COUNTER TERRORISM

NEW YORK STATE DIVISION OF HOMELAND SECURITY AND EMERGENCY SERVICES

Andrew M. Cuomo, Governor
Jerome M. Hauer, Commissioner

CRITICAL INFRASTRUCTURE PROTECTION AND RESILIENCE QUARTERLY NEWSLETTER

ISSUE #3 October 2013

Reflecting on the Anniversary of September 11th

This quarter we are reminded of the tragic events that occurred in Lower Manhattan, the Pentagon, and Shanksville, Pennsylvania that saw the loss of so many American lives. In a statement issued on September 11th, Governor Andrew M. Cuomo said:

"It's hard to imagine that it's been 12 years. In some ways so much has changed and in some ways so much remains the same. Physically there has been much progress. The stunning memorial that has been built, office buildings that have been built, the Freedom Tower now an international symbol of New York's resilience."

Today, when we look at lower Manhattan and the area around the World Trade Center the progress Governor Cuomo describes can be seen everywhere. The 10th anniversary of the attacks saw the opening of the memorial plaza, featuring twin reflecting pools where the twin towers originally stood. This site has seen over 10 million visitors in the 2 years since and the underground museum associated with it will be opening in the spring of 2014.

However, this area will not just be a memorial to the past but a key to New York's economic future. 72-story office building 4 World Trade Center is expected to open this November adding 1.8 million square feet of office space to Lower Manhattan. This will be followed early in 2014 with the opening of 1 World Trade Center, already the tallest building in the Western Hemisphere. This landmark achievement will not be the end either as the World Trade Center transportation hub will be completed in 2015, 3 World Trade Center is expected to be completed in 2016, and 2 World Trade Center after that.

While the World Trade Center seems poised to thrive again, we must not forget to remain vigilant against the threat of those that wish to harm this country like it was over a decade ago. It is important that all citizens remember to be aware of their surroundings and report suspicious activity. Only the with the help of all New Yorkers, will we be able to prevent future terrorist attacks and ensure we never have to suffer through another day like September 11th.

ALSO IN THIS ISSUE...

Annual Event: Preparedness Month

Preparedness Month is a national effort, now in its ninth year, sponsored by the Federal Emergency Management Agency's (FEMA) Ready Campaign in partnership with Citizen Corps. It is designed to encourage Americans to take simple steps to prepare for emergencies in their homes, businesses, and communities. In advance of September's observance, the New York State Division of Homeland Security and Emergency Services (DHSES) and Department of Health (DOH) had been showcasing preparedness information at the New York State Fair. Over 11,000 people visited DHSES and DOH at the fair receiving thousands of books, brochures and other preparedness materials. State agencies have also taken multiple steps to increase resiliency, preparedness and response capabilities.

Basic steps to follow in advance of any disaster include having an emergency plan, stocking up on emergency supplies, and remaining cognizant of potential hazards that could impact where you live or visit – including obtaining information through local news outlets during an emergency. New Yorkers should also subscribe to NY- ALERT, the State's alert and notification system, and download its new mobile app, iAlertz. To subscribe, visit www.nyalert.gov or www.ialertz.com.

New York State has also developed a website, available year round, to guide citizens to prepare for any type of incident at www.nyprepare.gov. This website serves as a clearinghouse of safety and preparedness information from the State agency websites of the DHSES, DOH, the State Police, the Department of Financial Services, and the Department of Agriculture and Markets, as well as the U.S. Department of Homeland Security, FEMA, and the American Red Cross.

Governor Andrew M. Cuomo announced on September 6th, that September is Preparedness Month across New York State. The Governor's proclamation can be viewed here.

DHSES Announces Addition to Senior Staff

DHSES is pleased to announce the addition of a new member to our senior staff. Dr. Pietro (Peter) D. Marghella joins DHSES as the Director of the Office of Emergency Management.

Dr. Marghella worked previously as a Professorial Lecturer at the School of Public Health and Health Services and as an Adjunct Professor School of Business at The George Washington University. He served for 20 years as a Medical Plans, Operations, and Intelligence Officer in the United States Navy, retiring as the Director of Medical Contingency Operations for the Office of the Secretary of Defense and is an expert on medical and public health preparedness and response for large-scale disasters and complex emergencies. His previous assignments include Chief of Medical Plans and Operations for the Joint Chiefs of Staff; Chief of Medical Plans and Intelligence for the US Pacific Command; and Chief of Medical Plans and Intelligence for the Office of the Chief of Naval Operations. Dr. Marghella is credentialed as a Certified Emergency Manager in the International Association of Emergency Managers, and is a Fellow in the American College of Contingency Planners (ACCP), which he Co-Founded and served as its first President.

