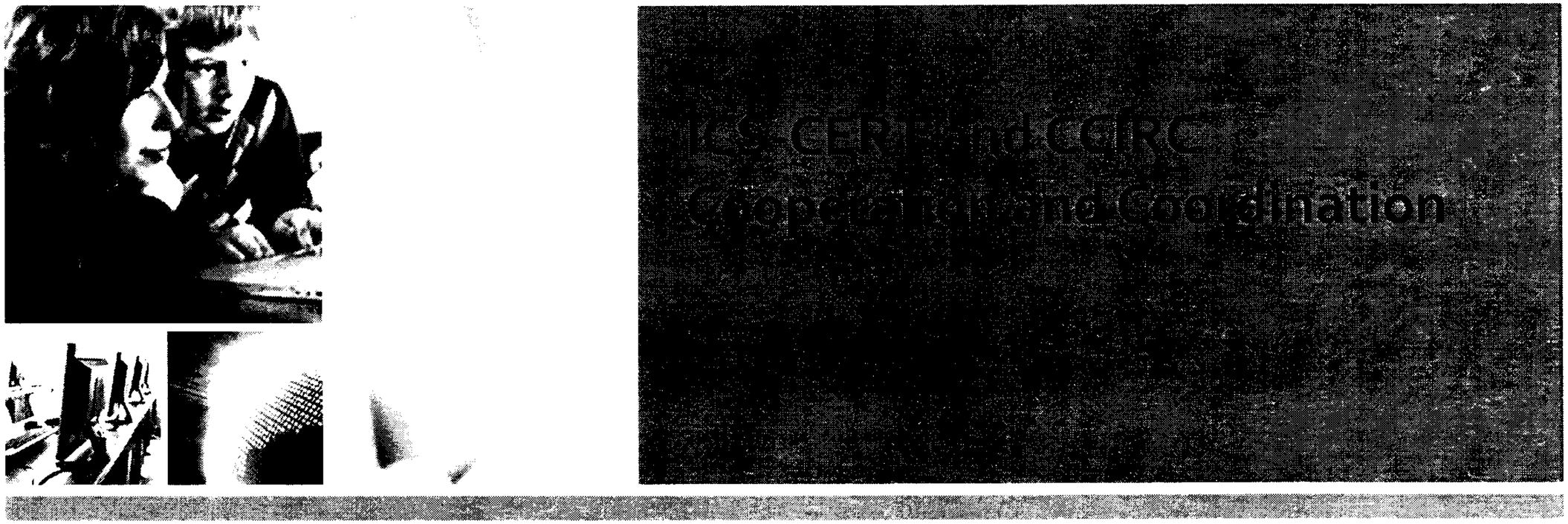
Public Safety Canada | Sécurité publique Canada

SAFE RESILIENT CANADA



November 2012
RDIMS: 724013

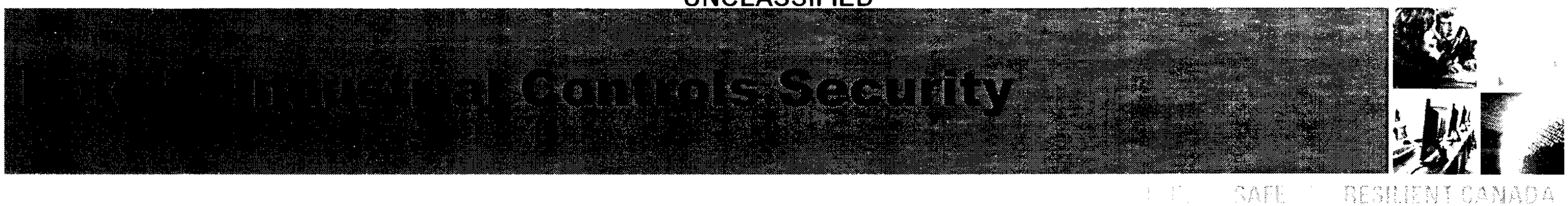
Canada

ICS-CERT

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) provides a control system security focus in collaboration with US-CERT to

- respond to and analyze control systems related incidents,
- conduct vulnerability and malware analysis,
- provide onsite support for incident response and forensic analysis,
- provide situational awareness in the form of actionable intelligence,
- coordinate the responsible disclosure of vulnerabilities/mitigations, and
- share and coordinate vulnerability information and threat analysis through information products and alerts.

http://www.us-cert.gov/control_systems/ics-cert/



CCIRC

- **Incident Handling and National Event Coordination and Assistance**
  - Direct technical assistance to partners and coordination of Government response to cyber events of national significance
  - Vulnerability and Malware Analysis, Digital Media Analysis
- **Provision of Mitigation Advice**
  - Timely development and dissemination of information on threats, vulnerabilities, and mitigation advice (ICS Security Best Practice Guide)
- **Operational Reporting and Analysis**
  - Daily, weekly, monthly and annual reports providing summary, trend, and operational analysis

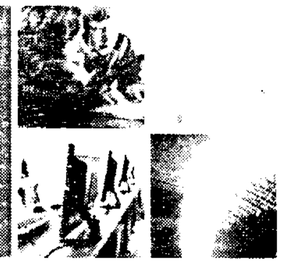
http://www.publicsafety.gc.ca/prg/em/ccirc/index-eng.aspx

CCIRC-NCSS-CERT Cooperation

Activities

- Communications and information exchange via dedicated portal
- Face-to-face meetings to establish operational points of contact and understand each others' operations
- Coordinated approach to handling cross border incidents
- Sharing of indicators of compromise

CCIRC / ICS-CERT Cooperation

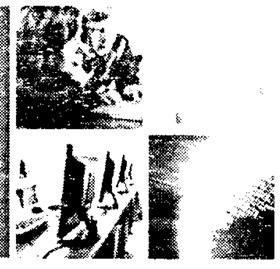


Recent Case: ICS Vendor Compromise

- Multinational with a significant Canadian footprint
- First fully coordinated non-government incident between Canadian federal S&I leads
- [redacted]
- Excellent collaboration between ICS-CERT and CCIRC

s.16(2)(c)

US-CERT Control Systems Security Program (CSSP)



- Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
- Industrial Control Systems Joint Working Group (ICSJWG)
- Information Products
- Training
- Recommended Practices
- Secure Architecture Design
- Assessments - Cyber Security Evaluation Tool (CSET®)

CCIRC Developing Capability

- Industrial Control Systems (ICS) network security test bed
  - ICS protocol vulnerability testing
  - ICS wireless infrastructure and protocol testing
- Digital media analysis capability
  - ICS and Mobile device forensics
- Threat notifications
  - Gathering of threat data
  - Warning to community members of actual or potential comprise
- Red team/Blue team exercise

Questions?

