Accomplishment may be highlighted in upcoming issues of this Newsletter.

John Layton Named Deputy Director of Operations for the Office of Emergency Management

Welcome and congratulations to John Layton, who was recently named the Deputy Director of Opera-tions of the New York State Office of Emergency Management.

John comes to DHSES from the Albany County Sheriff's Department where he served as the Commander of the Critical Incident Emergency Management Unit. In that capacity, he was the Emergency Manager for Albany County, overseeing the Fire Coordinator, Community Emergency Services, the Sheriff's Search and Rescue Team, and the Capital Region Forensic Haz-Mat Team. John has 28 years in public safety as a police officer, firefighter, EMT, Haz-Mat technician, rescue technician, instructor, and grant coordinator. John has been involved in emergency management since January 2001 and managed Albany County's response and recovery to Hurricane Irene, which was the largest disaster in Albany County history.

John's knowledge and experience in the field of emergency management will be a wonderful addition to the DHSES team.

The Department of Homeland Security Office of Infrastructure Protection and the Regional Consortium Coordinating Council Present: A Joint Critical Infrastructure Partnership Webinar Series

Each hour-long session is designed to assist critical infrastructure owners and operators, physical security and information security professionals, Chief Information Officers, risk managers, business continuity planners, information technology directors, and local homeland security and emergency management staff in their efforts to enhance the preparation, security, and resilience of communities and their critical infrastructure assets.

Upcoming Webinar:

Critical Infrastructure Security and Resilience November 18 & 20: Topics focus on tools and resources for improving the overall security of a critical infrastructure asset or facility:

- Public/Private Partnerships – A panel comprised of representatives from industry and local government will share innovative best practices from public/private partnerships they have collaboratively developed related to critical infrastructure security and resilience.
- Exercises – Learn from DHS and local critical infrastructure practitioners about scenarios and exercise plans that have been successfully developed to address the most salient threats to local communities, enhancing their ability to respond to and recover from all-hazard events.

Register here: http://www.govevents.com/word-redir.php?id=13965

Chemical Facility Anti-Terrorism Standards Advance Notice of Proposed Rulemaking

On August 18, 2014, the Department of Homeland Security published a Chemical Facility Anti-Terrorism Standards (CFATS) Advance Notice of Proposed Rulemaking (ANPRM) in the Federal Register. The ANPRM was available for public comment through October 17, 2014. As the Department continues to make significant progress and promotes program transparency, this ANPRM will provide an opportunity to hear and consider the views of the CFATS-regulated industry and other interested members of the public on their recommendations for program modification.

The Department is hosting a series of listening sessions across the country to allow stakeholders to comment in person. Additionally, two Webinars are scheduled for those who wish to provide verbal comments but cannot attend the in-person sessions. Dates, locations, and registration information can be found on the CFATS ANPRM registration page.

Comments can also be submitted through the Federal eRulemaking Portal or in writing to the U.S. Department of Homeland Security, National Protection and Programs Directorate, Office of Infrastructure Protection, Infrastructure Security Compliance Division, 245 Murray Lane, Mail Stop 0610, Arlington, VA 20528-0610.

For more information, email cfats@hq.dhs.gov or visit the CFATS Rulemaking Webpage.

Infrastructure Protection Gateway: Update

The Department of Homeland Security (DHS) Office of Infrastructure Protection (IP) has released the Infrastructure Protection Gateway (IP Gateway) to the states. Currently New York administrators are in the process of receiving training and reviewing system capabilities. Administrators will not be approving state, local, tribal, and territorial mission partner user access requests until a full review and assessment of the system has been completed.

When will the IP Gateway be released to users in New York?

The month of October has been identified for administrator review and assessment by state administrators. It is anticipated that user requests for system access will begin to be accepted in early November. All personnel who have requested to be informed on system availability and use will be notified when the administrators have opened the IP Gateway for access.

What can I do to prepare prior to requesting access?