FEMA Releases Guidance for Fire and EMS Operations During Active Shooter and Mass Casualty Events

Since 1999, there have been over 250 deaths in the United State attributable to active shooter incidents. Such events can occur in any community regardless of size or location. In order to adequately respond to these incidents it is essential that law enforcement, emergency medical services (EMS), and fire response have common tactics, communications, and standard operating procedures. To support fire and EMS in planning and preparing for these situations the US Fire Administration has released the *Fire/Emergency Medical Services Department Operational Considerations and Guide for Active Shooter and Mass Casualty Incidents*. This document serves to provide an overarching guide to preparing and responding to active shooter events specifically for EMS and fire personnel. Topics covered include, planning for casualty treatment, media relations, interagency practices, and post-incident demobilization among others. These are discussed in a manner that recognizes circumstances will make each such event unique. It is intended to be a living document, incorporating suggestions from local first responders in future editions. To view this document online please visit the USFA website located here.

DHS Announces New Insider Threat Training

The Department of Homeland Security (DHS) recently released an online independent study course titled *Protecting Critical Infrastructure Against Insider Threats*_(IS-915). The one-hour course was developed by the DHS Office of Infrastructure Protection (IP) in partnership with the Federal Emergency Management Agency (FEMA) Emergency Management Institute (EMI), Commercial Facilities Sector Specific Agency, critical infrastructure owners and operators, and other Federal and State agencies.

This is the sixth independent study course in the Critical Infrastructure Security Awareness Series developed by the DHS/IP and offered to government and private sector stakeholders through FEMA/EMI. The content covers a range of topics including defining insider threat; the scope and impact of insider threats; and identifying effective measures to counter insider threats. Designed for critical infrastructure employees and stakeholders, *Protecting Critical Infrastructure Against Insider Threats* enhances awareness of the potential threats to critical infrastructure from malicious actions taken by those inside the organization. The course also provides guidance on how to identify insider threats to critical infrastructure and an overview of common characteristics and indicators associated with malicious insiders. The course can be accessed by using the provided link:

http://www.training.fema.gov/EMIWeb/IS/courseOverview.aspx?code=IS-915

Partners Get Their First Look at NIST Draft of Voluntary Cybersecurity Framework

State and local partners, as well as private sector owners and operators, have begun the review process for the new voluntary Cybersecurity Framework. The need for a voluntary Cybersecurity Framework was highlighted in Executive Order 13636 (EO), which directed the National Institute of Standards and Technology (NIST) to develop the program. The EO calls for the framework to include a set of standards, methodologies, procedures, and processes that can inform the processes of responding to cyber risks in all phases — policies, business practices, and technology.

The framework is designed to assist government officials at all levels and private sector owner/operators by developing a common language for expressing, understanding and managing cyber resilience and security. This common language will allow for clearer descriptions of an organization's cybersecurity posture and target state, as well as to identify improvements, and assess progress. In addition, the framework uses industry standards and best practices as a means of enhancing critical infrastructure nationwide.

The Federal Government plans to make the framework flexible, cost-effective, and repeatable for owners and operators of all sizes. NIST plans to release the completed framework in February 2014, in accordance with the timeline laid out in the EO.

DHS to Add Cyber Assessments to Survey Tool

As part of the Federal Government's efforts to integrate cyber and physical resilience and security, the Infrastructure Survey Tool (IST) is gaining a cyber component.

The Cyber-IST is slated for release in February 2014 as part of the IP Gateway system. The tool will assist state, local, tribal, and territorial officials — as well as private sector owners and operators — gather data on their cybersecurity posture, and will also provide the basis for state and local cyber assessments.

The Cyber-IST is an update to the standalone tool that provides risk assessments for physical critical infrastructure assets.

Commercial Facilities Research and Development Working Group

The Commercial Facilities Sector partners face daunting challenges in finding products and tools that meet the security requirements of their diverse facilities and venues. Once compatible security products and tools are identified that meet their requirements; hardware and software costs, installation costs and staff training become financial considerations that stretch an organization's budgetary resources. Oftentimes, the security and protection requirements which they are seeking cannot be fulfilled to their specifications or they simply do not presently exist.