Public Safety Canada | Sécurité publique Canada

Canadian Cyber Incident Response Centre Overview

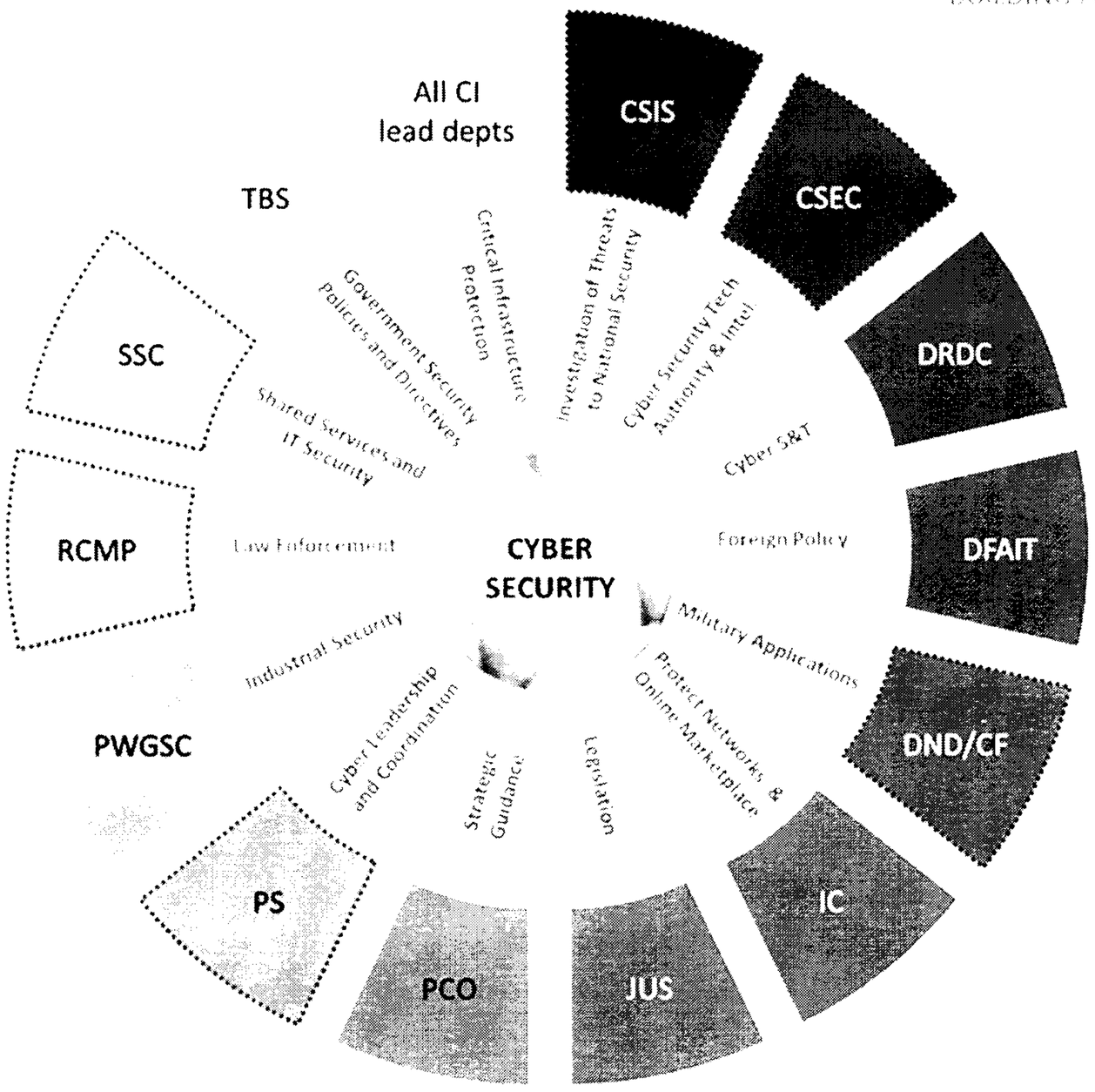
November 2012
RDIMS 604119

Canada

Outline

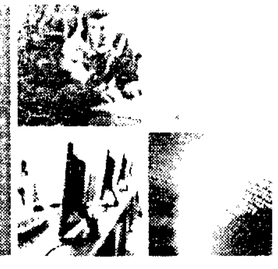
- **Government of Canada Cyber Lead Departments and Agencies**
  - Public Safety and CCIRC's roles
- **CCIRC Overview**
  - Who we are and what we do
  - Products
  - Progress
  - Partnering
  - ICS Lab Overview

BUILDING A **SAFE** AND **RESILIENT** CANADA



Departments outlined in red dotted line play a role in the *Government of Canada IT Incident Management Plan*

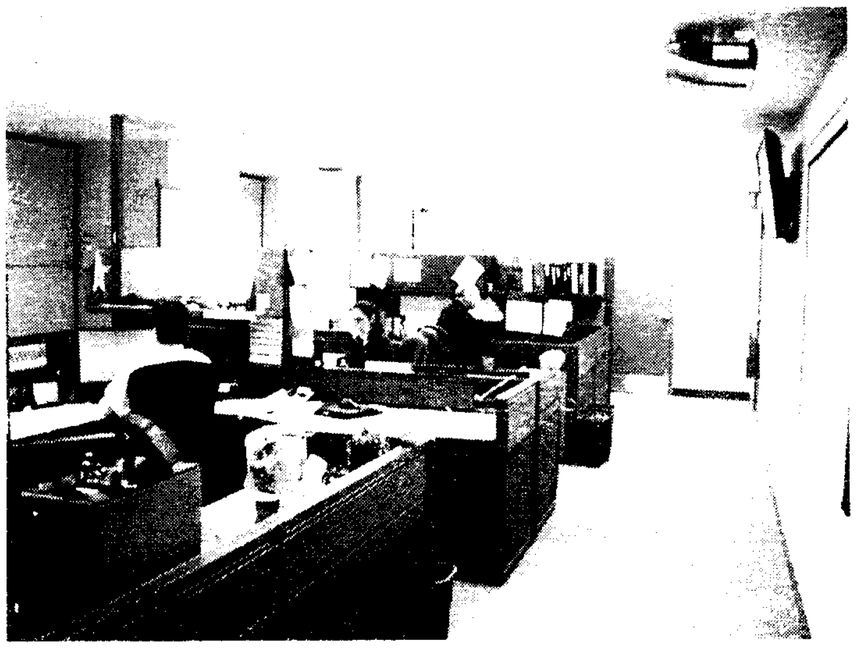
Cyber Security Roles and Responsibilities within Public Safety Canada



