CYBER SECURITY READINESS GOALS

SECURING OUR MOST CRITICAL SYSTEMS

VERSION 1.0

Communications Security Establishment Canada
Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications Canada
Centre canadien pour la cybersécurité

Canada

Cyber Security Readiness Goals: Securing our most critical systems

D96-122/2024E-PDF
978-0-660-73264-0

Effective Date

This publication takes effect on October 29, 2024.

Revision History

October 29, 2024 First release

Message from the Head of the Cyber Centre

I am pleased to announce the publication of the Canadian Centre for Cyber Security's Cyber Security Readiness Goals (CRGs). The CRGs have been developed in response to the growing susceptibility of critical infrastructure (CI) to cyber threats. The objective of these cross-sector goals is to enhance cyber security and minimize potential risks to society, public safety, and the overall stability of the Canadian economy. Canada's CI faces an enormous challenge to be resilient against cyber threats.

Helping Canada become more resilient is key to the role of the Cyber Centre as Canada's technical authority on cyber security. The CRGs present concrete actions for CI that are worth implementing at any time. The Cyber Centre is also developing a Cyber Security Readiness Framework (CRF) that will pull together these cross-sector goals with sector-specific goals to enable CI to effectively mitigate cyber threats. The Cyber Centre is designing these resources to allow you — system owners and operators — to protect systems vital to Canadian infrastructure, national security, and public safety. By implementing these measures and adopting a cross-sectoral approach, we are establishing a strong and effective defence mechanism to collectively address the ever-changing cyber security threat landscape.

Our highest priority is to ensure the safety, security, and prosperity of Canada and Canadians. The CRGs represent a noteworthy milestone in our ongoing efforts to safeguard our vital infrastructure, systems, and services. We sincerely appreciate your support and cooperation, as you play a crucial role in the success of these initiatives. We recommend that you remain well informed of and actively engage in our collaborative cyber security endeavours.

Rajiv Gupta
Head of the Canadian Centre for Cyber Security
October 29, 2024

Overview

The CRGs consist of 36 foundational goals for improving cyber security. The goals are grouped into the six pillars of the National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0[1]. Each goal is linked to concrete recommended actions that, if taken, will elevate the cyber security posture of Canada's CI. The goals are also associated with:

- outcomes
- risks addressed
- references to the Cybersecurity Framework 2.0
- supplementary guidance

The CRGs are intended for cyber security practitioners and can be found, in full, in the Cross-Sector Goals Toolkit[2].

Although the CRGs were developed for CI, the recommendations can be used by any organization in Canada to improve its cyber security posture. The CRGs are a shared objective and a shared language that can foster connections that improve the resilience of the networks that underpin the lives of Canadians.

The cyber threat landscape is continuously evolving. As such, the CRGs will be updated regularly to support organizations in effectively mitigating emerging cyber threats. These updates will prioritize sector-specific goals and incorporate feedback from stakeholders.

1 https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
2 https://www.cyber.gc.ca/en/cyber-security-readiness-goals/cross-sector-cyber-security-readiness-goals-toolkit

Table of Contents

List of Figures

List of Annexes

THE CYBER THREAT LANDSCAPE

The security and prosperity of Canada depends on strong and resilient CI. Canadians rely on CI to deliver and support the necessities of daily life, including services like water, energy, and financial services. Disruptions to CI could result in loss of essential services, compromise of intellectual property, harm to the public, or even loss of life. As such, protecting Canada's CI is essential to national security.

Canadian CI operators and owners are confronted with an evolving threat landscape as malicious cyber activities increase in scale and sophistication. The Cyber Centre as part of the Government of Canada (GC) works with internal departments, CI operators and owners, Canadian businesses , and international partners to prepare for, respond to, mitigate, and recover from cyber incidents. The CRGs provide Canadian CI sectors with realistic, achievable goals to increase their cyber security posture; the CRGs can reduce both the number of cyber attacks and the severity of the impact from those events.

Cyber Threats Facing Critical Infrastructure Sectors

In the National Cyber Threat Assessment 2023 to 2024[3], the Cyber Centre reported that CI is increasingly at risk from cyber threat activity from both cybercriminals and state-sponsored actors. We assess that over the next two years, financially motivated cybercriminals will almost certainly continue to target high-value organizations in CI sectors in Canada and around the world.[1]

↘ Malicious Cyber Activity from State-backed Cyber Actors

CI has been a prime target for state-sponsored cyber programs of China, Russia, Iran, and North Korea. Cyber threat actors operating on behalf of state adversaries primarily use cyber threat activity to:

- advance their geopolitical objectives
- conduct cyber espionage
- pre-position in case of future hostilities
- project power and intimidate other countries

In February 2022, Russia-sponsored malicious cyber activity against Ukraine disrupted or attempted to disrupt government, finance, and energy organizations, often coinciding with conventional military operations. These attacks expanded beyond Ukraine to implicate European CI as well. For example, Russia attacked a European satellite Internet provider, which resulted in a significant outage in several European countries.[2] Cyber and military activities were also bolstered by coordinated disinformation operations to support Russia's narrative about the invasion.[3]