The Commercial Facilities Sector Specific Agency and DHS Science & Technology (S&T) Directorate, Commercialization Office have collaborated to form a Research and Development Working Group (RDWG). The RDWG will allow industry experts to play an active role in identifying requirements and gaps of technologies, products and services that exist within their sector; and attempt to locate existing products and/or programs that can fulfill those needs. Comprised of members from the Commercial Facilities Sector's eight subsectors, the knowledge and expertise that will be brought to this working group by those Subject Matter Experts will ensure that the needs and requirements of the industry will be addressed and conveyed to S&T. Once S&T receives feedback from the RDWG, they will begin the process of researching and evaluating products that meet those requirements.

RDWG had its Kick-Off Meeting in June 2013. If you have any interest in joining the RDWG Team, they can be reached at: CFSTeam@hq.dhs.gov.

NIPP Revision Nears the Final Draft Stage

After months of development, review, and revision, DHS is nearing its October 10 deadline for a final draft for the updated National Infrastructure Protection Plan (NIPP). With more than 1,000 comments submitted regarding the plan, DHS has been working to incorporate the perspectives of stakeholders, both in the public and private sectors.

The revised plan seeks to advance the security and resilience of critical infrastructure; maintain service continuity under adverse conditions; preserve public safety; and assisting communities and businesses in adapting to changing conditions and disruptions. The plan emphasizes the importance of public-private partnerships in developing enhanced security and resilience, and notes that there are eight attributes central to a successful collaborative effort. These include a defined purpose; clearly articulated goals; appropriate membership; leadership involvement; clear governance; robust communication; a trusted environment; and measurable outcomes.

Other key topics in the plan include an outline of the critical infrastructure strategic environment, the benefits of collaboration as a means of managing risk; and specific steps that can be taken to advance the national critical infrastructure security and resilience.

Key Differences

The following are some of the notable changes in the 2013 plan:

- Expansion of the central mission to include the concept of resilience
- Recognition of the role of cyber systems and assets as high-priority issues
- Emphasis on collaborative efforts in the critical infrastructure community as a means of managing both cyber and physical threats
- Acknowledgement of the Lifeline sectors — Water, Energy, Communications and Transportation — and the dependencies and interdependencies that other sectors have with the lifeline sectors

Nationwide Suspicious Activity Reporting Initiative

Efforts to address crime and threats in our communities are most effective when they involve strong collaboration between law enforcement and the communities and citizens they serve. It is essential that local, state, tribal, territorial, campus, and federal representatives are united in efforts to make our country safer. One of these efforts relates to Suspicious Activity Reporting. To address this issue, in 2011, the International Association of Chiefs of Police (IACP) hosted a meeting of representatives from numerous local, state, and federal agencies and law enforcement organizations to create a unified approach to reporting and sharing suspicious activity.

As a result, these leaders have partnered to support a strategy that will unify the efforts of all agencies and organizations involved in the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI). The NSI establishes standardized processes and policies that provide the capability for local, state, tribal, territorial, campus, and federal law enforcement to share timely, relevant Suspicious Activity Reports while working to ensure that privacy, civil rights, and civil liberties are protected. The overall effort focuses on (1) increasing public awareness of reporting suspicious activity to law enforcement, (2) generating Suspicious Activity Reports by law enforcement, (3) analysis conducted by fusion centers and Federal Bureau of Investigation (FBI) Field Intelligence Groups (FIGs), and (4) investigation by the FBI's Joint Terrorism Task Forces (JTTFs).

It is vitally important that law enforcement agencies conduct SAR training with all law enforcement personnel, including supervisors, and document completion. However, it may be just as important for emergency managers, private sector security, and other first responders to integrate SAR training into initial and recurring training curricula. More information, including online-based training, can be found at the NSI website here. Furthermore, through Operation Safeguard, New York State provides free, printable brochures including descriptions of suspicious activity and methods of reporting this behavior. These brochures are provided in a variety of languages and can be found here.

Reporting Suspicious Activity

- Agencies at all levels of government and infrastructure owner/operators should utilize the "If You See Something, Say Something™" program to raise public awareness of indicators of terrorism and to emphasize the importance of reporting suspicious activity to the proper law enforcement authorities, while protecting privacy, civil rights, and civil liberties.
- The public should contact law enforcement via 9-1-1 when an immediate response is needed regarding suspicious activity for any type of crime, including terrorism.
- All other tips and leads should be shared with the New York State Intelligence Center using the New York State Toll-Free Terrorism Tips Line: 1-866-SAFENYS (1-866-723-3697).