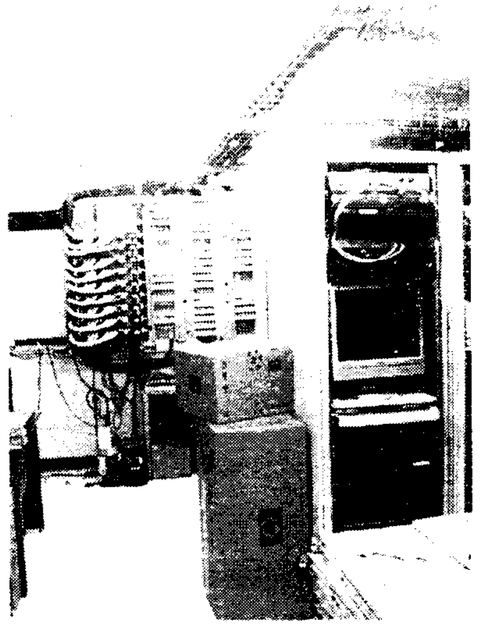
- **National Cyber Security Directorate**
  - Incident management, information sharing, and cyber policy coordination
- **Critical Infrastructure and Strategic Coordination Directorate**
  - Critical infrastructure protection
- **Communications Directorate**
  - Public Awareness

CCIRC – What It Is

- Incident response centre
  - Primary contact point into Government for domestic and international partners
  - CCIRC subject matter experts on shift duty 0600-2100, 7 days a week
  - 24/7 on-call response



- Computer lab
  - Isolated from corporate network for analyzing malicious software and testing solutions
  - Industrial control system equipment for security testing and analysis in support of CI sectors



CCIRC – Who It Is

- Personnel
  - Mainly highly specialized computer specialists (CS) with knowledge of IT security, computer forensics, and incident handling
  - Augmented by non-computer specialists for analysis of multi-source intelligence and technical data and writing strategic assessments
- Organized into three functions:
  - Incident Handling – assists partners in identifying, mitigating, and managing incidents
  - Technical Support – operates CCIRC lab infrastructure and provides technical analysis support to incident handling and analysis

  Operational Support and Analysis – builds and maintains operational relationships with partners, and produces operational analysis products for decision makers

CCIRC – Concept Of Operations

These partners

Government S&I community

Critical Infrastructure

Provinces and territories

Five Eyes and International CERTs

Trusted vendors

Academia

Cyber security expert community

Open source

provide information to

CCIRC

which provides these services

Incident Handling and National Event Coordination and Assistance

Direct technical assistance to partners and coordination of Government response to cyber events of national significance

- Audience: Operational and technical staff in partner organizations responding to cyber incidents
- Metrics: (Oct 2012 Year to Date) 722 incidents handled; 8704 notifications to partners with compromised systems; 94 requests issued to deactivate malicious systems

Provision of Mitigation Advice

Timely development and dissemination of information on threats, vulnerabilities, and mitigation advice

- Audience: technical staff in partner organizations
- Metrics: (Oct 2012 Year to Date) 15 Cyber Flashes, 43 Advisories, 12 technical products.

Operational Reporting and Analysis

- Daily, weekly, monthly and annual reports providing summary, trend, and operational analysis

Audience: technical staff, decision makers

CCIRC – Mandate

In support of Public Safety Canada's mission to build a safe and resilient Canada, CCIRC contributes to the security and resilience of the vital cyber systems that underpin Canada's national security, public safety and economic prosperity.

As Canada's computer emergency readiness team, CCIRC is Canada's national coordination centre for the prevention and mitigation of, preparedness for, response to and recovery from cyber events. It does this by providing authoritative advice and support, and coordinating information sharing and event response.

2012 – A Year of Progress

- Strengthened CCIRC's legal, policy and process foundations
  - Updated and focused mandate
  - Approved CCIRC Privacy Impact Assessment
  - Developing comprehensive Standard Operating Procedures suite
  - Standardized reporting criteria, impact assessment guidelines and information sharing protocols
- Expanded collaboration with external and internal partners
  - Enhancing trust through partner Non-Disclosure Agreements – MOUs
  - Secure collaboration via the CCIRC Community Portal
  - Tactical synchronization between CCIRC, the GOC and PS Communications
  - Validation through incident reporting trials with Ontario, Alberta and Manitoba
  - Harmonization with partners via part time personnel exchanges (DHS, GC CTEC)
- Enhanced analytic capability
  - Service consistency through the implementation of a comprehensive training package for CCIRC personnel
  - Increased analytic capability provided by the acquisition of a world-class malware analysis lab
  - Extended expertise and credibility with the development and deployment of an Industrial Control Systems (ICS/SCADA) Lab

Milestones

- Transition to 15/7 operations effective Nov 5, 2012
- Industrial Control Systems Best Practices Guidelines published
- Behavioral Analysis using Virtualization and Experimental Research
  - Automated Malware Analysis Capability
  - Integration of analysis engines for both static and dynamic malware analysis
  - Additional staffing within the technical analysis team
  - Media analysis enhancement, including mobile forensics
  - 21,000,000+ malware samples
  - Automated extraction of indicators
- Quarterly Operational Summary
- IN12-502 CCIRC Products and Services
  - Inform partners of recent changes at CCIRC including new procedures to work in collaboration with the CCIRC and access its products and services.
- Third-Party CCIRC Assessment (Starting end-November 2012)
- Weekly Technical Report with Network Indicators

Where CCIRC fits in Canada's Cyber Security Strategy

- Securing Federal Government Systems

Key actors:

- CSEC
- Shared Services
- TBS CIOB
- Canadian Forces

- Partnering to Secure Vital Systems Outside the Federal Government

Key actors:

- PS CCIRC, NCSD, CISCD
- CI Sector lead departments

Existing effort:

- PT, select CI (telecom, energy, finance)
- US-CERT, ICS-CERT
- Other U5 CERTs
- trusted vendors (possible area of collaboration with DHS/US-CERT)

Future effort:

