NEW YORK STATE | Counter Terrorism

Andrew M. Cuomo
Governor
John P. Melville
Commissioner

CRITICAL INFRASTRUCTURE PROTECTION AND RESILIENCE QUARTERLY NEWSLETTER

ISSUE #10 July 2015

Understanding Zero-Day Vulnerabilities and Exploits: A Brief Summary

As cybersecurity continues to attract a significant amount of attention in Critical Infrastructure Protection and Emergency Management, it is important for decision makers to understand some of the terminology used by cybersecurity practitioners. One of the more commonly used terms is "zero-day," which may refer to a vulnerability or an exploit.

A zero-day vulnerability is a security hole in software that is not yet publically known, though it may be known to attackers. While every responsible software manufacturer tries to be mindful of security during the software development life cycle, it is impossible to foresee every possible method of attack. This is especially true in the case of software that we use frequently, such as operating systems and web browsers. A zero-day exploit is code that attackers use to take advantage of a zero-day vulnerability. Famous zero-day exploits include Conficker, Aurora and Heartbleed.

From the moment software is released to the public it is studied and analyzed for zero-day vulnerabilities. Adversaries seeking to do harm may exploit these vulnerabilities themselves or sell this *(continued on page 2)*

Item Open for Public Comment: Community Resilience Guide

The National Institute of Standards and Technology (NIST) is working closely with public and private sector stakeholders in the development of the Community Resilience Planning Guide for Buildings and Infrastructure Systems. The guide aims to:

- Define community-based resilience for the "built environment."
- Identify consistent performance goals and metrics for buildings and infrastructure and lifeline systems to enhance community resilience.
- Identify existing standards, codes, guidelines, and tools that can be implemented to enhance resilience.
- Identify gaps in current standards, codes, and tools that, if successfully addressed, can lead to enhanced resilience.

The document is divided into two volumes, with Volume 1 addressing the methodology for resilience planning and illustrating the planning process for a fictional town. Volume 2 serves as a resource document with detailed information on characterizing social and economic systems, dependencies and cascading effects, buildings, and infrastructure systems.

The two volumes are available through the NIST Website.

ALSO IN THIS ISSUE...

Cover Photo Credit: community.norton.com

Understanding Zero-Day Vulnerabilities/Exploits *(continued)*

information to others on the so-called "dark web." However, not all of this work is being done by malicious actors. Individuals, security firms, government agencies and, of course, the vendors themselves all actively search for vulnerabilities. Typically, outside parties (such as individuals and security researchers) will notify the software maker while keeping the potential exploit confidential until it has been fixed. Some software manufacturers will go so far as to offer "bounties" for discovering zero-day vulnerabilities and sharing the information confidentially. Depending on the severity, the software vendor may elect to make the vulnerability public along with possible mitigation measures before they are able to release a patch.

Although Zero-Day exploitation is difficult to defend against, a strong policy regarding the installation of software updates may minimize a system's vulnerability. Such a policy ensures updates are routinely reviewed and applied in a timely fashion. As always, personnel should be aware of and use safe computing habits, such as not opening email or clicking on links from unknown sources.

Introducing New IP Deputy Assistant Secretary

The DHS Office of Infrastructure Protection (IP) Assistant Secretary Caitlin Durkovich recently announced that Bob Kolasky was selected as the new Deputy Assistant Secretary (DAS) for IP and would begin serving in his new role on June 15, 2015. Over the past several years, Bob has served as IP's Director of Strategy and Policy, where he established solid strategic planning, performance management, and budgeting for IP and immersed himself with a vast understanding of the critical infrastructure security and resilience mission.

Bob's outstanding work across the Infrastructure Protection spectrum on significant and complex issues has been widely recognized across the IP community, and his overall experience and leadership will help IP to continue on a path of leading the national effort in securing critical infrastructure from all hazards by managing risk and enhancing resilience through collaboration with the critical infrastructure community.

