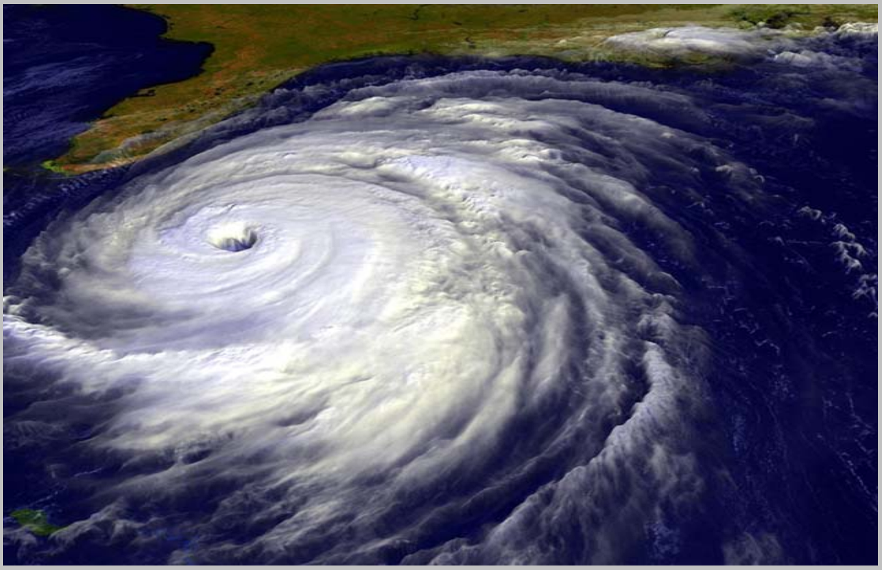
COUNTER TERRORISM
NEW YORK STATE DIVISION OF HOMELAND SECURITY AND EMERGENCY SERVICES

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

CRITICAL INFRASTRUCTURE PROTECTION AND RESILIENCE QUARTERLY NEWSLETTER

ISSUE #6 July 2014

Coastal Storm Forecast and Preparedness 2014



While hurricane forecasters are predicting below-average activity for the 2014 hurricane season, emergency management officials along the coast are urging state and local governments to keep citizens and equipment prepared for potential storms that may be looming on the horizon. The National Oceanic Atmospheric Organization (NOAO) reports a 50% chance of a below-average number of storms this season, a 40% chance of an average amount of storms, and a 10% chance of having an above average amount of storms. Forecasters completed their predictions, estimating that there is a 70% chance that the 2014 Hurricane Season will have a total of 8-13 named storms, 3-6 intermediate hurricanes and 1-2 major hurricanes. Regardless of the forecast, coastal emergency management officials have made significant improvements to hurricane preparedness since the events of Hurricane Sandy.

Following the events of Hurricane Sandy, Governor Cuomo established two 64-member commissions charged with evaluating the State's emergency management capabilities throughout the events of Hurricane Sandy. The NYS Ready and the NYS Respond Commissions prepared recommendations which were enacted almost immediately following their release. These included the importance of a coordinated, unified training effort among local and state governments, the establishment of localized emergency stockpiles for emergency management teams, and investment in emergency gasoline reserves.

NOAA Coastal Flood Exposure Mapper

The National Oceanic and Atmospheric Administration has made available the Coastal Flood Exposure Mapper which helps citizens identify coastal areas along the northeast that are particularly susceptible to flooding. This tool allows users to select a location and create various maps that show people, places, and natural resources exposed to coastal flood hazards. Guidance is also provided for how these maps can be interpreted and used in public forums. Currently, the tool only supports most of the Hurricane Sandy impact area (coastal counties of Delaware, New Jersey, Pennsylvania, and New York) however, expansion plans are underway for the rest of the East Coast and Gulf of Mexico. The tool can be accessed at the NOAA website here: http://www.csc.noaa.gov/digitalcoast/tools/flood-exposure

ALSO IN THIS ISSUE...