- international CERTs
- remaining CI sectors
- economic interests
- academia

- Helping Canadians to be Secure Online

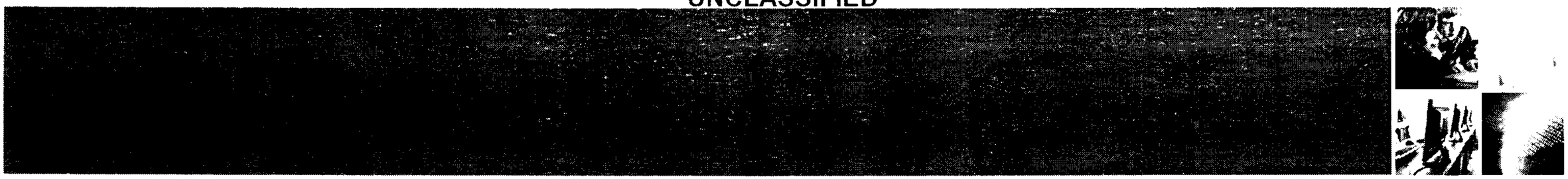
Key actors:

- PS Communications
- law enforcement
- Industry Canada
- CRTC
- Privacy Commissioner
- Competition Bureau

Audiences:

- Home users
- Academia
- Small business

State-sponsored cyber espionage — *Risk* — Crime

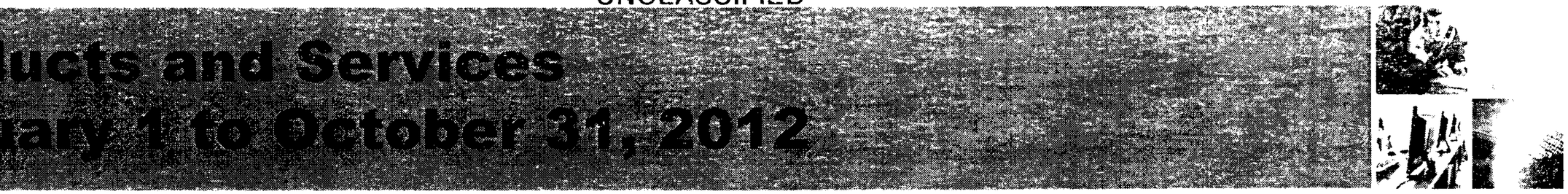


Currently Produced | In Development

Product	Daily Report	Weekly Technical Report	Cyber Flash	Alert	Advisory	Technical Report	Information Note	Weekly Statistics Report	Cyber Operational Summary	Cyber Notifications and SITREPs	Quarterly Report	Annual Report
Description	Daily situation report	Summary of daily reports, CCIRC products / events / activities / indicators / and cyber reporting	Time sensitive reports for immediate security issues - Security fix not available	Cyber security advisory on threat and vulnerability - Security fix not available	Cyber security advisory on threat and vulnerability - Security fix available	Detailed report WRT a cyber security issue - Ad hoc	Report on significant cyber events - For general awareness	Weekly statistics of CCIRC activities / incidents / products	Notable cyber incidents / CCIRC products / open source reports	Provide timely awareness of noteworthy cyber incidents	Quarterly status report WRT to CCIRC incidents / products / trend analysis	Yearly status report WRT to CCIRC incidents / products / trend analysis
Clients	CCIRC / trusted GoC partners	P/T/CI/GoC operational contacts	P/T/CI operational contacts	P/T/CI operational contacts - Posted on website	P/T/CI operational contacts - Posted on website	P/T/CI operational contacts	P/T/CI/GoC - Posted on website	CCIRC / NCSD senior mgt	Public Safety / GoC / P/T/CI partners	Public Safety / GOC / PS Comms	Public Safety / GoC / P/T/CI partners	Public Safety / GoC / P/T/CI partners

Operational / Technical | Strategic

Products and Services
January 1 to October 31, 2012



Current Partnership Focal Areas

- Federal Government Partners
  - Security and Intelligence Leads
  - Royal Canadian Mounted Police - > Canadian Anti-Fraud Center, RECOL
  - Industry Canada / Competition Bureau / Privacy Commissioner
- Provinces and Territories
  - Municipalities remain a gap
- Critical Infrastructure
  - Canadian Electrical Association
  - Canadian Association of Petroleum Producers
  - Finance Sector – Bank of Canada
  - Telecommunications Sector
  - North American Electric Reliability Corporation (NERC)
- International Partners
  - US-CERT, ICS-CERT
  - Other U5 CERTs
  - International Watch and Warning Network (IWWN)
  - Forum for Incident Response and Security Teams (FIRST)

CCIRC Cyber Community Portal ▸

Home | Electric Utilities | Finance | Government | ICT | Industrial Control Systems | Manufacturing | Oil and Gas | Research | Safety | Transportation

Search this site...

Libraries
- CCIRC Documents
- Contributed and Reference Documents
- CCIRC Tools
- Incidents
- Threat Indicators
- Tools

Lists
- Calendar
- FAQ
- Site Members
- Links

Discussions
- Team Discussion

Announcements

Title	Body
Portal testing has started	Community portal testing has started. Feedback to [redacted]
BIOS exploit : a reality	Looking into many reports of exploits for various BIOS versions. Academic paper are increasingly being published with POC.

CCIRC Documents (see more...)

Type	File Size	Name	Date Published
	12 KB	CF12-005_FR	4/24/2012
	11 KB	CF12-005_EN	4/24/2012
	13 KB	CF12-004_EN	4/3/2012
	15 KB	CF12-004_FR	4/3/2012
	8 KB	CF12-003_EN	3/30/2012
	9 KB	CF12-003_FR	3/30/2012

Contributed and Reference Documents (see more...)

Type	File Size	Name

There are no items to show in this view of the "Contributed and Reference Documents" document library.

Security Partners

- RCMP-GRC
- CBSA-ASFC
- CSIS-SCRS
- ITAC-CIET
- GOC-COG
- DRDC-RDDC

Tools

Title

Team Cymru Golden Networks Change Monitoring

Team Cymru tracks the network status of key name server IPs, containing prefix, and ASN, as well as observed DNS response times from a variety of points within the network.

Team Cymru Root DNS Monitoring

Team Cymru monitors a number of key name servers vital to the operation of the Internet.

National Vulnerability Database

CVE® is a publicly available and free to use list or dictionary of standardized identifiers for common computer vulnerabilities and exposures.

Zeustracker block list

With the ZeuS Tracker you are able the generate a IP- and domain-blocklist which contains all ips / domains which are currently used as Command&Control server (C&C) by the ZeuS crimeware. Both blocklists will be generated in text format. This alows you to import the blocklist into your firewall or corporate webproxy to block all traffic to the malicious ZeuS C&C servers.

s.16(2)(c)

SCADA Lab Project Overview

- Establishment of a SCADA network security test bed model within the Public Safety Canada CCIRC (Canadian Cyber Incident Response Centre) secure lab facility.

