NEW YORK STATE | Counter Terrorism

Andrew M. Cuomo
Governor
John P. Melville
Executive Deputy Commissioner

CRITICAL INFRASTRUCTURE PROTECTION AND RESILIENCE QUARTERLY NEWSLETTER

ISSUE #8 January 2015

NYS OCT Critical Infrastructure Unit 2014 in Review

2014 was a busy and successful year for the Office of Counter Terrorism's Critical Infrastructure Protection (CIP) Unit. The year started with two major initiatives from 2013 reaching their culmination. First was the successfully delivery of the Chemical Security Legislative Report, a statutory requirement of the unit to review and analyze chemical sector security throughout the State. The second was the Enhanced Visual Assessment Program (EVAP) team's support of New York City and the NFL during the Super Bowl. During this time, and the months leading up to it, the EVAP team successfully created virtual tours of event venues and surrounding infrastructure to assist first responders with their ability to prepare for any emergency.

Beyond the Super Bowl, the EVAP team continued to create a wide variety of products throughout the State and across sectors. Through the team's work in 2014, Infrastructure in sectors including Commercial Facilities, Energy, Transportation, Government Facilities, and Food and Agriculture now utilize EVAP products for planning and response with first responders. *(continued on page 2)*

DHSES Comments on Federal Research and Development Plan

During December, the New York State Office of Counter Terrorism (OCT) responded to DHS' request for comments to inform development of the National Critical Infrastructure Security and Resilience Research and Development Plan.

As part of this response OCT encouraged the development of cross-sector response and resilience plans in particular regarding cybersecurity.

Furthermore OCT stressed the importance of coordination between Federal agencies to avoid duplicative projects. Reducing the amount of overlapping programs would improve the allocation of budgetary resources.

Other concepts suggested to DHS include a public data repository for infrastructure resilience information, creation of simulation and visualization tools for policy makers, and a resilient communication system for infrastructure owner/ operators with government partners.

ALSO IN THIS ISSUE...

NYS OCT Critical Infrastructure Unit 2014 in Review *(continued)*

Of course, working with private and public center security officers involves "walking the ground" with them i.e. conducting and reviewing site security and threat assessments. In 2014, OCT-CI worked with federal, state and local partners to conduct over 60 site visits. OCT-CI then developed usable documents and briefings to review strengths and areas of concern.

Also throughout 2014 the CIP Unit provided extensive feedback to the Federal Department of Homeland Security on the development of the IP Gateway information sharing platform. The efforts of the CIP Unit concentrated on ensuring that local jurisdictions would be able to access the system and that it would provide functionality that supports their own infrastructure protection mission.

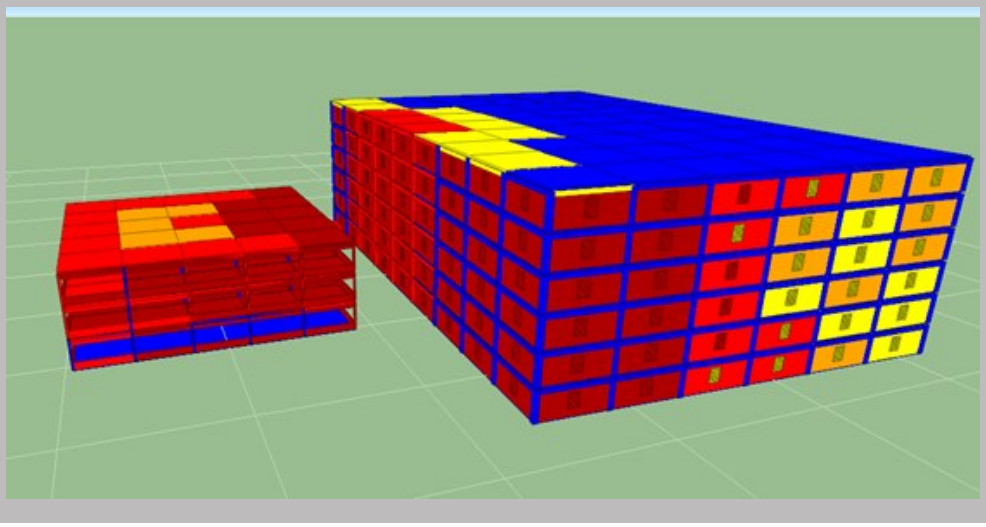
Throughout the summer the CI Unit worked closely with our partners in New Jersey to identify areas where we could work together to improve infrastructure protection and resilience from a regional perspective. This partnership was built out of Governors Andrew Cuomo and Chris Christie signing a Memorandum of Understanding which increased bi-state cooperation of counter-terrorism efforts. This partnership will continue to be important to the CI Unit's role in 2015 .