In May 2023, Volt Typhoon, a cyber threat group associated with the People's Republic of China, was detected in U.S. CI networks.[4] The group's primary tactics, techniques, and procedures (TTPs) involve living off the land, which uses built-in network administration tools to perform its objectives and allow the group to have persistent presence and evade detection. In February 2024, the U.S. confirmed that Volt Typhoon had compromised the IT environments of multiple CI organizations in the U.S. primarily in the communications, energy, transportation systems, and water and wastewater systems sectors.[5]

3 https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2023-2024

↘ Ransomware

CI is a particularly attractive target for ransomware. Cybercriminals perceive CI operators to be more willing to pay significant ransoms to limit or avoid physical disruption and follow-on impacts to their customers. Also known as "big game hunting", targeted ransomware attacks have hit thousands of healthcare and other CI providers, governments, and large businesses in Canada and around the world.

↘ Connected Operational Technology

CI providers are increasingly adopting information technologies (IT) to connect their operational technology (OT) environment. Internet-connected OT can make processes more efficient through better data exchange, centralized management, and automation. The global market for smart OT is expected to grow to over $4 trillion by 2030.[6] Technological improvements have accelerated the adoption of connected OT, making it even easier to connect devices remotely and at scale, including 5G and satellite Internet infrastructure. While connecting OT brings many benefits, it also increases CI providers' vulnerability to cyber threat activity.

↘ Artificial Intelligence – Enabled Technologies

CI operators and owners are also adopting artificial intelligence (AI) technologies to make their processes and operations more efficient. However, using AI technologies without proper safeguards introduces new risks to CI. The same technologies that enable CI operators to streamline their work processes, for example, through remote control of systems via a web interface, can also allow cyber threat actors to hijack OT systems and cause damage and destruction.

AI technologies, such as Open AI's ChatGPT, can be leveraged by cyber threat actors to create more sophisticated attacks including phishing, social engineering, misinformation/disinformation, and identity theft. Threat actors can also use AI to develop advanced malware that evades traditional monitoring systems and anti-virus software.

A huge concern with AI technologies is that they can provide threat actors with great powers to influence. For example, deliberate manipulation of the underlying code and the tools using it can introduce supply chain risks from insider threats at all stages, from the design level to the distribution and patching of software.

Ransomware attacks targeting critical infrastructure

MAY 2021

An attack on the Colonial Pipeline in the U.S. and on the North American and Australian operations of JBS Foods resulted in multimillion-dollar payouts for threat actors. These incidents caused significant disruptions to fuel and food supply chains.[7][8]

OCTOBER 2021

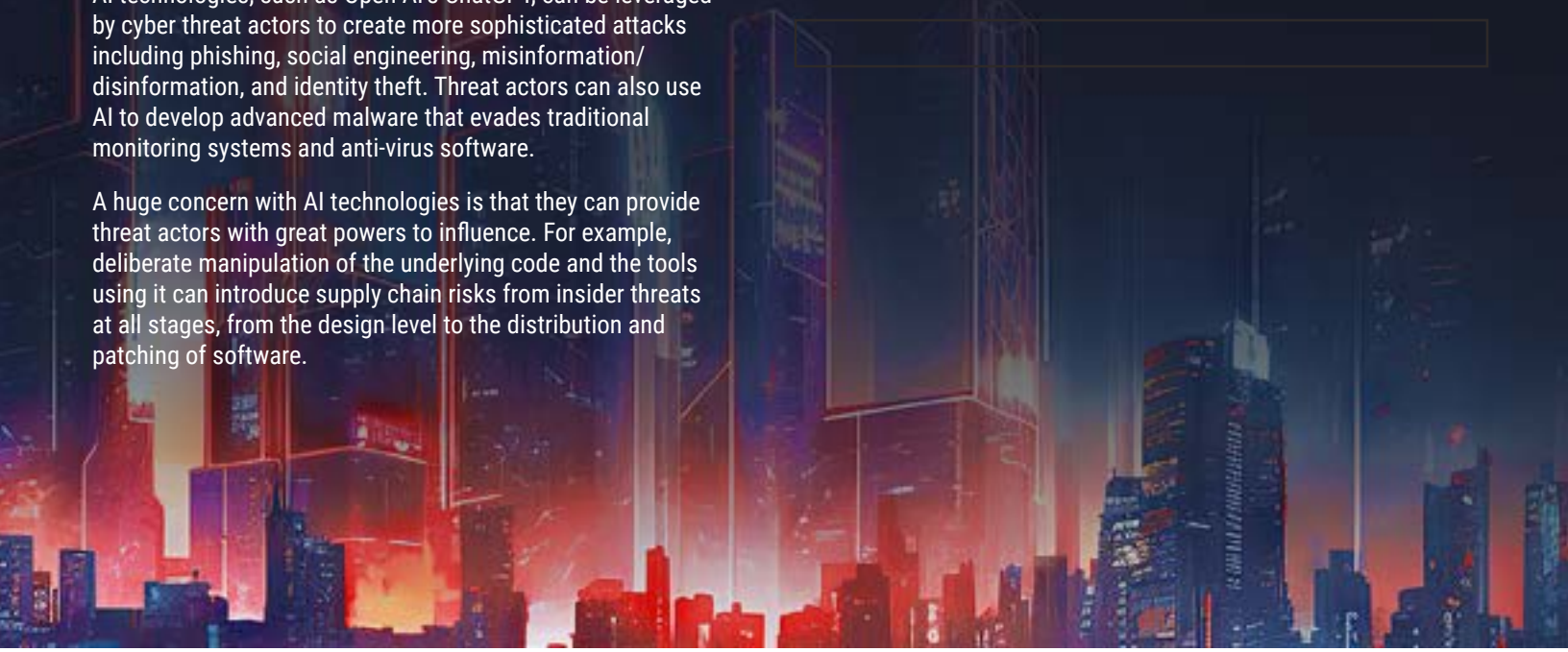
The Newfoundland and Labrador healthcare system fell victim to a ransomware attack. The Hive ransomware group was responsible for the attack that caused an IT systems outage,[9] affecting more than 1 in 10 people in the province and incurring just under $16 million in damages.[10]