- Each test bed model establishes a capacity to implement and evaluate various SCADA network architectures and key security technologies.

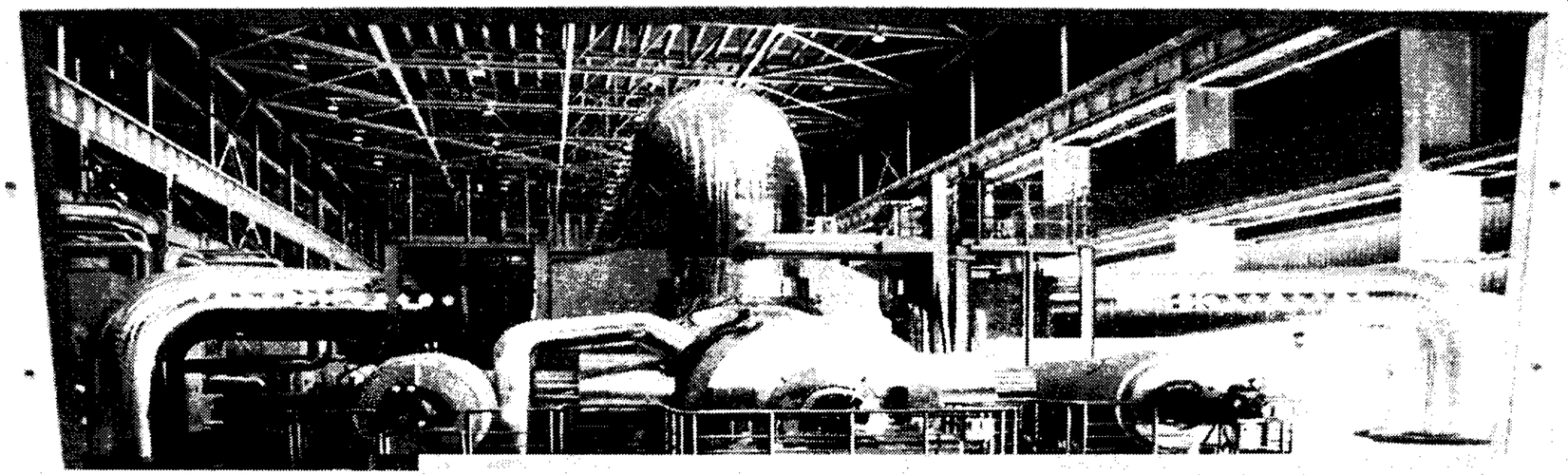
- A key objective is to build greater capacity among Canadian government, industry and academia in the area of SCADA network security.

- Models should be built in such a way that they could be organically extended to increase in scope, size and type of industrial processes.

Project Outcomes

- Two (2) SCADA network security test bed models composed of industrial control devices from multiple vendors were developed and delivered:
  - Oil & Gas Industry test bed
  - Power generation test bed
- Best Practices Guide for securing SCADA networks.
- Red Team/Blue Team exercise environment with practical threat scenarios.
- Establishes a capacity to implement and evaluate various SCADA network architectures and key security technologies including firewalls, intrusion detection systems, specialized network forensic tools, and security testing tools for industrial systems.

SCADA Test Bed Model



Next Steps

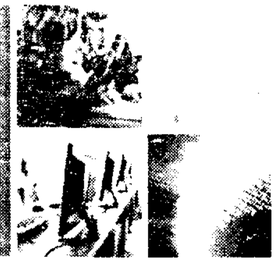
- Establish institutional relationships with federal, provincial, and private sector organizations with existing or emerging SCADA cyber security programs.

- Publish Technical Report Summarizing the SCADA Best Practices Guide.

- Utilize the test beds as a vehicle for validating the security posture of SCADA network components that are deployed and utilized in Canada.

- Further development of CCIRC capacity and capabilities for SCADA network security, leveraging the tools, techniques, and lessons learned during the project.

Contacting CCIRC



s.16(2)(c)

- E-mail:
  - Main Incident Handling mailbox:
  - Public mailbox used to report incidents: cyber-incident@ps-sp.gc.ca
  - Products and Notifications distribution mailbox: CCIRC-CCRIC@ps-sp.gc.ca
  - Malware and suspicious email intake:
  -
- Phone:
  - Local :
  - Toll-free:
- Portal:
  - Send account request to CYBERDO
- Website:

  http://www.publicsafety.gc.ca/prg/em/ccirc/index-eng.aspx

Public Safety Canada | Sécurité publique Canada

Emergency Management Ontario

RCMP·GRC

2012 Control Systems Security Workshop
HYATT Regency, Toronto, Ontario
370 King Street West
Agenda
Monday, November 19, 2012

08:00 - 08:30	**Registration** (identification required)
08:30 - 08:45	**Welcome and Opening Remarks** Allison J. Stuart, Assistant Deputy Minister/Chief, Emergency Management Ontario
08:45 - 09:15	**State of Control Systems Cyber Security** Mike Chaney, Department of Homeland Security
09:15 – 9:45	**Cybercrime Threat in Control Systems** Lee Shields, Royal Canadian Mounted Police
9:45- 10:30	**Networking break**
10:30 - 11:15	**Current Threats and Trends** Joel Langill, SCADAhacker
11:15 - 12:00	**Smart Grid and Advanced Metering Infrastructure Security Research Activities** Mark Fabro, Lofty Perch
12:00 - 13:00	**Lunch break**
13:00 - 13:45	**Hack Session** Joel Langill, SCADAhacker
13:45 - 14:30	**Cyber Security Evaluation Tool and Control Systems Cyber Security Training Opportunities** Mike Chaney, Department of Homeland Security
14:30 - 15:00	**Networking break**
15:00 - 15:45	**National Energy Infrastructure Test Centre** Dr. Felix Kwamena, Natural Resources Canada **Cyber Security Partnership Program** Tom Campbell, Public Safety Canada
15:45 - 14:00	**Closing remarks**

Public Safety Canada | Sécurité publique Canada

RCMP·GRC

2012 Control Systems Security Workshop
HYATT Regency, Toronto, Ontario
370 King Street West
Agenda
Tuesday, November 20, 2012