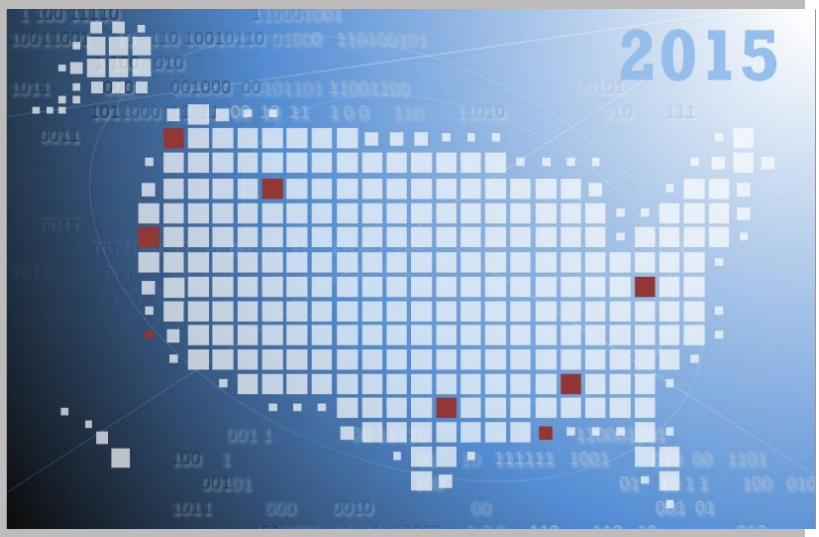
Concurrently, IP will also see familiar faces move to other leadership positions, which is a testament to the flexibility and professionalism of IP's senior executives. These changes will further support the IP mission as each individual will bring cross-cutting experience while generating new vantage points, insights, and perspectives.

- Linda Solheim, who expertly stepped into the role of Acting DAS after the retirement of Bill Flynn this past December, will serve as the Director of Sector Outreach and Programs Division (SOPD), bringing her extensive field operations perspective and management expertise to provide leadership to SOPD to bridge their national work with our regionalization efforts.
- Tonya Schreiber will join Dave Wulf and serve as the Deputy Director of the Infrastructure Security Compliance Division (ISCD), a role that will build on her experience across regulatory and voluntary programs as the division carries forward with all of the work associated with the long-term authorization of CFATS and establishing the Ammonium Nitrate program.
- Scott Breor will become the permanent Director of Protective Security Coordination Division (PSCD), leveraging his expertise across ISCD and now PSCD to implement our regionalization efforts.
- Sarah Ellis Peed will serve as acting director of the newly-renamed IP Strategy, Policy, and Budget.

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

2015 National Preparedness Report



On Thursday, May 28, 2015, the Federal Emergency Management Agency (FEMA) and its partners released the 2015 National Preparedness Report (NPR). The NPR is an annual status report summarizing the nation's progress toward reaching the National Preparedness Goal of a secure and resilient nation. The 2015 NPR places particular emphasis on preparedness progress in implementing the National Planning Frameworks, which describe how the whole community works together to achieve the National Preparedness Goal.

The 2015 report identifies 43 key findings across the Prevention, Protection, Mitigation, Response, and Recovery mission areas, in addition to six key overarching findings:

- Recent events, including the epidemic of Ebola virus disease, have highlighted challenges with coordinating the response to and recovery from complex incidents that do not receive Stafford Act declarations.
- Businesses and public-private partnerships are increasingly incorporating emergency preparedness into technology platforms, such as internet and social media tools and services.
- Environmental Response/Health and Safety, Intelligence and Information Sharing, and Operational Coordination are additional core capabilities to sustain, which are capabilities in which the nation has developed acceptable levels of performance for critical tasks, but which face potential performance declines if not maintained and updated to address new challenges.
- Cybersecurity, Housing, Infrastructure Systems, and Long-term Vulnerability Reduction remained national areas for improvement, and Economic Recovery re-emerged as an area for improvement from 2012 and 2013. Access Control and Identity Verification is a newly identified national area for improvement.
- Perspectives from states and territories on their current levels of preparedness were similar to previous years. All ten core capabilities with the highest self-assessment results in 2012 and 2013 remained in the top ten for 2014; cybersecurity continues to be the lowest-rated core capability in state and territory self-assessments.
- While Federal departments and agencies individually assess progress for corrective actions identified during national-level exercises and real-world incidents, challenges remain to comprehensively assess corrective actions with broad implications across the federal government.

Questions can be directed to FEMA at: NPR@fema.dhs.gov.

For further information visit: National Preparedness Efforts.

Regional Consortium Coordinating Council News

Who is the Regional Consortium Coordinating Council (RC3)?

