Critical Infrastructure Partners: The Office of Infrastructure Protection is pleased to introduce the first issue of *The Partnership Quarterly*. The publication includes critical infrastructure security and resilience articles, highlights of cross-sector initiatives, training and exercise opportunities, new tools, and resources. You will also find a Partnership Perspectives section which will feature interviews with critical infrastructure partners.

We want to hear from you! Please send your story ideas or event content to: Sector.Partnership@hq.dhs.gov with "*The Partnership Quarterly*" in the email subject line. We hope that you will find *The Partnership Quarterly* useful, informative and a means of sharing and communicating your activities to the larger critical infrastructure community.

Homeland Security

The Partnership Quarterly

From the National Protection and Programs Directorate | Office of Infrastructure Protection

March 2014 Volume 1, Issue 1

In This Issue...

Message From the Director, Sector Outreach and Programs Division

Welcome to the inaugural issue of *The Partnership Quarterly*. As the Director of the Office of Infrastructure Protection's (IP) Sector Outreach and Programs Division (SOPD), I am very proud to introduce this new quarterly publication. The publication will be yet another means for us to connect with our partners and stakeholders on important topics that address the security and resilience of our Nation's critical infrastructure.

In keeping with SOPD's mission to execute the national effort to build, align, and leverage public-private stakeholder partnerships and programs to enhance critical infrastructure security and resilience, inside each *Quarterly* edition you will find useful partnership information on IP initiatives; exercises and training activities; an events calendar; interviews; cross-sector news; and other information.

The Partnership Quarterly will be supplemented by a monthly resource called *The Partnership Bulleti*n, which will highlight training opportunities, meetings, and other select or key event announcements from across DHS, IP and our Federal partners to assure timely and actionable information sharing.

Your feedback is critical to the success of both products and we welcome your suggestions for upcoming issues. Please send your comments and ideas to us via the Sector.Partnership@hq.dhs.gov mailbox.

I would also like to take this opportunity to introduce Shawn Graff, the new SOPD Deputy Director. He brings with him extensive experience through his previously held positions as the National Infrastructure Coordinating Center (NICC) Director, his tenure at the Office of the Director for National Intelligence, and his U.S. Army service.

I look forward to strengthening our partnership through this and many other initiatives. Please feel free to share *The Partnership Quarterly* or *Bulletin* with your colleagues and stakeholders.

Photo Above: Tonya D. Schreiber, Director, SOPD

Now Available: NIPP 2013: Partnering for Critical Infrastructure Security and Resilience

In response to Presidential Policy Directive-21 on Critical Infrastructure Security and Resilience, the NIPP 2013 was developed through a collaborative process involving stakeholders from all 16 critical infrastructure sectors, our 50 States, and from all levels of government and industry. The enhanced and updated NIPP 2013 was released on December 20, 2013.

For more information and to download, please visit the NIPP 2013 Webpage.

Partnership Perspectives: Interview with Jami Haberl, Executive Director, Safeguard Iowa Partnership

Jami Haberl joined the Safeguard Iowa Partnership on September 11, 2007. Prior to joining Safeguard Iowa, she served as a senior program manager at the Iowa Foundation for Medical Care and the executive director for the Centers for Disaster Operations and Response at the Iowa Department of Public Health.

Why was Safeguard Iowa Partnership established and what are some of the focus areas?

The Safeguard Iowa Partnership is a voluntary coalition of the State's business and government leaders, who share a commitment to strengthen the capacity of the State to prevent, prepare for, respond to, and recover from disasters through public-private collaboration. Created in 2007 by the Iowa Business Council and representatives from key State agencies, the Partnership empowers businesses to integrate business resources, expertise, and plans with those of Government during all stages of disaster management. The Government cannot and should not be the only responders in a disaster situation, as the private sector has a wealth of knowledge and assets that may be needed during an emergency.

Who are some of your partners?