08:00 – 08:30	**Registration** (identification required)
08:30 – 09:15	**SHODAN search engine** Bob Radvanovsky, Infracritical
09:15 – 10:00	**Analysis first! A Model for Actionable Critical Infrastructure Cyber Intelligence** Sean McBride, Critical Intelligence
10:00 – 10:30	**Networking break**
10:30 – 11:15	**Real Time Forensics on SCADA/ICS: A Technical Case Study** Mark Fabro, Lofty Perch
11:15 – 12:00	**Control Systems Security Program cyber security products and services for owners and operators of Control Systems** Mike Chaney, Department of Homeland Security
12:00 – 13:00	**Lunch**
13:00 – 13:45	**Using traffic analysis to secure the power grid SCADA system** Antoine Lemay, Polytechnique Montréal
13:45 – 14:30	**Canadian Cyber Incident Response Centre** Kenneth Bendelier, Canadian Cyber Incident Response Centre
14:30 – 15:00	**Networking break**
15:00 – 15:45	**ICS-CERT/CCIRC Joint Operational Brief** Mike Chaney, Department of Homeland Security Kenneth Bendelier, Canadian Cyber Incident Response Centre
15:45 – 16:30	**Closing remarks**

Public Safety Canada | Sécurité publique Canada

RCMP·GRC

Protecting Canada's Critical Infrastructure: 2012 SCADA and Industrial Control Systems Security Workshop Toronto, Ontario

Dates November 19 - 20 2012

Event details The workshop is a two-day training and community building opportunity aimed at assisting Canada's critical infrastructure owners and operators better secure their most critical SCADA and industrial control system and information technology assets.

Recognized experts along with representatives from the federal Government will provide briefs on the latest threats and steps that can be taken to increase the security of SCADA and industrial control systems.

Benefits of attending

- ✓ Gain a greater awareness of the threats to SCADA and industrial control systems and how to defend against them
- ✓ Learn about what resources are available to assist organizations
- ✓ Learn the challenges of securing control systems and arm yourself with case studies showing what others have done and the lessons they have learned
- ✓ Learn about some of the latest research activities
- ✓ Exchange information and ideas in a trusted environment with other control systems owners and operators
- ✓ Better understand the role of government and its current capabilities

Technical level The training is lecture style (hands-off) but technical in nature and takes place at the intermediate to advanced level.

Who should attend

- ✓ Plant Managers, Engineering and Operations Management, Project Managers, Automation and Control Managers, Process Control and SCADA Engineers, Plant Engineers
- ✓ Information Security and IT Professionals in Organizations that Deploy Industrial Control Systems
- ✓ Control System Vendor Developers and Integrators
- ✓ Government Leaders Responsible for Policy and Regulation of Utilities and Other Process Control Users
- ✓ Academic and Research Laboratory Leaders

Public Safety Canada | Sécurité publique Canada

RCMP·GRC

Speakers

- ✓ Public Safety Canada
- ✓ Canadian Cyber Incident Response Centre
- ✓ Royal Canadian Mounted Police
- ✓ Department of Homeland Security Control Systems Security Program
- ✓ Mark Fabro, President and Chief Security Scientist, Lofty Perch
- ✓ Joel Langill, SCADAhacker
- ✓ Sean McBride, Critical Intelligence

Topics

- ✓ Threats and vulnerabilities
- ✓ Incident management and forensics analysis
- ✓ Architecture and operation best practices
- ✓ Emerging research
- ✓ Security technologies and standards
- ✓ Red and blue team training exercise overviews
- ✓ Procurement standards and best practices

Cost

There is no cost for entry to the workshop. All other costs (transportation, accommodations, meals, etc.) are the responsibility of the attendee.

Venue

HYATT Regency Toronto
370 King Street
Toronto, ON, M5V 1J9
http://hyatt.com/

Application to attend

Due to the sensitive nature of some of the material presented entry to the workshop will be restricted to approved participants. The workshops are limited to 150 participants.

To register send the following information to the contacts provided below.

- ✓ Name
- ✓ Position title
- ✓ Organization
- ✓ Email address
- ✓ Telephone number

Contact

Ashley Bencke
Ashley.bencke@ps-sp.gc.ca
613-990-7533

Public Safety Canada | Sécurité publique Canada

Cyber Brief
Cyber Security Partnership Program

November 19, 2012

PRIME # [illegible]

Canada

[redacted]

Leverage existing activities and investments

- Key legislation and policies
- Structural changes
- Cyber Security Awareness Month

Canada's Cyber Security Strategy

- Secure Government systems
- Partner to secure systems outside the Government of Canada
- Help Canadians to be secure online