All users requesting access to the IP Gateway will be required to have a valid Protected Critical Infrastructure Information (PCII) Authorization Number. To receive the PCII authorization or ensure your authorization number has not expired, you can visit the PCII website at https://pciims.anl.gov/pciims/Index.aspx. Additionally, all users will be required to communicate their "need to know" to justify access at the county or state level within the system.

Interim Critical Infrastructure Information submission process

Documents containing Critical Infrastructure Information can be submitted through the PCII Office eSubmission link at http://www.dhs.gov/submit-information. Once validated as PCII this process will provide submitters with a PCII number for their documents and attach PCII protections. For additional information and assistance with this process, send a request for assistance to the Critical Infrastructure Protection Inbox at CIP@dhses.ny.gov.

Understanding the Current Threat Environment

The current terrorism threat environment facing the United States and New York State is more diverse than any time since the attacks of September 11, 2001. Al-Qa'ida has evolved from a highly centralized organization into a broad movement composed of numerous affiliates and allies. Most recently, the former al-Qa'ida affiliate in Iraq – now known as the Islamic State – has launched a successful and brutal military offensive throughout Iraq and Syria. Efforts to detect, deter and prevent terrorist attacks have become more complex and difficult as a result of the increasingly decentralized and diverse evolution of the jihadi threat. The current danger to the U.S. homeland has grown significantly, whether from the Islamic State, seasoned al-Qa'ida planners and operatives, or similar groups or individuals who share a common ideology, and underscores the importance of a unified, comprehensive counter terrorism strategy which includes regional, state and local governments, and our federal partners.

Foreign fighters – individuals who have traveled to jihadist battlegrounds such as Syria, Iraq, Yemen, or Somalia to fight alongside terrorist groups are of increasing concern. Fighters possessing Western passports are of particular interest, due to their ability to travel to the United States and the concern that they may return home with improved capability and increased intent to launch homeland attacks. However, Homegrown Violent Extremists (HVE)—individuals inside the United States without ties to foreign terrorist groups, yet inspired to action by their violent rhetoric—remain the most persistent threat to the homeland. The April 2013 Boston Marathon Bombings demonstrates both the willingness of such radicalized individuals to conduct an attack, and the ability to acquire the means to do so.

History has demonstrated that the New York metropolitan region, with its large and diverse ethnic population and plethora of iconic, economic and cultural settings, has been disproportionately targeted by jihadist terrorism. According to analysis by the New York State Intelligence Center, nearly one-third of homeland plots since 9/11 targeted New York and New Jersey. Analysis of the current threat environment confirms and reinforces the assessment that the New York / New Jersey region will continue to remain a priority target.

Understanding the Insider Threat (Part 2)

Part 1 of the *Insider Threat* (CIPR Quarterly Newsletter, July 2014) provided an overview of this unique threat to an organization. It noted several key issues including the identification of critical assets and that peers and first line supervisors are best able to identify malicious insiders. One noted best practice was to "crowdsource" security. In other words, businesses should strive to develop an organizational culture where **security (like safety) is everyone's business.** Part 2 draws again on several sources including the recently published *"National Risk Estimate: Risks to U.S. Critical Infrastructure from Insider Threat"* (Dec. 2013, FOUO) and Carnegie-Mellon's updated *"Common Sense Guide to Mitigating Insider Threats, 4th Edition"* (May 2014) to briefly identify additional best practices for detecting and minimizing this threat. These are grouped under three areas: People, Policies and Procedures, and Tools.

People

Training/Education: All personnel need to be informed about the insider threat. A sampling of the many aspects of this issue that could be covered as part of routine security training might include:

- What are the common characteristics of an insider who has the skill and motivation to cause damage to the organization?
- What assets are considered sensitive and why?
- What are company policies regarding computer use and monitoring?
- What are employee and supervisor responsibilities?
- How do I report concerns?
- What privacy rights are applicable?

"Before Entering" – Screening New Employees Before Hiring: The first step in minimizing the insider threat is to not let him/her in the door! A key element of this is comprehensive screening of all employees before hiring including a review of their employment history and any "red flags" that warrant further review and discussion. A thorough review prior to employment is a key first step in minimizing this threat.