We currently have 102 public-sector organizations, 117 private sector organizations, and 39 nonprofit organization/associations that are partners of the Safeguard Iowa Partnership. The partners range from small to very large corporate organizations.

What are your thoughts on the value of public-private partnerships?

I continue to be impressed with the level of commitment and effort between the public and private-sector partners in working together to protect our communities from devastating disasters. We have all come to realize and recognize that communities are built on Government services and private businesses—big and small, nonprofit organizations—and most importantly, our individual citizens. When a disaster of any magnitude strikes a community, there are impacts within each sector of the community. Based on lessons learned from recent disasters, it's been recognized that the entire community is responsible for ensuring resiliency within that community. Without Government, businesses, nonprofit organizations, and community members, there is no community. As resources continue to dwindle, now more than ever we must all work together to prepare for, respond to and recover from disasters impacting our State.

What are some of Safeguard Iowa Partnership current initiatives and products?

Some of our products and initiatives—which all can be found on our Safeguard Iowa Partnership Website—include business continuity planning tools and templates; the emergency operations center liaison program in which private sector liaisons are positions within the county or State emergency operations centers; employer vaccination toolkit; business damage survey; and critical infrastructure and key resources planning, training and exercises.

How can stakeholders/partners contact you?

What kinds of training programs does the Partnership have?

Coming up, we have a cybersecurity training series which will be followed up with a Tabletop Exercise. The series is targeted towards employees without a technical or IT background and includes business continuity, leadership, and crisis management training. The purpose is to increase awareness among emergency management and owners and operators on the roles and responsibilities during a cyber-event. More information can be found on our registration page.

Photo Above: Jami S. Haberl, MPH, MHA Executive Director Safeguard Iowa Partnership

Photo Right: Safeguard Iowa Partnership coordinates numerous outreach and training activities, such as Tabletop Exercises, which provide opportunities for partners to gain an understanding of the roles and responsibilities of the partners within the community. (Safeguard Iowa Partnership Photo)

To be featured in the Partnership Perspective section please email: sector.partnership@hq.dhs.gov.

Quarterly Highlights:

Regional Partnership Engagement Webinars Raise Awareness

Through IP's Regional Partnership Engagement (RPE) efforts, the Regional Consortium Coordinating Council (RC3) and InfraGard, IP co-sponsored a series of Joint Critical Infrastructure Partnership (JCIP) workshops, conducted as Webinars to inform and engage with regional stakeholders.

More than 400 attendees participated in five Webinars designed to raise awareness of DHS programs, tools, and resources available to public and private critical infrastructure stakeholders and partners. "The Webinars also provided information on resources and programs that assist enhancing the preparation, security and resilience of facilities and assets," said Chris Terzich, RC3 council chair.

The 3-month series focused on different themes including: national preparedness, cybersecurity awareness, and critical infrastructure security and resilience. The Webinars featured presentations from the Active Shooter Preparedness Program, Office for Bombing Prevention, the Enhanced Critical Infrastructure Protection (ECIP) Initiative, and the Business Continuity Planning Suite.

Based on positive feedback from participants, IP plans to continue the JCIP workshops with additional Webinar series throughout 2014, with topics of interest including climate change/extreme weather, aging and failing infrastructure, and implementation strategies for the release of the NIPP 2013: Partnering for Critical Infrastructure Security and Resilience.

New Protective Measures Guide Released

The Commercial Facilities Sector Specific Agency (SSA) announced the release of the *Protective Measures Guide for U.S. Commercial Real Estate*, a For Official Use Only (FOUO) document designed to provide owners and operators of commercial office buildings with information that can be used to maintain a safe environment for occupants, employees, contractors, and visitors. The guide's protective measures provide suggestions for successfully planning, organizing, coordinating, communicating, operating, and training to augment the overall security posture at a building. This is the fifth such guide that Commercial Facilities has published in collaboration with our key industry partners. Previous protective measures guides include *U.S. Sports Leagues* (2008), the *U.S. Lodging Industry* (2010), *Mountain Resorts* (2011), and *Outdoor Venues* (2011). Though the protective measures presented in the guides are provided in part by our private sector partners, our Federal partners are also collaborators. The Commercial Facilities SSA works with their Government Coordinating Council to ensure that the guides accurately represent their programs and equities. For more information on the Protective Measures Guide series, please contact cfsteam@hq.dhs.gov.