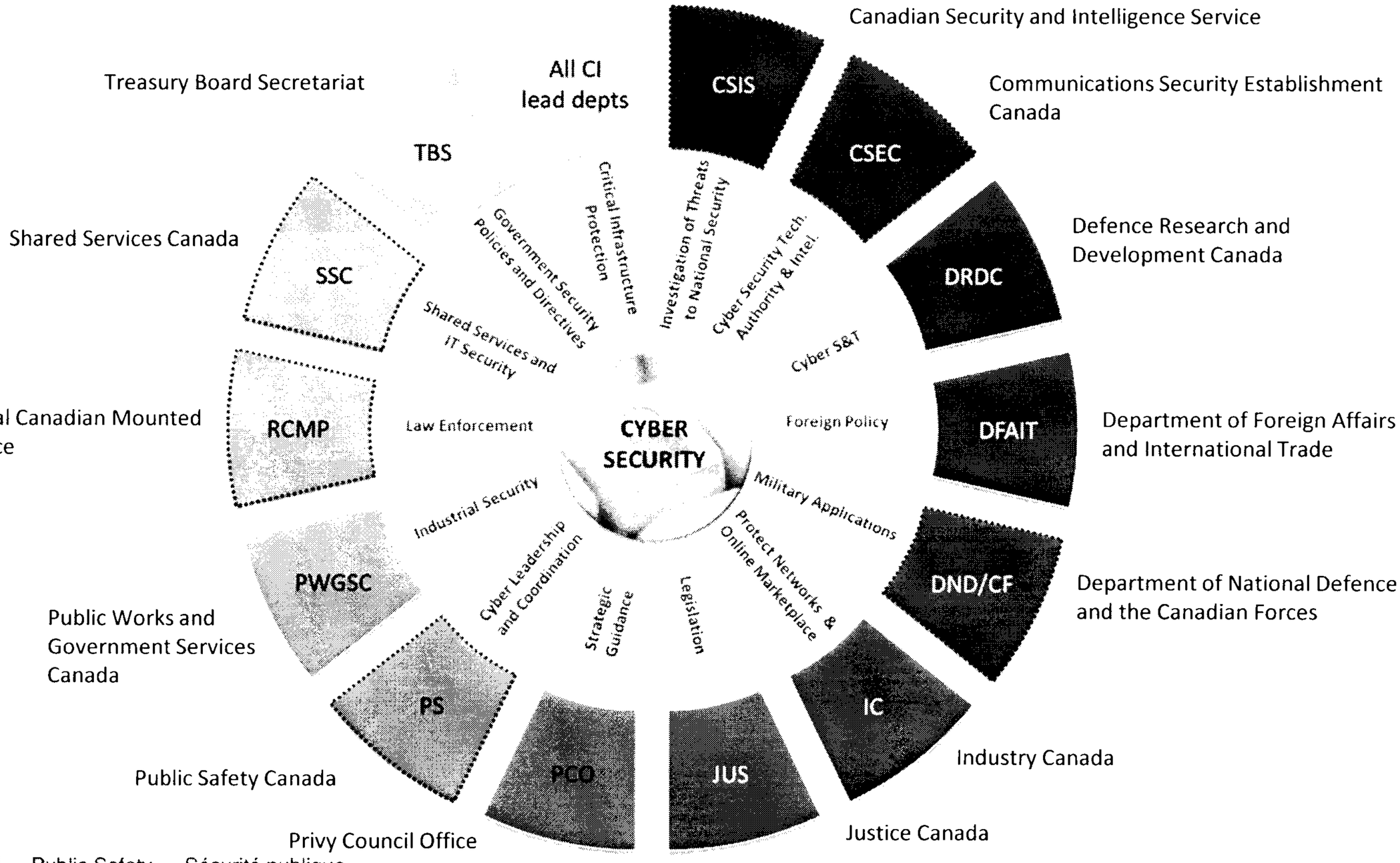
Meet our goals

- Strengthen capability
- Build credibility
- Promote awareness

Support national priorities

- National security
- Economic prosperity
- Quality of life

Roles and responsibilities with respect to cyber security



What is being done by Government

- Securing Government Systems
  - Established Shared Services Canada to consolidate and secure its IT architecture
  - Additional $155 million being invested to reinforce cyber security of federal systems

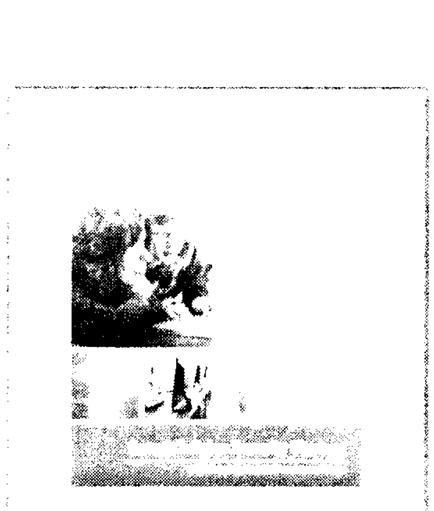
- Partnering to secure systems outside the Government:
  - Strengthened CCIRC's relationships and service offerings
  - Creating a *National Incident Response Framework*
  - Developing cyber partnership program
  - PS-DHS Cybersecurity Action Plan

- Help Canadians to be secure online
  - Launched a nationwide communications campaign

ICS and Canada's Cyber Security & Critical Infrastructure Strategies

- *Canada's Cyber Security Strategy*
  - Identified process control systems security as a key area for Government to collaborate with the private sector

- *National Strategy and Action Plan for Critical Infrastructure*
  - Established a risk-based approach for strengthening the resiliency of Canada's vital assets and systems



Challenges

- ~80% of Canadian critical infrastructure is privately owned
- The federal Government does not own or operate a significant number of critical control systems and has limited expertise in the field
- Regulation is often Provincially mandated
- Cross border impacts (i.e. electrical grid)
  - Infrastructure spans Prov-Territorial or Can-U.S. border
  - Impacts of U.S. regulation on Canada
- Heterogeneous systems
- Wide variance in sizes and capabilities of companies running ICS

What is Government doing (1/2)

- Raising awareness
  - Threat briefs
  - RCMP CI Bulletins
  - CCIRC information products

- Developing guidance
  - CCIRC ICS Security Guide

- Providing training
  - Workshop series
  - NRCan National Energy Infrastructure Test Centre

What is Government doing (2/2)

- Enhancing information exchange
  - National Cross Sector Forum
  - Canadian Security Telecommunications Advisory Committee
  - ICS compartment on CCIRC Community Portal
  - MOU signed with 32 CEA members

- Coordinating Incidents
  - CCIRC trained incidents handlers on ICS and integrated an ICS test bed into its lab
  - RCMP training tech crime investigators in cyber forensics
  - Developing National Cyber Incident Management Framework

Cyber Security Partnership Program

- Program goal
  - Improve the Government's ability to partner with owners and operators of Canada's vital systems to enhance the cyber security of those systems

- Grants and contribution funding mechanism

- Launches in 2013

- Program streams:
  - Facilitating cyber security assessments
  - Supporting the development of sector specific cyber security best practices and guidelines
  - Promoting innovation and research
  - Developing alternative measures to safeguard vital electronic systems

Program streams

- Facilitating cyber security assessments
  - Focus on vital systems (corporate and ICS)
  - Identifying vulnerabilities and mitigation recommendations
  - Facilitated self assessments
  - Looking at partnering with NERC on table top exercises

- Supporting the development of sector specific cyber security best practices and guidelines
  - Work with CI sectors
  - Achievable baseline security level

Program streams

- Promoting innovation and research
  - Cyber security research funding
  - Will complement DRDC PSTP program
  - Will consider policy, legislative, economic research
- Developing alternative measures to safeguard vital electronic systems

Other initiatives

- Develop Community of Experts
  - Harness ICS expertise and infrastructure to build a community of experts across Canada with ICS labs and/or test beds
  - Provide advice and assistance
  - Extend CCIRC's capabilities and capacity
  - Collaborate on testing

- Supporting on-site technical security training

- Suggestions?

Public Safety Canada | Sécurité publique Canada

Canada

The National Cyber Security Directorate (NCSD)

Public Safety Canada

Public Safety Canada was created in 2003 to ensure coordination across all federal departments and agencies responsible for national security and the safety of Canadians. As Canada's lead department for public safety, Public Safety Canada works with five agencies and three review bodies. They are united in a single portfolio and report to the same minister. The result is better integration among federal organizations dealing with national security, emergency management, law enforcement, corrections, crime prevention and borders. Our mandate is:

"To keep Canadians safe from a range of risks such as natural disasters, crime and terrorism."

