ICS Security Program

Industrial Controls Systems (ICS) Security Symposiums take place several times each year and bring together experts and industry leaders to present on in-depth and timely topics related to ICS and cyber security. The symposiums allow Public Safety Canada (PS) to engage with stakeholders regularly throughout the year as well as provide opportunities to update the community on security topics, and build relationships with the critical infrastructure (CI) community in Canada.

Industrial Control Systems Security Symposium
Symposium sur la sécurité des systèmes de contrôle industriels

Understanding ICS
NOW YOU KNOW

CI Cyber Partnerships also hosts focused informational sessions called **Now You Know**. These sessions include presentations and facilitated discussions, for those unfamiliar with the complexities of ICS security. The objective of these foundational sessions is to upskill Canadian CI personnel that includes management and senior officials and anyone working at CI sites where ICS are employed.

CI Cyber Partnerships' **ICS Technical Workshops** focus on the development of basic incident handler skills for the ICS environment. The objective of these training sessions is to raise awareness through hands-on experience using industry and open source tools and operating environments. Participants will be expected to have a basic to moderate level of computer security training and proficiency within a networked environment to participate.
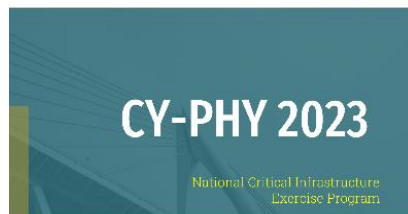

CI Cyber Exercises Program

PS conducts, coordinates and participates in **national and international cyber security exercises** to strengthen readiness and response efforts to potentially disruptive physical and cyber-based events. Through these exercises, CI stakeholders are able to validate their plans, procedures, processes that enable response, recovery, and continuity of essential operations. The planned exercises allow stakeholders to safely explore real-world situations, and to improve communication and coordination while strengthening CI partnerships.

Note: PS is also coordinating the upcoming Exercise Cy-Phy program, which is a national 2 year exercise (2022-2023) aimed at exploring the linkage between the cyber and physical security domains.

CY-PHY 2023
National Critical Infrastructure Exercise Program

EXERCISE REMOTE RESILIENCE
EXERCICE RÉSILIENCE À DISTANCE

Cyber Assessments Program

The **Canadian Cyber Security Tool (CCST and CCST 2.0)** is a virtual self-assessment tool developed by PS in collaboration with the Communications Security Establishment and its Canadian Centre for Cyber Security (Cyber Centre). The tool is specifically designed for Canadian CI owners and operators to take part in a voluntary, short, and easy to use self-assessment that provides the participant with an overview of their organization's operational resilience and cyber security posture, as well as comparative results across their sector.
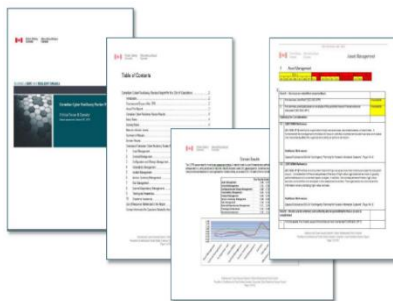
The **Canadian Cyber Resilience Review (CCRR)** offers organizations an in-depth assessment of their cyber security programs and practices. The comprehensive survey-based tool measures the cyber security of an organization, and is facilitated by a PS assessor. The participating organization receives two reports with scores across the 10 domains of the NIST Cyber Security Framework, peer comparisons, and resilience enhancement options and guidance.

Note: All assessments are free of charge. CCST and CCST 2.0 are available to CI organizations on demand through registration, and the CCRR is reserved for specific engagement requests.

CI Resilience Development Program

The **CI Resilience Development Program** aims to provide the appropriate combination of security measures, business continuity practices and emergency management planning to prepare organizations for unforeseen disruptions and natural disasters.

PS' **Insider Risk Program** includes a guide and a self-assessment tool which outlines eight security actions that can be used to initiate or enhance an organization's approach to protecting against threats from within.
(ir-ri@ps-sp.gc.ca)

The **IED Awareness Program** provides an introduction to the terrorist attack cycle, an overview of IEDs, homemade explosives, and a response to suspicious behaviors and items. This basic awareness is used to enhance bombing prevention measures.
(ps.cyberengagementsengagementscybernetiques.sp@ps-sp.gc.ca)

The guide to develop an Operational Technology and Information Technology Incident Response Plan offers summary recommendations when creating a Cyber Incident Response Plan that can be catered to the specific needs of an organization.
(ics-sci@ps.sp.gc.ca)