Homeland Security Information Network Update / New Air Domain Awareness Portal

The newly enhanced Critical Infrastructure Community of Interest on the Homeland Security Information Network – Critical Infrastructure (HSIN-CI) allows DHS and sector stakeholders to efficiently communicate, coordinate, and share information on a single platform. HSIN-CI serves as the primary vehicle for nationwide information sharing and collaboration between DHS, all 16 critical infrastructure sectors, and State and local fusion centers.

In addition to providing tactical and planning functionality for vetted users, HSIN-CI is equipped with improved security measures to protect its libraries of more than 60,000 publications, providing a trusted network to ensure the sustainability and integrity of service delivery and the productivity of our Nation's critical infrastructure.

New initiatives are underway to expand the relevant content available on HSIN-CI. Examples include the Air Domain Awareness portal, which provides security and safety information to aviation owners and operators. To gain access to HSIN-CI, please email your name, employer, work email address, and the critical infrastructure sector with which you are associated to: hsinci@hq.dhs.gov.

HSIN-CI Snapshot: Air Domain Awareness Portal

The Air Domain Awareness (ADA) portal is the single place for government and public/private sector owners and operators of aviation assets to share security and safety information for the purpose of reducing risk to operations and assets.

Types of Aviation-specific communication:

- Routine communication and collaboration (daily decision-making)
- Country-specific alerts, warnings, and notifications
- Incident communication and collaboration
- Suspicious Activity Reporting (SAR)

Value of the ADA Portal on HSIN-CI:

- Situational awareness and preparedness
- Operational planning and response

Please click here to return to the top of The Partnership Quarterly

The Center for Infrastructure Protection and Homeland Security

The January 2014 *CIP Report* featured an article about IP's efforts to promote national critical infrastructure resilience, while the November 2013 edition highlights academic programs for critical infrastructure security and resilience professionals. To read about these initiatives, current or past issues, or to subscribe, visit: http://cip.gmu.edu/the-cip-report/.

The *CIP Report* is a monthly newsletter published by The Center for Infrastructure Protection and Homeland Security at the George Mason University (GMU) School of Law that informs readers of key critical infrastructure security and resilience issues. IP has partnered with GMU to foster development of a multi-disciplinary academic framework to support future workforce requirements needed to continue the critical infrastructure security resilience component of the homeland security mission.

The report is electronically distributed to interested professionals and provides the latest information about emerging legislation, Government and industry initiatives, and academic endeavors.

Training and Exercises

Training

IS-913.a: Critical Infrastructure Security and Resilience: Achieving Results through Partnership and Collaboration

The purpose of this online course is to introduce the skills and tools to effectively achieve critical infrastructure security and resilience through partnership and collaboration. The course provides an overview of the elements and processes to develop and sustain successful critical infrastructure partnerships. It is designed for critical infrastructure owners and operators from the Government and private sector, as well as for those with critical infrastructure duties and responsibilities at the State, local, tribal, and territorial levels. The course can be at: http://training.fema.gov/EMIWeb/IS/courseOverview.aspx?CODE=IS-913.a

IS-921.a: Implementing Critical Infrastructure Security and Resilience

This online course introduces those with critical infrastructure duties and responsibilities at the State, local, tribal, and territorial levels to needed information they need and available resources in executing the mission to secure and improve resilience in the Nation's critical infrastructure. The course can be accessed at: https://training.fema.gov/EMIWeb/IS/courseOverview.aspx?code=IS-921.a

General training inquiries should be directed to: IP_Education@hq.dhs.gov

Exercises

National Level Capstone Exercise 2014
(March-April 2014)

The National Level Exercise is tentatively scheduled to focus on response and long-term recovery efforts from a natural disaster. Recovery efforts will be examined in three response stages: the immediate aftermath of an earthquake, several weeks following the event, and then several months post incident.