The National Cyber Security Directorate

Public Safety Canada is the federal government lead on the Cyber Strategy. The National Cyber Security Directorate is primarily responsible for developing and implementing Canada's Cyber Security strategy. Built on three pillars, the Canadian Cyber Security strategy aims to increase cyber security of Canada through the following initiatives:

1. **Securing Government Systems**: NCSD continues to enhance the security of Government systems to better protect the private information of Canadians. This includes the sensitive business, economic and national security information on Government systems. NCSD is also aiming to ensure the continued delivery of Government services to Canadians.

2. **Partnering to Secure Systems Outside the Government of Canada**: NCSD is collaborating with Canadian Provinces and Territories, private sector, international partners and academia to implement ways to contribute to each other's efforts to understand and mitigate cyber attacks.

3. **Helping Canadians to be Secure Online**: NCSD is working towards further enhancing individual Canadians' awareness of cyber security. This is primarily achieved through October Cyber Security Awareness Month campaign, and the getcybersafe.gc.ca web presence.

The National Cyber Security Directorate is part of the National Security Directorate under Public Safety Canada, and consists of the following four sections:

The Canadian Cyber Incident Response Centre (CCIRC)

- Responsible for monitoring and providing mitigation advice on cyber threats and coordinating the national response to any cyber security incident. Its focus is the protection of national critical infrastructure against cyber incidents.

The Partnership and Engagements Team

- Responsible for the development and facilitation of partnerships with vital sectors in support of the Cyber Security Strategy. In addition, the team provides event coordination and project

management services to ongoing NCSD programs and initiatives in support of enhancing the Canadian cyber security posture.

The Technical Advice Team

- Responsible for the development and distribution of cyber-related technical advice, and for the production and implementation of a national cyber security framework.

The Policy and Issues Management Team

- Responsible for the development of international and domestic policies in relation to Canada's position on cyber security.

Services offered

The Canadian Cyber Incident Response Centre

- Incident, vulnerability and threat response products designed to increase the organizational awareness and cyber posture of the recipients
- Incident response services in the form of operational assistance involving proactive, reactive and defensive cyber security situations

The Partnership and Engagements Team

- Responsible for the design and implementation of the Cyber Security Partner Program (CSPP)
- Responsible for the facilitation and coordination of partnerships and collaboration opportunities in support of Canada's Cyber Security Strategy.
- Coordination and facilitation of security conferences and cyber based workshops.
- Coordinating the delivery of cyber security threat briefs and information sessions.

The Technical Advice Team

- Provides strategic reports such as cyber threat briefings to support decision makers.

If you would like more information on the National Cyber Security Directorate, or the services provided by the directorate, please contact the Engagement and Partnership team using the following email address:

robert.pitcher@ps-sp.gc.ca

Public Safety Canada: "Enhancing the security of government networks and systems to protect against malicious cyber threats"

The Canadian Cyber Incident Response Centre

Mandate

As Canada's national computer emergency readiness team, CCIRC contributes to the security and resilience of the vital cyber systems that underpin Canada's national security, public safety, and economic prosperity. CCIRC does this by providing authoritative advice and support, and coordinating information sharing and incident response.

CCIRC works with domestic and international partners who include provincial, territorial, and municipal governments, Canada's critical infrastructure sectors, security researchers, and international counterparts.

Products and Services

CCIRC provides a number of products and services to its partners. These include:

Incident, Vulnerability and Threat Response Products: The following products are designed to increase the cyber security awareness and defensive posture of the recipient organizations:

- ***Cyber Flash***
  - Time-sensitive reports containing threat descriptions and mitigation advice.
- ***Advisory***
  - Vulnerability reports on significant software/hardware products for which a vendor patch is available.
- ***Alert***
  - Time sensitive reports on an emerging threat for which mitigation advice is available.
- ***Information Note***
  - General cyber security information intended to enhance cyber security awareness on a specific topic.
- ***Technical Report***
  - Detailed cyber security advice for a specific issue or technology.
- ***Cyber Operational Summaries***
  - Bi-weekly and quarterly reports that provide information about cyber incidents seen by CCIRC to help support organizations' operational and security decision-making.

Incident Response Services: Operational assistance involving proactive, reactive and defensive cyber security situations comprised of:

- ***Incident Coordination***
  - Provision of incident response coordination for ongoing cyber based incident(s), 15 hours a week, 7 days a week, with 24/7 on call support.
- ***Mitigation Advice***
  - Provision of advice with the intention of increasing a client's cyber security posture.
- ***Technical Analysis***
  - Technical analysis and reporting on malware samples, digital media analysis and forensics.
- ***Victim Notifications, Code Removal Requests, Domain Deregistration Requests***
  Coordination of the notification of potential victims of cybercrime, removal of malicious content, or termination of access to a site/IP using domain registrant or Internet Service Providers (ISPs).

Partners

CCIRC's partners include the following:

- **Critical infrastructure operators**
  - Health, food, finance, water, information and communication technology, safety, energy and utilities, manufacturing , transportation, government (federal, provincial and territorial, and municipal)
- **Operators of vital cyber systems underpinning national security, public safety and economic prosperity**
  - Including but not limited to; Internet infrastructure providers (ISPs, hosting service, DNS infrastructure), Internet technology providers, operating system vendors, SCADA/ICS software and hardware providers, Internet technology vendors (routing/link HW and SW), and key software providers.
- **International counterparts**
  - National computer emergency readiness teams (CERTs)
- **Various national communities**
  - Intelligence, law enforcement, regulatory bodies, emergency management, academia, cyber security research firms and groups, and other trusted partners.

Sharing Information with CCIRC

Cyber security is a shared responsibility, and partners are encouraged to share operational information for the purposes of enhancing the Canada's cyber environment. Through collaboration, CCIRC facilitates the analysis and sharing of cyber information to reduce the risk faced by all partners. Where possible and applicable, incident reports should include the following operational information:

- Logs collected at network devices including server connections, netflow, firewall, DNS and web proxy logs;
- Suspicious emails, such as spear-phishing emails and associated header information, suspicious links and attachments;
- Malware samples;
- Infection related packet capture; and
- Metadata: any associated analysis/report performed by security teams.

Contacting CCIRC

CCIRC uses a number of communication systems to exchange with its partners nationally and internationally, at different levels of classification and sensitivity. The primary points of contact to reach CCIRC are the following:

- Email: cyber-incident@ps-sp.gc.ca
- Website: http://www.publicsafety.gc.ca/prg/em/ccirc/index-eng.aspx

Public Safety Canada "Strengthening Canada's efforts to achieve a secure, stable, and resilient digital infrastructure."