Critical Infrastructure Security & Resilience Research (CISRR)

Science and Technology

CHALLENGE: SAFEGUARDING THE NATION'S CRITICAL INFRASTRUCTURE

Organizations are facing more diverse, sophisticated threats—cyber, physical, technological, or natural—that may have cross-sector impacts. The evolving risk landscape necessitates an evolved response.

The Department of Homeland Security (DHS) Science and Technology Directorate (S&T) provides research and development (R&D) to ensure the security and resiliency of Critical infrastructure (CI). CI consists of the physical and cyber systems and assets that are so vital to the United States that their incapacity or destruction would have a debilitating impact on our physical or economic security or public health or safety. The nation's CI provides the essential services that underpin American society.

S&T CREATES PROGRAM TO MEET DHS MISSION CHALLENGES

The Infrastructure Investment and Jobs Act became Public Law #117-58 on Nov. 15, 2021, and tasked DHS S&T to conduct CI security and resilience research, development, test, and evaluation for the following areas:

1. Planning tools for conducting risk assessment ratings for special events;
2. Electromagnetic pulse (EMP) and geo-magnetic disturbance (GMD) resilience capabilities;
3. Positioning, navigation, and timing (PNT) capabilities;
4. Evaluation of "soft target" security for public safety, including countering improvised explosive device events and protection of U.S. CI;
5. Research supporting security testing capabilities relating to telecommunications equipment, industrial control systems (ICS), and open-source software.

S&T has created the Critical Infrastructure Security and Resilience Research (CISRR) Program to oversee activities performed under the Infrastructure Act and report to Congress on the progress of CISRR R&D activities.

IMPACT OF CISRR

CISRR will accomplish strategic objectives defined through S&T and CISA coordination:

- Ensure effective physical security at Special Event Assessment Rating (SEAR) events.
- Improve our understanding of the effects of EMP/GMD events on communications infrastructure.
- Work with industry to fully understand the impacts of new PNT threats and resources for industry adoption.
- Enhance soft target and crowded places security across the spectrum of prevention, protection, response, and mitigation. This includes strengthening physical security through capability advancements and countering improvised explosive devices (IEDs).
- Enhance the interoperability, integrity, reliability, and security of critical communication systems for DHS Components through the promotion and use of standards-based solutions.
- Leverage advanced methods and capabilities to inform the cybersecurity of legacy and bleeding-edge ICS systems from network-based cyber-attacks.
- Develop tools and capabilities that will enable innovation and make for a more informed, resilient end-user community that is able to mitigate security vulnerabilities and operational risk during the use of open-source software.