Homeland Security

National Infrastructure Protection Plan (NIPP) Security and Resilience Challenge

2016 NIPP Challenge Submissions Selected for Development and Implementation

Interstate National Gas Association of America – Improving Cyber Threat Information Sharing (Oil and Gas Sector Coordinating Council)

Goal: Facilitate and encourage the automated sharing of cyber threat information, including indicators of compromise, between members of the natural gas pipeline sector.

Bay Area Center for Regional Disaster Resilience – Toolbox to Enable Risk-Based, Cross-Sector Decision-Making for Regional Critical Infrastructure Security and Resilience (RC3)

Goal: Produce and test a toolbox of closely integrated, customizable, and scalable "products," which together enable cross-sector information sharing and decision-making to improve regional critical infrastructure security and resilience.

American Water Works Association– Improving Cybersecurity for Small and Medium-Sized U.S. Water Utilities (Water SCC)

Goal: Design, develop, and deliver no-cost research workshops to equip water sector managers and operators with the skills needed to effectively use available cybersecurity resources. Effective use of these resources will result in identification of gaps in cybersecurity coverage, as well as discovery of detailed, actionable steps to address such gaps to increase security and preparedness.

ChicagoFIRST – Secure Regional Coalition Web Portal (Financial SCC and RC3)

Goal: Develop an Internet portal and workspace for critical financial sector firms to use in conjunction with public sector agencies before, during, and after local emergencies that impact the regional and national economy. The system will allow for secure access to emergency operations procedures, a messaging system, and work group areas for physical security, cybersecurity, business continuity, and regulatory compliance teams.

All Hazards Consortium – Building Common Regional Operating Picture for Disaster Resilience (RC3)

Goal: Advance the development of a sensitive information sharing framework currently being incorporated by multiple states and private sector organizations within the electric sector as part of an ongoing East Coast effort used for regional disaster/disruption responses.

Cyber Resilience Institute – Cyber Market Development (RC3)

Goal: Stimulate demand for cyber solutions by employing a community model, a marketplace environment, and tools and practical approaches that adopt commonly understood market forces principles and characteristics.

Pegasus Program – Creation of a National Crisis Event Response, Recovery, and Access Process Standard (Emergency Services SCC)

Goal: Develop a crisis event response, recovery, and access process standard that would extend efforts by the Emergency Services Sector Coordinating Council (ESSCC) to cooperatively define a process approach that could enable stronger resiliency, preparation, and response for communities during crisis events.

Defense Industrial Base Information Sharing and Analysis Center – Improving Human Resource Resilience through Two-Way, Location-Based Information Sharing (Defense Industrial Base-ISAC)

> ***Goal:*** *Improve Defense Industrial Base (DIB) human resource security and resiliency by employing proven, state-of-the-art information exchange and mobile location-based technologies that protect employees through awareness of threats and incidents as well as speed their return to work following events to assure minimal disruption of delivery of DIB products and services.*

South Carolina Sea Grant Consortium – Development of Multi-Hazard Coastal Resiliency Assessment and Adaptation Indices and Tools for the Charleston, South Carolina, Region (Charleston Resilience Network)

> ***Goal:*** *Research, design, develop, and implement multi-hazard indices and tools for Coastal Resilient Infrastructure Assessment and Adaptation for small business, municipalities, and individuals in the Charleston, SC, region, which could be adapted for use by other regions.*

Public Health Sector Coordinating Council - Handbook and Website for Healthcare & Public Health Leaders to Strengthen Risk Management and Resilience Due to Cyber, Physical and Human Threats to Critical Infrastructure Including an Electromagnetic Pulse (EMP) Event

> ***Goal:*** *Provide a handbook and website guidelines for healthcare and public health leaders on what can be done to strengthen risk management and resilience due to cyber, physical, and human threats to their critical infrastructure, including an electromagnetic pulse (EMP) event.*

***

The NIPP Security and Resilience Challenge is managed by the Office of Infrastructure Protection, within the National Protection and Programs Directorate of the Department of Homeland Security (DHS), in partnership with the National Institute for Hometown Security (NIHS).