Homeland Security

National Infrastructure Protection Plan (NIPP) Security and Resilience Challenge

2018 NIPP Challenge Submissions Selected for Development and Implementation

Cyber Risk Management Toolkit for Small Government Entities (IT Sector Coordinating Council)

Goal: Accelerate the adoption rate of the National Institute of Standards and Technology (NIST) Cybersecurity Framework in small government entities, and assist those entities in the adoption of an improved cyber posture. *Drastically reduce the cost of adoption of the NIST Cybersecurity Framework by sourcing common data, fractionalizing the effort of highly skilled analysts, and leveraging automation.*

Condition Assessment Procedures for Concrete Dams with Post-Tensioned Anchors (Dams Sector Coordinating Council)

Goal: Develop assessment and diagnostic procedures by performing a field test that evaluates the existing condition of a concrete dam and includes the influence and effects of the dam's major components, such as its foundation, reservoir, and post-tensioned anchors. *Publish requirements and process information for using modern instrumentation requirements and diagnostic and reporting procedures to effectively determine the safety of dams.*

Location Detection of Rogue Base Stations/IMSI Catchers (Communications Sector Coordinating Council, Communications Information Sharing and Analysis Center)

Goal: Research and determine actionable steps that can be used by mobile service providers and other appropriate users to detect rogue base stations and protect mobile communications critical infrastructure. *Develop a white paper that will provide research findings, recommendations for best practices, and a proposed algorithm to detect rogue base station devices in a real-world carrier network.*

Synchronization of Situational Awareness Between Critical Infrastructures and the Public Sector Using Unmanned Aerial Systems (UAS) (Regional Consortium Coordinating Council)

Goal: Develop plans, procedures, processes, and mechanisms for leveraging UAS to collect and exchange damage information to assist owners and the public sector obtain faster situational awareness on the status of their infrastructures. *Research cross-sector interdependencies between infrastructures through conducting discussion-based exercises and developing relationships across multiple sectors.*

Building Disaster Resiliency in the Public Sector by Leveraging Critical Healthcare Supply Chain Information (Healthcare and Public Health Sector Coordinating Council)

Goal: Facilitate a coordinated commercial and public response to emergencies by leveraging healthcare supply chain data to create a supply chain mapping tool. *Develop a mapping framework and formal method of communication that public agencies can access during a* *disaster to see where their private sector healthcare distributor partners are located and what supplies are available.*

Convenience Store and Fuel Retailer Emergency Preparedness: Resilience for the Last 50 Feet (Commercial Facilities Sector Coordinating Council)

Goal: Improve the resilience of convenience stores and gas stations, due to their critical and underrecognized role in community resilience. *Research and report on the current state of resilience and training materials available to convenience store retailers.*

Biopolymer-Stabilized Earth Materials for Resilient and Adaptable Infrastructures (Dams Sector Coordinating Council)

Goal: Conduct research and a field experiment regarding the properties and uses of biopolymers as a stabilization agent for soils surrounding earthen infrastructures. *Develop models to understand living organism properties for the purpose of soil improvements for rebuilding and maintaining critical infrastructure.*

Small Telecommunications Operator Information Sharing Study and Pilot Project (Communications Sector Coordinating Council)

Goal: Research how to create a long-term sustainable mechanism that helps small telecom operators actively participate in the information sharing community and receive critical cyber threat intelligence. *Create a daily cyber threat intelligence report for the small operator community to provide recipients with information and analysis on the most critical threats facing their companies and with recommendations to mitigate identified cyber risks.*

Safeguarding Patients by Enabling Accelerated Government and Utility Response through Real Time Data Sharing of Hospital Generator Status During Disasters (Healthcare and Public Health Sector Coordinating Council)

Goal: Create a prototype that utilizes remote monitoring and reporting systems to provide the status of generators in critical healthcare facilities around the country. *Create a first-in-the-nation, non-commercial prototype that harnesses the power of existing technology to dramatically improve situational awareness for government officials and utilities when emergency power at hospitals, water systems, and wastewater treatment plants is threatened.*

Phase 2: Expand/Enhance a Regional Common Operating Picture for Disaster Resilience (Regional Consortium Coordinating Council)

Goal: Achieve better unity of effort, situational awareness, and increased efficiencies between public and private sectors during incedent response. *Leverage the Sensitive Information Sharing Environment (SISE), a private sector operated trust framework, to conduct planning, exercises, and solution development in order to create mechanisms that can support and work with DHS components to share more reliable, timely, and actionable information during disasters.*

***

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