Coastal Storm Forecast and Preparedness 2014 *(continued)*

Hurricanes remain one of the world's most volatile reoccurring natural hazards and are capable of producing wind speeds above 100mph, spin-off tornadoes, flooding rains, and hurtling debris. History has shown that catastrophic damage imposed on areas of critical infrastructure can have a paralyzing effect on a state's economic well-being and threaten the stability of a local government. The Department of Commerce estimates that construction costs to repair and replace the damage caused by Hurricane Sandy in downstate New York will cost roughly $41.9 billion, (http://www.esa.doc.gov/sites/default/files/reports/documents/sandyfinal101713.pdf).

The continued improvement of New York's emergency preparedness and response capabilities will ensure the preservation of critical infrastructure throughout the State while further mitigating the damage caused by tropical storms such as Hurricane Sandy.

New York State Homeland Security Strategy

In March, the Division on Homeland Security and Emergency Services (DHSES) released the 2014-2016 State Homeland Security Strategy. The Strategy outlines the State's vision, goals and objectives to ensure that New York State is strong, secure, and resilient and is recognized as a national leader in homeland security and emergency management.

The Strategy is a critical document, providing the "big picture" of Homeland Security from a State perspective. It helps to guide State and local homeland security planning and investments. DHSES worked to develop the Strategy in coordination with more than 1,700 Federal, State, and local stakeholders across New York State. The Strategy is available of the DHSES website at: dhses.ny.gov/media/documents/NYS-Homeland-Security-Strategy.pdf

Critical Infrastructure Grant Program 2014

The New York State Division of Homeland Security and Emergency Services Critical Infrastructure Grant Program (CIGP) supports local first responder's efforts to mitigate risk and enhance protection capabilities at government owned critical infrastructure sites and special events or seasonal at risk locations. The grant has issued $1.2 million in funding to date and purposefully advances a common understanding of, and approach to, risk management that requires grant investments be linked to formal risk assessments. This program is a significant component to the State's implementation of the 2014-2016 New York State Homeland Security Strategy, "Goal 2: Protect Critical Infrastructure and Key Resources." The primary objectives of this Strategy Goal are to: conduct a systematic process of identifying and cataloging infrastructure; conduct site visits and risk assessments; invest in target hardening projects; and, provide additional protective and mitigation measures based on the current threat environment.

DHSES released the FY2014 CIGP grant opportunity on June 12th making up to $500,000 available to eligible jurisdictions. **Applications are due August 4th, 2014.** Past grantees have leveraged this grant program to protect key critical infrastructure in their jurisdictions by purchasing allowable equipment to perform targeted hardening measures (e.g. physical security enhancements, information technology upgrades, surveillance installation, etc.), conducting training and exercise opportunities to enhance first responder and CI/KR staff awareness, as well as engaging in planning opportunities to assess risk and identify equipment, training, and exercise needs. A best practice from this grant program is the leveraging of funding by the City of Albany and City of Syracuse to support "local assessment teams" which are comprised of multi-disciplinary representation to conduct risk-based, holistic assessments of critical infrastructure in their communities.

How Is Your Jurisdiction Protecting Your Critical Infrastructure?

We would love to hear from you. Contact CIP@dhses.ny.gov.

Infrastructure Protection Gateway: Update

When will the IP Gateway be released?

The Office of Infrastructure Protection has made the decision to postpone the release of the IP Gateway. Although DHS has not provided a release date, we remain actively engaged to assist with a solution that will benefit State and Local users.

What is the status of ACAMS?

On June 6, 2014 the Automated Critical Asset Management Systems (ACAMS) was taken offline and formally decommissioned. Unfortunately ACAMS was unable to be extended pending the deployment of IP Gateway. Information in ACAMS will be imported to the IP Gateway once it becomes operational.

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 Insider Threat (Part 1)

How much time and money is spent buying and monitoring systems designed to protect critical infrastructure from an external threat, but what if the main threat is not outside, but inside your organization?

