ISSUE
16
May
2016

Regional Consortium Coordinating Council Newsletter

RC3

Upcoming Meetings

June 21, 2016
Full Membership Meeting

July 19, 2016
Executive Committee Meeting

August 16, 2016
Full Membership Meeting

September 20, 2016
Executive Committee Meeting

October 18, 2016
Full Membership Meeting

November 15, 2016
Executive Committee Meeting

December 20, 2016
Full Membership Meeting

*If you are not on the invite list, email sector.partnership@hq.dhs.gov.

RC3-SLTTGCC Critical Infrastructure Cybersecurity Webinar Series

You are cordially invited to participate in a joint Council Cyber Webinar Series sponsored by the Regional Consortium Coordinating Council (RC3), and State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC), in conjunction with the Department of Homeland Security/ Infrastructure Protection.

With the growing cyber security concerns and evolving cyber threats across the United States, organizations in both the government and private sector are working to better understand cyber vulnerabilities, cyber threats, and methods used to protect critical infrastructure networks. The webinar series will focus on the cybersecurity efforts of federal and non-federal government agencies as well as regionally significant organizations and stakeholders by showcasing the stories and efforts of government and community cyber initiatives. The overall goal is to create a forum for dialogue about best practices, awareness of government programs and organizational capabilities within the cyber realm. The webinars will be monthly beginning June, 2016 and will culminate in October for Cyber Awareness month.

This webinar's first presentation is “**Federal Cyber Resources and How to Tap Into Them**”, presented by Howard Tsai, Office of Cybersecurity and Communications, Department of Homeland Security. This presentation will demonstrate to participants the best way to interact with the content within the Critical Infrastructure Cyber Community Volunteer Program (C3VP) website and show the mapping between the National Institute of Standards and Technology (NIST) cybersecurity framework’s 5 core functions and its relationship with DHS cybersecurity programs.

The second presentation is "**Building the CyberMaryland Initiative**", presented by David Powell, Chief Operating Officer, Federal Business Council. This presentation will showcase Cyber Maryland, a state that is recognized as a cybersecurity leader and creates opportunities to unite stakeholders and ideas together for meaningful dialogue.

Date: June 2, 2016 at 3:00 p.m. Eastern Time
Registration: Click Here

ISSUE
16
May
2016

Regional Consortium Coordinating Council Newsletter

RC3

RC3 and SLTTGCC Conclude Regional Overview Project

Overview

RC3 and the State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC) have reached the conclusion of the Regional Overview of Critical Infrastructure Programs, a collaborative project to document the current state of critical infrastructure mission implementation across the Nation. Throughout 2015, the councils engaged over 200 critical infrastructure professionals through council-sponsored questionnaires and Virtual Roundtable Webinars to detail the structure and mission of programs and partnerships, critical infrastructure activities, and major needs and challenges.

The Regional Overview project represents Phase 2 of an ongoing RC3 and SLTTGCC effort. Phase 1 comprised the SLTTGCC Regional Initiative (2011–2013), the SLTTGCC Tribal Critical Infrastructure Capabilities and Needs study (2014), and the RC3 Member and Mission Landscape Study (2013–2014). Since Phase 1 of the project, public-private partnerships and SLTT critical infrastructure programs have continued to evolve to address the changing critical infrastructure risk landscape amidst limited resources.

The results of the project are consolidated in a Summary Report that highlights the councils' findings on the implementation of the critical infrastructure mission by public-private partnerships and SLTT programs. Included here are the project's findings related to public-private partnerships working on critical infrastructure issues, as well as recommendations submitted by the councils to the DHS Office of Infrastructure Protection (IP) to improve Federal critical infrastructure programs, tools, and capabilities utilized by partnerships. The full Summary Report can be obtained by emailing the RC3: RegionalCCC@gmail.com.

- Regional Overview of Critical Infrastructure Programs: Region Snapshots

Project Findings: Regional Partnerships

Public-private partnerships are adapting to the changing risk landscape in a limited-resource environment by focusing their critical infrastructure efforts on activities that provide the most value to their members and partners. High-value preparedness and incident response activities include hosting events, sharing information, and coordinating private sector resources and expertise. Such activities continue to provide value to public-private partnerships, as was illustrated in Phase 1. Partnerships needs for sustained success include access to additional critical infrastructure education opportunities (e.g., basic cybersecurity guidance, mass-gathering preparedness, interdependency risk), stronger connections between partnerships through continuous engagement, and improved information-sharing programs and mechanisms.