Finally OCT-CI worked with other state agencies and DHSES partners on two significant reports. The first report was an analysis of five critical sites in the state and the feasibility of installing microgrids to improve reliability and resilience. The second was a study on crude oil rail safety in New York and specifically the State's capabilities with regard to modeling the possible "downwind" hazard to the public in the event of an accident.

While we have accomplished many of our goals for 2014 we look forward to an even more successful 2015. In order for this to happen, we understand that partnership with our stakeholders both public and private is essential. Continuing and strengthening these partnerships is a priority for us and, as always, we encourage you to reach out to us with your feedback on how we can work with you to secure the infrastructure of New York State.

VAPO (Vulnerability Assessment Protection Options)

In 2014, OCT-CI analysts were trained to use VAPO (Vulnerability Assessment Protection Options) by the Defense Threat Reduction Agency. This software allows the Critical Infrastructure team to model the effects of explosives on buildings. This is used to add extra detail and information to assessments conducted by the State and local teams. The software produces a three dimensional model that illustrates damage to individual systems and components of buildings. The software also models how fast a vehicle can approach a barrier or gate, and to understand if the gate is adequate to stop the vehicle. For more information or to request assistance with blast modeling please contact Kurt Osterman at kurt.osterman@dhses.ny.gov.



Governor Cuomo Announces Over $4 Million to Protect Critical Infrastructure

In October, Governor Cuomo announced that $4.4 million will be awarded through three grant programs to protect critical infrastructure, increase rescue team capabilities, and bring tactical response team capabilities in line with the state standards.

"This funding will go a long way toward strengthening the network of locally-based emergency response infrastructure across New York," Governor Cuomo said. "By assisting communities in protecting their infrastructure and ensuring that our first responders to receive up-to-date training, we will be able to keep New Yorkers safer and better protected in their time of need."

The funding, administered by the Division of Homeland Security and Emergency Services, will support three key areas of proactive defense. The 2014 Critical Infrastructure Grant Program will provide $435,000 in funding to protect critical infrastructure, the 2014 Technical Rescue and Urban Search and Rescue Grant Program will award $2 million to increase technical rescue team capabilities, and the Tactical Team Targeted Grant Program will provide $2 Million in funding to assist with the standardization of tactical teams statewide and bring them in line with the accepted Division of Criminal Justice Services standards for operation and training.

2014 Critical Infrastructure Grant Program

$435,000 in funding is being awarded under the Critical Infrastructure Grant Program, which provides up to $50,000 in funding to successful applicants to protect their critical infrastructure, including special events or seasonal at-risk locations.

The awardees submitted applications that were coordinated with at least two first responder agencies that had prevention or protection responsibilities at the selected site. These first responders were law enforcement, fire departments, and emergency management or public works agencies. Additionally, the applicants included the identification of a critical infrastructure site and submitted the completion of a risk assessment, evaluation of local first responder capabilities for the site, and a proposed budget that details how the funding would be used to mitigate the identified risks.

2014 Technical Rescue and Urban Search and Rescue Grant Program

$2 million in grant funds is being awarded under the competitive Technical Rescue and Urban Search and Rescue Grant Program to allow local emergency response teams to enhance their rescue-related capabilities related to structural collapse, trench, confined space, waterway, flood, and rope rescue response operations.

Local emergency response teams that provide these services could apply for up to $100,000 in grant funds for certain equipment, planning, and training costs to further enhance their team's ability to respond to acts of terrorism and other catastrophic events.

2014 Tactical Team Targeted Grant Program

A total of $2 million in funding is being awarded under the Tactical Team grant program, which focuses on sustaining, maintaining, and improving teams currently in action and to work to enhance their existing capabilities, specifically for IED or counter-terrorism missions. This is being done through the implementation of adopted statewide standards as set forth by the state Division of Criminal Justice Services.

These groups, who were eligible for up to $100,000 in funding, are active tactical team of more than 15 members who respond to calls for service outside of a correctional setting. Teams with at least 10 members and who have an agreement with the Division of Criminal Justice Services to meet the 15 member requirement were also eligible to apply for this funding.

Release of the Updated 2014 National Emergency Communications Plan

The updated 2014 National Emergency Communications Plan (NECP) is released by NPPD's Office of Cybersecurity and Communications (CS&C) and Office of Emergency Communications (OEC).

On November 12, 2014, Roberta Stempfley, the CS&C Deputy Assistant Secretary, announced the release of the NECP on the DHS official blog. This is the first update to the NECP since the original publication in 2008. The 2014 NECP provides information and guidance to those that plan, coordinate, invest in, manage, and use emergency communications systems. OEC worked closely with more than 350 representatives from Federal, State, local, tribal, and territorial jurisdictions, as well as the private sector, to update the NECP and provide a roadmap for stakeholders to implement strategies that address emergency communications challenges in the 21st century.