Two excellent resources were recently published: the federal DHS Office of Infrastructure Protection's *"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). What are the salient points and "action" steps from the recent research on this threat?

What Are We Protecting and Why? First, companies and organizations need to identify, quite explicitly, what systems and information are considered critical. This inventory identifies the "Crown Jewels" of the company – information and systems that are critical to the operation and success of the organization. Not all information needs to be protected, but all employees must know if they are handling vital information or systems. Related to this is an analysis of **who might be interested in acquiring this information and why**.

When identifying critical assets it is also important to analyze **What Is the Likely Impact or Consequence of Disclosure or Compromise?** The rationale for designating critical or sensitive information usually is correlated to the potential impact or consequence of the disclosure of the information. Companies and organizations should identify "worst case" scenarios regarding the disclosure of sensitive information or compromise of critical systems and the probability of that occurring. In addition, it is helpful to consider the Insider's definition of success – is it financial gain e.g., selling proprietary information to a competitor, sabotage or perhaps "embarrassing" the company?

Who in the Organization Has Access to Sensitive/Critical Information? CI professionals should expand their understanding of an "insider." Although the traditional definition i.e. "one or more individuals with the access and/or insider knowledge of a company or organization that would allow them to exploit the vulnerabilities of that entity's security, systems, services, products, or facilities with intent to cause harm" (NAIC, 2008) remains valid, it's application with respect to technological advances, globalization and outsourcing needs to be considered. Third party vendors with access to IT or other systems become "insiders" with the capability to cause damage or steal proprietary information. Many recent cases confirm this – companies were damaged not by direct employees, but by third party vendors with access to company systems.

Understanding the Insider Threat *(continued)*

Andrea Danti/ShutterStock.com

Organizations should identify all personnel who have the access and capability to disclose information or compromise systems. This should include not only the information itself, but where the information is stored e.g., on servers and shared drives and who has access to those systems.

How Can Organizations Detect and Prevent the Insider Threat? There are several theories about the motivation of those who reveal sensitive information or compromise systems. In almost all cases, they have expressed their displeasure with the company/organization to other employees and peers multiple times. It is usually clear to those around them in the workplace that they "aren't happy" and, for whatever reason, (fame, fortune, ideology) have chosen to take action to cause harm to their employer. The presence of the employee in the workplace "every day" is likely to provide indicators of this dissatisfaction.

Peers and first line supervisors are best able to identify malicious insiders. Employees must be aware of and companies must develop a culture of reporting unusual behavior for follow-up investigation. Comments such as "I could cause this company a lot of damage if I wanted to" should not be ignored. Employees should both be aware of and offered incentives to develop practical solutions for protecting sensitive company information. Some companies have found that anonymous "Tip" lines to report suspicious behavior are an effective tool.

In other words, organizations should "Crowdsource" security. They should strive to develop an organizational culture where **security (like safety) is everyone's business**. Protecting the organizations proprietary property and critical systems is not just for the security team, the IT department or upper-management. Annual training should focus on aspects of the insider threat and appropriate reporting procedures.

In the **next** issue of the CI Quarterly, **Understanding Insider Threat (Part 2)** will address additional best practices for prevention and detection.

Chemical Sector Security Summit

The National Protection and Programs Directorate / Office of Infrastructure Protection (NPPD/IP) and the Chemical Sector Coordinating Council (CSCC) are co-sponsoring the Eighth Annual Chemical Sector Security Summit. The Summit is scheduled for Tuesday, July 22, 2014 through Thursday, July 24, 2014 in Baltimore, MD.