Public-private partnerships embrace a non-profit, volunteer-based governance structure and are designed to focus on all critical infrastructure issues across all sectors.

- Although most partnerships are non-profits, some are managed by a State/local agency and many collaborate with State/local critical infrastructure programs.
- Many partnerships are managed by volunteers who have full-time jobs apart from the partnerships. The level of activity and success of these partnerships depend greatly on the energy and capabilities of these volunteers. The voluntary nature of partnerships is a characteristic consistent with Phase 1 findings.
- Primary motivations for organizations to join partnerships include (1) opportunity to network, collaborate, and exchange ideas; and (2) access to a trusted clearinghouse of relevant information and training opportunities. These benefits are due largely to the broad focus of partnerships, which often span all critical infrastructure issues across all sectors.

Public-private partnerships actively contribute to the critical infrastructure security and resilience mission through valued preparedness and incident response activities, including hosting events, sharing information, and coordinating private sector resources and expertise.

- Partnerships offer their members value by enabling networking and access to trusted information and training opportunities; this is consistent with Phase 1.
- Preparedness and steady-state activities include gathering and supporting the dissemination of information (e.g., reports, surveys, briefings, and training opportunities), hosting or conducting events (e.g., workshops, exercises, meetings, and conferences), and facilitating relationship development and direct contact between public and private sector stakeholders.
- Incident response activities include coordinating private sector resource allocation and distribution, integrating private sector personnel within SLTT EOCs, and sharing situational awareness information.
- Sectors most often engaged by partnerships relating to these activities include Energy, Emergency Services, Information Technology, Healthcare and Public Health, Financial Services, and Commercial Facilities.

Sustainability is a major concern for public-private partnerships across the Nation. In order to continue to demonstrate value through relevant activities for critical infrastructure stakeholders, partnerships need access to additional critical infrastructure education opportunities, stronger connections between partnerships, and improved information-sharing programs and mechanisms.

- Adaptation to the changing risk environment requires continued education and awareness regarding prominent and emerging critical infrastructure issues (e.g., basic cybersecurity guidance, mass-gathering preparedness, interdependency risk). Partnerships are commonly interested in more and advanced critical infrastructure security and resilience education opportunities relating to such issues.
- Continuous, routine engagement of stakeholders (through meetings, conference, exercises) is imperative to sustain partnerships, especially in the time between incidents or disasters when it is difficult to maintain the momentum

of private sector participation. More robust connections are needed among partnerships, the private sector, and government in order to maintain partnership viability and share best practices. These challenges and needs are consistent with Phase 1.

- Providing accurate, timely, and actionable information is important to critical infrastructure security and resilience. Information sharing is a core capability of partnerships and is one of the principal ways partnerships show value to their members. In order to be better prepared, informed, and able to respond effectively, improved information-sharing programs and mechanisms are needed. Key improvements include coordination of Federal, SLTT, and private sector platforms (e.g., HSIN, fusion center, Information Sharing and Analysis Center [ISAC] portals); integration of mobile computing technologies (including social media); and stronger protections for sensitive private sector information.

Project Recommendations: Federal Programs Utilized by Partnerships

Recommendations to improve Federal programs utilized by partnerships pertain to grants, exercises, regional capacity building, information sharing, and DHS field offices.

Grants: Update the State Homeland Security Grant Program and Urban Areas Security Initiative guidance documents. Ensure eligible expenses reflect current public-private partnership needs, such as:

- Mechanisms to access real-time local and regional threat information, collaborate, and share best practices (e.g., sustaining engagement in steady state and emergency, regional resilience planning, business continuity plans).
- Integration of private sector representatives into emergency operations centers (in-person or virtually).
- Training (with technical assistance) for private sector-specific issues. Topical needs include cybersecurity response, supply chain issues in response/recovery, soft target threats, and active shooter response.
- Exercises coordinated with public and private sector participants. Topical needs include cybersecurity response and regional sector dependency identification and management.
- Collaborative projects between two or more public-private partnerships.
- Common, user-friendly business processes for all-hazards risk management.