The Regional Consortium Coordinating Council (RC3) is one of four Cross-Sector Councils described in the National Infrastructure Protection Plan (NIPP). Their goal is to understand, connect, enable, and build partnerships for the protection and security of critical infrastructure and the resilience of surrounding communities. The Council is comprised of 24 multi-jurisdictional partnerships with representatives and subject matter experts from business, government, and non-profit organizations.

Cybersecurity Working Group

The RC3's Cybersecurity Working Group was formed to address the growing community of interest related to cyber threat analysis and the capabilities that occur with increased information sharing. The working group is currently establishing liaison relationships with organizations engaged in cyber resilience to further the RC3's connections and knowledge of cybersecurity capabilities. RC3 is currently seeking more nominations for organizations to participate in this endeavor.

How To Connect

As the homeland faces new and evolving threats every day, RC3 is constantly looking for ways to expand and improve the council. New member applications, Affiliate applications, and Subject Matter Expert applications are being accepted and reviewed by the RC3 Executive Committee Board Members. For more information about how to become a member, please visit the RC3 website.

Naval Postgraduate School: A Public Employee Opportunity

In Issue #3 of the newsletter, the importance of obtaining relevant certifications was highlighted as it relates to working in the infrastructure protection field. Building upon the benefits gained by the individual and organization through obtaining certifications such as the Physical Security Professional or Certified Protection Professional, public employees should also consider higher homeland security education opportunities.

The Naval Postgraduate School & The U.S. Department of Homeland Security Center for Homeland Defense and Security regularly offers a Master's Degree Program to full-time public employees at all levels of government that have homeland security experience and responsibilities. The school routinely graduates law enforcement, fire protection, emergency management, healthcare and a wide range of other personnel that play a role in protecting our homeland.

Learn more about this 18-month Master's program, provided at no cost to the student, here. Applications for Spring and Summer 2016 are currently being accepted.

Chemical Facility Anti-Terrorism Standards (CFATS) Update

Established in 2007, the Chemical Facility Anti-Terrorism Standards (CFATS) program has helped make the nation more secure by identifying and regulating high-risk chemical facilities. On December 18, 2014, President Obama signed into law the Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014 ("the Act"), Public Law No. 113-254 (2014). The Act re-codifies and reauthorizes the CFATS program and adds new provisions, while preserving most of the existing CFATS regulations. This Act recognizes the success of this program by DHS, industry stakeholders, and Congress.

The Act establishes numerous reporting requirements, including Section 2109, which requires DHS to establish an outreach implementation plan in coordination with public and private stakeholders to identify "chemical facilities of interest," as defined in Section 2101 of the Act, that may be required to report to CFATS and to make available compliance assistance materials and information on CFATS-related education and training. This plan aims to achieve three main goals:

- Expanding DHS efforts to identify chemical facilities of interest.
- Strengthening CFATS compliance assistance materials and information on education and training.
- Expanding stakeholder engagement to raise awareness of CFATS requirements and compliance resources and gathering input to make program improvements.

The department developed the Outreach Implementation Plan, which includes specific activities, milestones, and metrics relating to these goals to improve the CFATS outreach and engagement for identifying these chemical facilities of interest. The plan was provided to more than 20 stakeholders and incorporates comments received from federal and state partners, as well as industry, labor, and community organizations. The plan was published on March 18, 2015, within the timeline mandated by the Act.

This plan is a milestone, not an endpoint, toward maturing the CFATS program. If you have any questions or comments, please contact CFATS@hq.dhs.gov for more information.

Reporting a Chemical Facility Anti-Terrorism Standards Violation

The Act also requires DHS to establish a procedure for employees and contractors of a chemical facility of interest to report a CFATS violation no later than 180 days after the date of enactment (June 16, 2015). To provide the public with information on how to report a CFATS violation, the Department developed a Webpage, and fact sheet. Additional information is posted on the CFATS Knowledge Center.

Any individual may report a potential CFATS violation to the department, and chemical facilities of interest are prohibited by law from retaliating against an employee or contractor for reporting the potential violation. To submit a report to the Department regarding a potential CFATS violation, contact the CFATS Chemical Facility Security Tip Line at 877-FYI 4 DHS (877-394-4347) or email CFATSTips@hq.dhs.gov. Individuals may also report violations via mail at:

Director, Infrastructure Security Compliance Division
Office of Infrastructure Protection
Department of Homeland Security
Mail Stop 0610
245 Murray Lane
Washington, D.C. 20528

To speak with a DHS representative about the CFATS regulatory program, please contact CFATS@hq.dhs.gov.