Applying CI Strategies to Nonprofit Locations

Community centers, parochial schools and other nonprofit organizations, often the bedrock of local communities, can benefit greatly from similar protection strategies and attention normally applied to Critical Infrastructure. This is especially true for faith-based organizations such as churches, mosques and synagogues which not only are soft-target facilities likely accessible to the public, but have a history of being targeted in attacks and plots. Despite the explicit and ongoing threats faced, many nonprofit locations have little resources and know-how to ensure they have adequate protection. Already operating on constrained budgets, it is hard for many nonprofits to make a priority of allocating scarce funds for security hardware, planning or dedicated security personnel.

Recognizing the vulnerability and target attractiveness of these types of facilities, the New York State Division of Homeland Security and Emergency Services (DHSES) regularly assists and coordinates with state-wide associations, umbrella groups and individual locations to ensure their constituencies and facilities are receiving appropriate guidance and support for their security initiatives. DHSES is also the State Administrative Agency for the annual Nonprofit Security Grant Program (NSGP) funded by the United States Department of Homeland Security. The NSGP provides target hardening grants to 501(c)3 organizations (nonprofits) in eligible Urban Area Security Initiative areas. DHSES personnel closely assist nonprofits in applying for and best utilizing these grant dollars.

Local law enforcement and emergency management agencies often provide assistance tailored for nonprofit and religious organizations as well. Depending on the capacity of the agencies this can include trainings, meetings, site-visits and more. Those individuals dedicated to the protection of Critical Infrastructure can also offer their valuable knowledge and expertise that is so desperately needed by nonprofit organizations. Encourage locations in your community to assemble a security committee and assist them in developing a relationship with their local police departments and first responders. Other available and useful resources are the other local organizations and nonprofits with the specific mission of assisting nonprofits and faith-based institutions improve their security levels and plan for emergencies. See http://www.dhses.ny.gov/oct/nfp/ for a list of some of these organizations and resources.

ASIS Certifications

Supported by federal funding sought in 2009, the New York State Office of Counter Terrorism Critical Infrastructure Team adopted the ASIS CPP® and PSP® certifications as a part of our professional development program and encourages our team to obtain and maintain board certification.

ASIS International is the leading organization of security management professionals, with more than 38,000 members and 230 Chapters worldwide. Members of ASIS International represent virtually every industry in the public and private sectors. Since 1977, ASIS International has set the standard for professional excellence in the security industry. ASIS International offers three certifications that provide an objective measure of an individual's knowledge, skills, and abilities: Certified Protection Professional (CPP) ®, Professional Certified Investigator (PCI) ®, and Physical Security Professional (PSP) ®.

The CPP® credential provides demonstrable proof of knowledge and management skills in eight key domains of security: security principles and practices, business principles and practices, investigations, personnel security, physical security, information security, crisis management and legal aspects. Those who earn the CPP® are ASIS board-certified in security management. The eligibility requirement for the CPP® is nine years of security work experience, with at least three of those years in responsible charge of a security function or a bachelor's degree or higher and seven years of security work experience, with at least three of those years in responsible charge of a security function.

The PCI® credential provides demonstrable proof of an individual's knowledge and experience in case management, evidence collection, and preparation of reports and testimony to substantiate findings. Those who earn the PCI® are ASIS board-certified in investigations. The eligibility requirement for the PCI® is a high school diploma or GED equivalent and five years of investigations experience with at least two years in case management.

The PSP® credential provides demonstrated knowledge and experience in threat assessment and risk analysis; integrated physical security systems; and the appropriate identification, implementation, and ongoing evaluation of security measures. Those who earn the PSP® are ASIS board certified in physical security. The eligibility requirement for the PSP® is a high school diploma, GED equivalent, or associate degree and six years of progressive physical security experience or a bachelor's degree or higher and four years of progressive physical security experience.

Thomas Vonier, CPP and Senior Regional Vice President of the ASIS International European Advisory Council stated "Earning a CPP, PCI or PSP, tells your colleges and employer that you possess substantial relevant experience, as well as demonstrated and tested competence … ASIS was the first organization to offer a credential specifically for security mangers and our program remains the global standard." Once certified, ASIS International requires continuing education requirements for recertification, offering assurance that practitioners will remain current will best industry practices. For more information about ASIS International Certifications, visit their website here.