For more information about IP exercises, contact ip.exercise@hq.dhs.gov.

Exercise & Workshop Success Stories:

"South Sandy" Power Restoration Workshop

At the request of Assistant Secretary Durkovich and in coordination with the Department of Defense (DOD) and the Department of Energy (DOE), IP conducted the "South Sandy" Power Restoration workshop in Arlington, VA. More than 60 people from five private sector energy companies, DOD, DOE, and DHS participated in the scenario, which was based on a Category 4 hurricane impacting the National Capital Region and causing severe damage to both energy and transportation infrastructure. The December 2013 workshop provided participants an opportunity to discuss prioritizing DOD restoration activities for mission critical needs while examining competing requests from Federal departments and agencies and State and local officials.

As a result of the exercise, participants gained a better understanding of the power restoration process, of how DOD facilities can request priority restoration, and which actions require further coordination and discussion.

New Mexico Playas Series II Exercise: Cascading Events (March 2014)

This exercise is co-sponsored by the IP and the State of New Mexico Department of Agriculture (NMDA). The exercise will focus on the protection of agriculture and food resources and the State's response to cascading effects of severe weather on livestock and the commercial food supply chain.

The New Mexico Agriculture and Food Exercise (Playas II Series) brings together public and private critical infrastructure stakeholders from the Food and Agriculture, Emergency Services, and Health and Public Health Sectors to validate and exercise mitigation activities and measures. This exercise will identify existing gaps and issues in New Mexico's response, mitigation, and recovery capabilities in the wake of a catastrophic event affecting the agriculture and food industries and the resulting cascading effects.

The full-scale exercise has been designated by the New Mexico Department of Homeland Security and Emergency Management to be the State's Annual Capstone Emergency Preparedness Exercise for 2014. On November 6, 2013, SOPD's Stakeholder Readiness and Exercise Section facilitated the "Discussion Based Exercise," which brought together various stakeholders, including the New Mexico Department of Agriculture, New Mexico Department of Health, New Mexico Department of Homeland Security and Emergency Management, and Socorro County Emergency Planners. The exercise emphasized information sharing and communications between New Mexico's Emergency Support Function (ESF) 11 and other ESF support agencies, as well as information sharing between private and public sector partners.

The November 6, 2013 exercise set the foundation for the March 2014 Full Scale Exercise (FSE). Resulting analysis from that event drove the selection of FSE activities to cover in the full scale exercise.

For more information about IP exercises, contact ip.exercise@hq.dhs.gov

Please click here to return to the top of The Partnership Quarterly

Feature Topic

Climate Change: A Complex Challenge

The impact of climate change and the challenge of extreme weather adaptation are concerns for DHS and critical infrastructure stakeholders. As a result, climate change adaptation will be a component of many IP risk assessment and analysis activities in the coming years.

On November 1, 2013, the White House released the Executive Order (E.O.) "Preparing the United States for the Impact of Climate Change." This Executive Order reinforces the President's Climate Action Plan that requires Federal agencies to continue their efforts in promoting collective action to increase resilience to extreme weather and to prepare for other impacts of climate change. In June 2012, pursuant to the President's Executive Order 13514, DHS published the Climate Change Adaptation Roadmap to outline a strategy to assess the threats, vulnerabilities, and potential consequences of climate change to the DHS mission of protecting the homeland.