Exercises: Consolidate and disseminate a suite of successful exercise scenarios for use by SLTT agencies and partnerships in running critical infrastructure exercises, such as:

- Joint exercise across SLTT agencies and with the private sector
- Regional exercise testing sector dependencies
- Cybersecurity incident (e.g., cyber attack, cyber-physical dependency incident)
- Soft target attack (e.g., shopping malls, schools)
- Public health incident
- High-risk transportation security incident

Regional Capacity Building: Sponsor regional forums—in collaboration with the RC3 and SLTTGCC—to improve regional capacity, facilitate the sharing of best practices across SLTT programs and partnerships, and enable collaboration with peers and experts on emerging issues.

- Develop an action plan to implement regional collaboration between DHS IP, RC3, and SLTTGCC partners. Coordinate the development of regional forums and the action plan with DHS regional capacity pilots and projects.

Information Sharing: Develop a toolkit to facilitate more robust information sharing between SLTT agencies and private sector owners and operators. Include a listing of resources and where to obtain more information for the following topics:

- Overview of PCII uses and limitations
- Information security markings at the Federal, SLTT, and private sector levels
- Overview of State sunshine laws and public records laws
- Operational mechanisms for sharing real-time information during emergencies (e.g., memoranda of understanding and agreement, nondisclosure agreements)
- Common methodology for engaging SLTT fusion centers as the primary hub of information sharing between public and private stakeholders
- SLTT interaction with Information Sharing & Analysis Organizations (ISAOs)

DHS Field Offices: Future DHS National Programs and Partnerships Directorate regional offices should:

- Serve as coordination hubs for DHS field personnel, SLTT programs, and partnerships. A centralized framework for critical infrastructure coordination would increase efficiency of stakeholder activities, reduce redundancy, and provide more opportunities to bring valued critical infrastructure activities to a broader audience.
- Include additional Protective Security Advisors (PSAs) and CSAs, based on SLTT and partnership needs. PSAs are integral to the effectiveness of many SLTT programs and are increasingly relied upon to lead and support critical infrastructure activities, especially conducting infrastructure assessments and engaging the private sector. As more SLTT focus and resources are directed to cybersecurity, CSAs can provide exceptional value to SLTT programs and partnerships by coordinating cybersecurity assessments, education, guidance, and training from the Federal Government.

Next Steps

The councils look forward to continuing related engagements by hosting Webinars and reaching out to colleagues to learn more from those focused on critical infrastructure across the country.

If you want to find out more about the project, please email RegionalCCC@gmail.com or SLTTGCC@hq.dhs.gov.

Upcoming Events

Register Now: DHS I&A Corporate Security Symposia—The DHS Office of Intelligence and Analysis (I&A) Private Sector Outreach Program provides continuous opportunities for public and private sector entities to engage with one another. The Private Sector Outreach Program's Corporate Security Symposia are a series of regional conferences held around the country to generate discussion regarding some of the most challenging cross-sector issues our Nation faces today. Each corporate security symposium is a day-long event bringing together government and private sector subject matter experts for the benefit of private sector attendees.

The Corporate Security Symposia typically focus on topics that are critical to security – both within the private sector and the public sector. Events feature prominent speakers from both private and public backgrounds, shedding light on issues such as cyber security, infrastructure protection, communications, global intelligence, border security, and counterintelligence. Past private sector companies that have hosted Corporate Security Symposia include Fortune 500 companies such as Sony, the Walt Disney Company, Gulfstream and Microsoft.

- Tuesday, June 7, 2016; Chicago, IL.
- Tuesday, June 21, 2016; Denver, CO.
- Wednesday, August 24, 2016; Las Vegas, NV.
- Tuesday, October 4, 2016; New York, NY.
- Tuesday, November 1, 2016; Cincinnati, OH.

To RSVP or if you have any questions, please email at I&APrivateSector@hq.dhs.gov.

2016 America's Small Business Summit, June 13 – 15, 2016, Washington D.C.—Join more than 800 business owners and chamber executives from across the country in Washington D.C. on June 13-15, 2016 to network, hear from business and policy experts, and tell Congress what your business needs to succeed. The action packed event will feature high caliber keynotes, small group breakout sessions, business to business matchmaking workshop, and a variety of other networking opportunities. Learn more

Regional Cyber Regional Cyber Resilience Workshop, June 23-24, 2016, Rockville, Maryland—There is a considerable body of knowledge, governance structures, tools and techniques that have been developed to address regional resilience from a physical infrastructure perspective. However, there has been little done to date to understand and address cyber resilience at a regional level. Even the definition of what constitutes regional cyber infrastructure and whether that is a useful context for examining regional resilience are open questions. As a result, a number of regional consortia, organizations, and programs have begun to focus on this regional cyber challenge and are considering options for addressing regional cyber resilience in a meaningful manner. Please join us on June 23-24 2016, for the inaugural Regional Cyber Resilience Workshop. The workshop will be held at the NCCOE facility located at 9700 Great Seneca Highway, Rockville, MD 20850. You will:

- learn how regions are defining and tackling regional cyber resilience
- acquire information on emerging research, tools and techniques you can use at the regional level
- have a chance to meet with thought leaders from other regions to compare needs and requirements

The registration website is now open. Please register at https://register.mitre.org/regionalcyber/. If you have any questions, please contact Stacey Stanchfield, sstanchfield@mitre.org or 703-983-5225.

National Homeland Security Conference, June 28 – 30, 2016, Tampa, Florida—The National Homeland Security Association sponsors the National Homeland Security Conference. The Conference is the annual meeting of local Homeland Security and emergency management professionals from the Nation’s largest metropolitan areas. It has become the best attended and most highly anticipated homeland security and emergency management conference of the year as it focuses on all emergency response disciplines at all levels of government. Learn more

Sixth National Conference on Building Resilience through Public-Private Partnerships

Attend the Sixth Annual Building Resilience through Public-Private Partnerships (P3) Conference this summer in Colorado Springs, CO, on August 30-31, 2016. Hotel, registration, and event information coming soon!
Based on the terrific response to the earlier call for topics, the conference planning team is including a new portion of the agenda on Public-Private Partnership Talks or "P3 Talks." These presentations are intended to share an idea, program, or concept related to building resilience through public-private partnerships.

To Participate: Submit your P3 Talk proposal using the guidelines below to PPPConference@hq.dhs.gov by May 27, 2016. This is a separate request from the Call for Topics. If you have a presentation that meets the below criteria, please submit a proposal regardless of whether or not you responded to the Call for Topics.

- Your P3 Talk submission must include a title and executive summary of 200 words or less and a YouTube link to a 3-5 minute video of the presentation to screen applicants for quality control.
- The Conference Planning Team will post a survey that will include the title/executive summary for each of the submissions for a vote in early June to select the top P3 Talk proposals.
- The Conference Planning Team will notify the individuals that rank the highest in the survey.

Criteria:

- Must be focused on building resilience through public-private partnerships.
- Must be tied to this year's theme: "Building and Leading Successful Partnerships in an Evolving Risk Environment."

- Total time allotted for each P3 Talk presentation will be 20 minutes followed by 10 minutes of Q & A.

For questions and comments please contact PPPConference@hq.dhs.gov.

Secure 360 Conference, September 19, Des Moines, Iowa—SAVE THE DATE! Secure360 is the premier educational conference in the Upper Midwest for the information risk management and security industry. The conference is supported by the Upper Midwest Security Alliance (UMSA). UMSA is proud to present Secure360 Iowa, the first expansion of the Secure360 Conference which celebrated its 10-year anniversary in 2015! Secure360 Iowa website

Secure 360 Conference, September 26, 2016, Brookfield, Wisconsin—SAVE THE DATE! Secure360 is the premier educational conference in the Upper Midwest for the information risk management and security industry. The conference is supported by the Upper Midwest Security Alliance (UMSA). UMSA is proud to present Secure360 Wisconsin, the first expansion of the Secure360 Conference which celebrated its 10-year anniversary in 2015! Secure360 Wisconsin website

Cyber Security Summit, Tuesday, October 11 and Wednesday, October 12, 2016, Minneapolis, Minnesota—SAVE THE DATE! Learn more.

2016 IAEM Conference—International Association of Emergency Managers, October 14-19, 2016, Savannah, Georgia—Conference—more information.

FBI Citizens Academies—Want to find out first-hand how the FBI works? Hear how the Bureau tracks down spies and terrorists? Learn how to collect and preserve evidence? See what it is like to fire a weapon and put yourself in the shoes of a special agent making a split-second, life-or-death decision? If you are a leader in your community, you just might be able to do that and more—through an FBI Citizens Academy, open for business in all 56 of our field offices. Learn more

Connect with us and be social

The RC3 is looking for membership engagement and would like to hear from you! If you have ideas for our membership webinars, newsletter articles, blog stories...please send them to our Communications Chair, Erica Wirtz. If you would like to join our distribution list, email Secretariat Support.

- Visit our website
- Read our blog
- Join us on LinkedIn
- Like us on Facebook