This event has generated high interest in the chemical industry and is an excellent opportunity to gain a better understanding of the security landscape as well as providing networking opportunities with DHS and other Government agency officials, industry representatives, and security experts in the field. This year's speakers and session topics will provide a wealth of information and resources to enhance your security efforts. Session topics include Executive Order 13650: Improving Chemical Facility Safety and Security, Chemical Facility Anti-Terrorism Standards (CFATS) updates, international trends in chemical security, transportation (trucking, rail and pipelines), and voluntary programs. Summit participation enhances the protection and resilience of the Nation's fixed critical infrastructure and emphasizes the Department's commitment to bilateral information sharing—essential elements of the DHS mission and core responsibilities.

For more information on this event, please visit: www.dhs.gov/chemical-security-summit.

National Homeland Security Conference 2014

Conference Session: ***The Current Landscape of State, Local, Tribal, and Territorial Critical Infrastructure Security and Resilience Efforts***

On May 21, 2014, the State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC) hosted an interactive panel discussion at the National Homeland Security Conference to showcase the findings from a series of reports examining SLTT critical infrastructure programs across all ten FEMA regions. Topics included an overview of the SLTTGCC, the major findings from the regional reports, and how they relate to conference participants' efforts in emergency preparedness, emergency management, and critical infrastructure security and resilience. SLTTGCC leadership then engaged the audience in highlighting key preparedness, response, and resilience issues and challenges of the SLTT community.

Panelists included Curtis Parsons, SLTTGCC Chair, Homeland Security & Emergency Management Coordinator, Lenawee County, Michigan and Mark Hogan, SLTTGCC Executive Committee Member, Chief of Security, City of Tulsa, Oklahoma. Participants included approximately 30 representatives of government agencies, owners and operators, and non-profit organizations, including:

- SLTTGCC and Regional Consortium Coordinating Council Members
- Other State and local critical infrastructure program personnel
- Participants in SLTTGCC activities, such as Real Time Forum Webinars

Among the highlights and key learnings from this interactive session were:

♦ **State and local critical infrastructure programs are actively identifying critical infrastructure and leading assessments.**

Example: The Alaska Division of Homeland Security and Emergency Management is offering vulnerability assessments, using the Automated Critical Asset Management System (ACAMS) asset visit forms, to owners and operators around the State. Current focus is on government-owned assets in Anchorage. The Division is interested in guidance from the SLTTGCC on conducting site visits on tribal and local infrastructure.

♦ **State and local critical infrastructure programs are actively partnering and sharing information with owners and operators.**

Example: The Northeast Ohio Regional Fusion Center disseminates a weekly open-source report, which includes national and local information and situation reports on all 16 critical infrastructure sectors.

♦ **This session was also significant in that it helped identify critical infrastructure program challenges and needs associated with SLTTGCC partners, such as:**

◊ SLTTGCC should continue to provide feedback to the DHS Office of Infrastructure Protection on Federal critical infrastructure programs, tools, and capabilities, including IP Gateway.

◊ Continued training and education for SLTT critical infrastructure personnel is needed, particularly in the areas of asset identification and assessments.

◊ Fusion center critical infrastructure capabilities are still in a state of maturity, with many fusion centers lacking the expertise to positively contribute to the mission to reduce risk to critical infrastructure.

DHS Industry Engagement and Resilience Branch Releases Cyber Trends Review Forecast

To stay informed about the constantly changing and evolving cyber landscape, the DHS Industry Engagement and Resilience (IER) Branch monitors the cybersecurity threat landscape; tracks cybersecurity events, such as security breaches or compromises; and follows new cyber developments, such as new technology and processes. IER supplements open-source information with context and analysis from its sector liaisons and develops products to share with sectors and other partners. In April 2014, IER released two annual cybersecurity reports:

- The *2013 Cybersecurity Review* highlights significant cybersecurity stories, attacks, and trends from the past year. The Review represents a survey of significant cybersecurity issues as reported by independent security experts, cybersecurity news sources, cybersecurity service providers, and security research organizations.
- The *2014 Cybersecurity Forecast* identifies potential cybersecurity issues and trends that may occur in the upcoming calendar year. The Forecast represents a survey of cybersecurity predictions collected from independent security experts, cybersecurity news sources, cybersecurity service providers, and security research organizations.