To help stakeholders prepare for the rapidly evolving emergency communications landscape, the NECP emphasizes the need to enhance and update the policies, governance structures, plans, and protocols that enable responders to communicate and share information under all circumstances. As a stakeholder-driven plan, the NECP aims to maximize the use of all communications capabilities available to emergency responders–voice, video, and data–and to ensure the security of data and information exchange.

Implementation of the NECP is a shared responsibility. Over the next several months, OEC will collaborate with its stakeholders across all levels of government and the private sector to assist in identifying NECP implementation activities aimed at ensuring emergency responders across the country can communicate effectively under all circumstances.

For additional information and to download a copy of the plan, please visit the DHS NECP Webpage. For any questions, please contact OECNECP@dhs.gov.

U.S/Canada Test Cross-Border Resiliency

Disasters aren't constrained by borders, so emergency response can't be constrained either. If a hurricane were to cause major damage in cities within the United States and Canada, responders and government leaders from both countries may need to work together to provide emergency assistance. The Canada-U.S. Enhanced Resiliency Experiment (CAUSE) uses cross-border information-sharing experiments to help increase resilience at our northern border.

The Department of Homeland Security (DHS) Science and Technology Directorate (S&T) and the Defence Research and Development Canada's Centre for Security Science (DRDC CSS) recently completed the first phase of the third cross-border information-sharing experiment with partners throughout New Hampshire and Nova Scotia.

The first phase of the experiment tested new methods of engagement and information sharing for a simulated major hurricane impacting the United States and Canada. Participants included representatives of the Nashua, N.H. Office of Emergency Management, members and collaboration partners of the DHS Virtual Social Media Working Group and private sector representatives. Virtual Operations Support Teams (VOST) – including teams from Colorado and New York, Pacific Northwest and Canada (CanVOST) – provided mutual aid support remotely to jurisdictions on both sides of the border.

Some outcomes of the CAUSE experiment included:

- Enhanced resilience through cross-border partnerships with interoperable communications and shared situational awareness;
- Integration of non-traditional resources, including crowd-sourced information, open technologies, and digital volunteers to augment traditional emergency response; and
- The ability to send and receive cross-border alerts via multiple channels and among multiple response partners.

This event is another milestone towards President Barack Obama and Prime Minister Stephen Harper's 2011 U.S. – Canada joint declaration, Beyond the Border: A Shared Vision of Perimeter Security and Economic Competitiveness. The CAUSE Resiliency Series supports the principles and key areas of cooperation of the 2011 U.S. – Canada Beyond the Border Action Plan.

Climate Adaptation and Critical Infrastructure Webinar Series

The National Protection and Programs Directorate, Office of Infrastructure Protection, will host a Webinar entitled "Regional Adaptation Strategies for Addressing Sea Level Rise and Its Cascading Effects." The second in a series of Climate Adaptation and Critical Infrastructure Webinars is scheduled for Friday, January 30, 2015, from 1:00 – 2:30 p.m. EST. This joint partnership Webinar will feature speakers from Federal, State, and local entities discussing regional adaptive strategies and activities for addressing the impacts of sea level rise on critical infrastructure and will cover the topics listed below:

- Sea level rise in the Southeast United States – cause, how high, and when
- Organizing communities
- Comprehensive planning

Role of Protective Security Advisors regarding extreme weather and climate adaptation

Registration is available here.

FERC Approves New Physical Security Standards for the Electric Grid

On November 20, 2014, the Federal Energy Regulatory Commission (FERC) approved new physical security standards that will apply to the most critical aspects of the Bulk Power System. In an unusually expedited manner, FERC had directed the North American Electric Reliability Corporation (NERC) to develop the standards in March and submit them for approval in July 2014. Thus, a process that often takes several years of development was accomplished in several months.

The new standards (Reliability Standard CIP-014-01) require owners and operators of transmission stations and substations to perform a risk assessment of their systems to identify critical facilities; evaluate potential threats to, and vulnerabilities of, those facilities; and develop and implement a security plans to protect against attacks on those facilities. In addition the standards require that an "unaffiliated third party" review the threat and vulnerability assessment and the security plan.

FERC did not adopt a proposal that would have allowed them, or any other appropriate governmental authority, to add or remove facilities from an entity's list of critical facilities. The Commission also directed that NERC submit an informational filing regarding if control centers should be held to the new physical security standards, but allowed NERC two years to submit this study.

Elements of the new standard will be effective over some period of time, with the first requirement (risk assessment to identify critical facilities) being required not earlier than six months after the effective date of the final rule.

Additional information on the new standard is available on the NERC website here.

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