IP's strategic framework to address and adapt to climate change will focus on series of strategies and resources to ensure that IP is the leader in critical infrastructure climate change science and risk-based mitigation activities. Those strategies include:

- Understanding the current science of climate change and its effect on critical infrastructure and identifying and filling gaps through research and development
- Developing risk-based mitigation and adaptation strategies and best practices for climate change adaptation
- Identifying and building decision-making support resources to assist stakeholders in their evaluation and choice of optimal investments
- Creating a venue for coordination and collaboration among the entire community by leveraging existing critical infrastructure partnership structures
- Incorporating adaptation science and considerations into IP's policies, programs, planning, and operations

Please click here to return to the top of The Partnership Quarterly

CIPAC Plenary Focus: Critical Infrastructure Security and Resilience

Together with the private sector and government partners, DHS takes a whole community approach to help ensure the resilience of our Nation's critical infrastructure. Promoting security and resilience—both physical and cyber—is a collaborative endeavor requiring effort and investment from both the Federal Government and the private sector. One way to facilitate that collaboration is through the Critical Infrastructure Partnership Advisory Council (CIPAC), established to facilitate coordination between the Federal government and State, local, tribal, territorial and private sector critical infrastructure security partners. Additional information on this collaboration can be found in the 2013 CIPAC Annual Report.

The CIPAC Plenary took place on November 5, 2013, in Washington, DC. This meeting is both a central event to the critical infrastructure public-private partnership and an affirmation of the shared national commitment to overarching system resilience that safeguards critical infrastructure from all threats and hazards. The plenary convened leadership from the DHS National Protection and Programs Directorate Office of Infrastructure Protection; the State, Local, Tribal, and Territorial Government Coordinating Council; the Partnership for Critical Infrastructure Security; the

attendees included representatives from the 16 critical infrastructure sectors in addition to public and private partners. The gathering of these groups in an annual open forum allows for transparency in developing that lead to increased critical infrastructure security and resilience.

Photo Left: Assistant Secretary Durkovich responds to a participant question during the CIPAC Plenary meeting. (DHS Photo)

The Private Sector Clearance Program

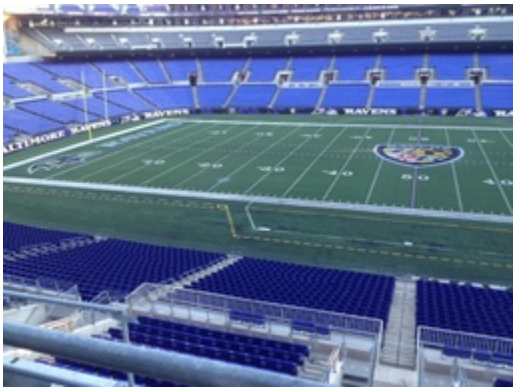
Ensuring critical infrastructure security and resilience requires ongoing cooperation between the Federal Government and the private sector. While most of the information that DHS shares with the private sector is at the unclassified level, some information may be classified, requiring a Federal security clearance.

The Private Sector Clearance Program for Critical Infrastructure ensures that private critical infrastructure owners, operators, and industry representatives— specifically those in positions responsible for the protection, security, and resilience of their assets—are processed for security clearances.

Through the use of geospatial maps and improved query capabilities, the Private Sector Clearance Program continues to enhance tools to assist Government officials in the coordination and logistics of sharing classified information with cleared private sector partners.

The Office of the Chief Security Officer provides policy oversight, manages the DHS Personnel Security Clearance Program, and is responsible for the implementation of Executive Order 13549, Classified National Security Program for State, Local, Tribal and Private Sector Entities.

SOPD Co-Sponsors Stadium Tabletop Exercise



Eighty participants and observers from the Maryland Stadium Authority, Baltimore Ravens and officials from the Federal, Maryland, and Baltimore governments held a Tabletop Exercise at the M&T Bank Stadium in Baltimore on September 24, 2013. The exercise focused on information sharing, public messaging and response to a game day incident. The lessons learned will assist in updating the sports leagues' Sector-Specific Tabletop Exercise Program, a modifiable "tabletop in a box" that can be sent to stadium owners and operators across the country to assist in building an exercise.