"While working" – Don't feed the problem. There are positive organizational steps that can be taken to minimize the motivation or desire of an individual to illegally profit or cause damage to an organization. Appropriate employee recognition programs that offer public praise aid in mitigating the insider threat motivated by ego. Providing avenues for employees to vent concerns and frustrations may help alleviate the insider threat motivated by disgruntlement. Managers should anticipate and manage negative issues in the work environment for example in a time of employee lay -offs.

Policies/Procedures

"When leaving" – Develop a comprehensive employee termination process: The literature on the insider threat has numerous examples of employee damage and theft in the weeks prior to and even after termination. Organizations must have comprehensive termination procedures including termination of access to sensitive material (keys, access badges, access to company intranet). Consideration should be given to restricting the access or increased monitoring of employees who are undergoing negative personnel actions which may provide the motivation to harm the company. Procedures must ensure that employees who have left the organization for whatever reason do not have access to shared networks and critical systems. Again, there are numerous examples of employees who continued to have access to sensitive company systems for months after being fired.

(continued on next page)

Insider Threat (*continued)*

Provide non-threatening, convenient ways for employees to report suspicious behavior: Employees should be encouraged to report suspicious behavior through a secure, (some would say anonymous) method. All employees should be periodically reminded that reporting security concerns is vital to protecting the company's future – in some ways protecting their own jobs.

Authorize users based on least access privilege and conduct periodic audits to detect inappropriately granted access or access that still exists from previous job roles/functions that should be removed: Organizations must know and continuously monitor who has access to restricted information and programs including strict password and account management policies and practices. This includes "temporary" access granted to private vendors or other organizations. Companies must enforce separation of duties and least privileges and institutionalize system change controls.

Require identification for all assets: Organizations should protect sensitive information like they protect sensitive property – by establishing controls to gain access. This could include access cards, passwords or inventory check out. Controls should identify who had access to critical company assets and when. An extreme example of this is nuclear weapons which require two-person, independent control to access.

Develop a formalized insider threat program: If the threat is real and the possible consequences significant, then all organizations should develop an insider threat program that identifies roles and responsibilities. This might include representation from the Human Resource, Information Technology, Operations, and Legal departments. Policies, procedures, education, and visibility are all responsibilities to be addressed. The group must address all aspects of the issue from the identification of critical assets to detection and prevention i.e. *How will the organization detect and prevent the unauthorized disclosure of information?* Response and recovery plans to an incident are also needed and might include implementing secure backup and recovery processes.

Tools

Deploy data centric, not system centric security: Watching all data, all the time is impossible from a resource standpoint. Watching select critical assets is more reasonable and appropriate. Organizations should focus time, attention, and resources on the highest value assets and work down from there.

Use available IT tools: There are numerous applications and programs including log correlation engine or security information and event management (SIEM) systems to log, monitor and audit employee actions. Programs can also routinely monitor computer networks for suspicious activity.

Monitor and control remote access from all end points, including mobile devices: Remote access to sensitive processes and information is a normal, and sometimes required, part of the IT architecture in an organization. Controls must be in place to effectively monitor remote access.

As discussed in Part I, the damage inflicted by a successful attack by a determined Insider may be significant. Acting on these recommendations will serve an organization well in minimizing the harm this threat may inflict. In addition, the establishment of strong countermeasures shows all employees that the company takes this unique threat seriously. In the end, successful companies inculcate a "security" mindset throughout all employees which is reinforced by leadership at the top and effective reinforcement by first-line supervisors. Simply put, security lapses, such as doors to secure areas left ajar, are quickly noted and corrected. Companies that embrace a strong security culture, including both physical and cyber components, are most likely to be effective in detecting and preventing an incident which may result in substantial harm to the organization.

We Want to Hear From You!

For feedback on this Newsletter and to suggest topics for upcoming Newsletters, email us at CIP@dhses.ny.gov