Both the *2013 Cybersecurity Review* and the *2014 Cybersecurity Forecast* focus on issues, events, and predictions that multiple sources within the cybersecurity community address and agree are significant to the cybersecurity landscape. They highlight these topics of discussion within the cybersecurity community and are not intended to prioritize particular issues over others, including issues not discussed in these documents.

Additionally, each month IER produces the *Cyber News Spotlight*, which is a monthly summary of publicly published information concerning significant cybersecurity and cyber infrastructure issues. The *Cyber News Spotlight, 2013 Cybersecurity Review,* and *2014 Cybersecurity Forecast* are available on the CS&C IER Homeland Security Information Network (HSIN) portal at https://hsin.dhs.gov/ci/iir/ier.

DHS Releases Sector Risk Snapshot

The Department of Homeland Security released the Sector Risk Snapshots, an overview and risk profile for the 16 critical infrastructure sectors and 11 of the subsectors and transportation modes. Each overview is 2 pages, providing a quick look at the sector, common threats and hazards concerning each sector, and listing primary dependencies and interdependencies between sectors.

The Snapshots provide an introduction to the diverse array of critical infrastructure sectors, touching on some of the key threats and hazards concerning the sectors, and highlighting the common, first-order dependencies and interdependencies between sectors. The Snapshots are intended to serve as quick reference aids for homeland security partners, particularly State and local partners, and fusion center analysts, and each Snapshot includes a list of resources that partners can go to for more comprehensive sector information. This document can be viewed online here: http://nacchopreparedness.org/wp-content/uploads/2014/05/OCIA-Sector-Risk-Snapshots.pdf

Long Island/New York City Emergency Management Conference

May 28-29, 2014 (Uniondale, NY)

This two-day conference was attended by 425 people and marked the 20th Anniversary of this event. The conference featured sessions on various topics to educate emergency management professionals on issues they face in their roles. Speakers and workshops focused on law enforcement, counterterrorism, response and recovery, natural disasters and public health issues.

Each year at the Conference, the Edward F. Jacoby, Jr. Excellence in Emergency Management Award is presented. This year, NYC Office of Emergency Management Commissioner Joseph Bruno was honored and accepted the award in person.

This year's keynote speaker was Dr. Stephen Flynn, Professor of Political Science and Director of the Center for Resilience Studies and Co-director of the George J. Kostas Research Institute for Homeland Security at Northeastern University. Dr. Flynn is one of the world's leading experts on transportation security and infrastructure and community resilience issues. He authored The Edge of Disaster: Rebuilding a Resilient Nation (2007), and the national bestseller, America the Vulnerable (2004).

The conference featured other sessions with subject-matter expert speakers. Dr. David Abramson, Deputy Director of the National Center for Disaster Preparedness and Assistant Professor of Socio-medical Sciences at Columbia University Medical Center discussed public health impacts of hurricanes. FBI-New York Supervisory Special Agent Barbara Daly, a member of the Violent Crime squad, spoke about behavioral indicators of homegrown terrorism, focusing on specific historic and present-day cases of violence in workplaces, schools and more. Suffolk County Assistant Chief of Patrol Stuart Cameron and NYPD Counter Terrorism Deputy Inspector Michael Riggio gave an animated overview of Securing the Cities (STC). STC is a pilot initiative to increase radiation detection and response capabilities around the nation's highest-risk urban areas. This program was intended to be a regional approach to enhance the ability to prevent a radiological or nuclear attack. Since its inception in 2006, STC has been integral to unifying efforts in combatting future attacks.

Additional workshop topics included social media, challenges to resident re-occupancy, catastrophic planning, and issues on the horizon. Experts from the National Weather Service (NWS) and U.S. Geological Survey (USGS) provided updates on weather warnings systems and other tools available to emergency managers.

For more information about this year's conference and to look out for next year's conference, visit www.LINYCEMCONFERENCE.com

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