Photo Right: Photo by Monika Junker (DHS Photo)

Mission Spotlight: Critical Resources Branch

The Office of Infrastructure Protection (IP) is the Sector-Specific Agency (SSA) for the Commercial Facilities and Emergency Services Sectors, which is managed by a team of individuals part of the Sector Outreach and Programs Division Critical Resources Branch. The branch also serves as the IP Sector Liaison to the Government Facilities and Health Care and Public Health Sectors.

Sector-Specific Agencies increase and sustain coordination and information sharing through public-private partnerships, enhance effective dialogue, and support planning to strengthen risk management capabilities and resilience. Although each sector has unique characteristics that require specialized knowledge and security expertise, they also share core mission processes, goals, and objectives, as outlined in the NIPP 2013.

The Commercial Facilities and Emergency Services SSA is responsible for ensuring that public-private partnerships exist to:

- Bolster security and resilience in places of mass gathering (e.g., stadiums, entertainment districts, theme parks, commercial buildings, and retail centers) by engaging national-level partners that use the open public access model with multiple options for deterrence
- Collaborate with organizations and Federal, State, local, tribal, and territorial governments that are responsible for the Nation's first line of defense to save lives, protect property and the environment, assist communities impacted by all-hazards, and aid recovery from emergency situations

Some of the SSA core responsibilities include:

- Identification of capabilities for partners to maximize their critical resources in securing our Nation
- Fostering sector-specific capacity-building products, education, training, and conduct security-focused exercises
- Collaborating with partners to identify dependencies and interdependencies between sector assets and other critical infrastructure sectors

For more information, contact:
Emergency Services - ESSTEAM@hq.dhs.gov;

Commercial Facilities - cfsteam@hq.dhs.gov

Please click here to return to the top of The Partnership Quarterly

Meet the Critical Resources Branch Leadership Team

Wilson (Dave) Crafton, Critical Resources Branch Chief – Dave is a retired Air Force Colonel whose assignments included public-private partnerships with the National Communications Systems, where he was responsible for representing 23 Federal departments and agencies and 30 private sector corporations. He is currently responsible for operational oversight and guidance for the Critical Resources Branch for partnerships for both the Commercial Facilities and Emergency Services sectors.

Daniel (Dan) Schultz, Emergency Services Sector Section Chief – Dan is a former Explosive Ordnance Disposal Team leader and has worked in numerous worldwide assignments focusing on explosive and HAZMAT threats and issues, the development of the DHS Buffer Zone Protection Plan program, and the implementation of the NIPP within the Transportation and Postal & Shipping sector. He has utilized his diverse background to lead the Emergency Services Sector in its efforts to strengthen public-private partnerships and sector resilience and to collaborate with HHS, the Health Care and Public Health Sector-Specific Agency.

Bill Schweigart, Commercial and Government Facilities Sector Acting Section Chief – Mr. Schweigart's focus is on Lodging, Entertainment & Media, Real Estate, and Cultural Properties. He is a former U.S. Coast Guard officer with a background in Continuity of Operations planning, emergency management, and pandemic planning.

Andrea Schultz, CPP, Commercial and Government Facilities Sector Section Chief – Andrea is currently on detail as Acting Chief for the Critical Industries Branch. She is a former Army Explosive Ordnance Disposal technician, a Certified Protection Professional through the U.S. Department of State's Post-Blast Investigative Techniques program, and holds a certificate in Global Terrorism from the United Nations. She is responsible for advancing the sector's protection and resilience capabilities in an all-hazards environment as well as collaborating with the Federal Protective Service and the Government Facilities Sector-Specific Agency.

Photo Left: Critical Resources Branch Leadership Team Left to Right: Bill Schweigart, Dave Crafton, Dan Schultz. Not pictured: Andrea Schultz. (DHS Photo)