DECEMBER 2022

SickKids Hospital in Toronto was attacked by an affiliate of the LockBit ransomware group. While the impact of the attack on patients and families was minimal, some patients did experience diagnostic or treatment delays.[11]

NOVEMBER 2023

There was an attempted attack on Moneris, a Canadian financial technology company specializing in payment processing. The Medusa ransomware group claimed responsibility but, according to Moneris, no critical data was accessed in the attack.[12]



HOW THE CRGs CAME TO BE

The GC recognizes the need for collaboration to secure vital cyber systems. Two consecutive National Cyber Security Strategies (2010 and 2018) have emphasized the government's leadership and facilitation role in supporting the private sector in their stewardship and implementation role.[13][14] This team approach is essential to raising the baseline of cyber security.

The Cyber Centre has created the CRGs to support investments that uplift the cyber security posture in CI. The CRGs are designed to meet the needs of system owners and operators in Canada. The CRGs are also in line with recent work of the Cyber Centre's international partners. For example:

- The UK's National Cyber Security Centre has compiled a collection of resources for organizations that play a vital role in the daily life of the UK, organizations such as those designated as forming part of the Critical National Infrastructure. This collection, known as the Cyber Assessment Framework[4] and first published in 2018, offers principles for cyber security and resilience, alongside guidance on how to apply the principles.
- In July 2021, the U.S. government established an Industrial Control Systems Cyber Security Initiative and directed the Cybersecurity and Infrastructure Security Agency (CISA) to develop cyber security performance goals for CI. CISA's Cross-Sector Cybersecurity Performance Goals[5] (CPGs) were first published in October 2022.

Value of the CRGs

The CRGs are a starting point to set Canadian CI on a path to a more resilient cyber security posture.

Your organization will benefit from this guidance to improve your cyber security readiness. As you implement the CRGs, you will note the value in their alignment with other models. The CRGs are linked clearly with existing frameworks, for example, CISA's CPGs and the NIST CSF 2.0, which allows your organization to focus its efforts on implementing the goals, rather than integrating a new model to your ongoing operations. This is especially beneficial for organizations operating across the border, in both Canada and the U.S .

Your organization will also benefit from joining other organizations as a collective. All organizations will benefit from the shared objectives of the CRGs. Once met, they will improve the overall cyber posture of all sectors in Canada. In addition to providing a common purpose, the CRGs also provide a shared language to foster discussion, collective learning, and continuous improvement. By adopting this exchange, the CRGs will contribute to building and sustaining connections that can ultimately improve the resilience of the infrastructure that is essential to Canada's national security and wellbeing.

The following section provides guidance on how to use the CRGs to support cyber security in your organization.

4 https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework
5 https://www.cisa.gov/cross-sector-cybersecurity-performance-goals

THE CRGs EXPLAINED

The cross-sector CRGs are a prioritized subset of foundational recommendations that can be used by any CI organization in Canada. These are actions that, if taken, will significantly improve cyber security in all CI sectors. Each goal is tied to intended cyber security outcomes.

The CRGs should be achievable for organizations of any size and from any sector. They are intended to establish a foundational standard for cyber security practices, a baseline that connects with other existing frameworks and guidance, both in Canada and from our international partners. The CRGs are voluntary actions aimed at augmenting your organization's cyber security posture. They should not be seen as a comprehensive cyber security framework or a one-size-fits-all approach to cyber security.

Given that the CRGs are a starting point, we encourage your organization to make risk-informed decisions based on your context. For example, your organization should determine how often you should revisit the goals identified in the CRGs. Your organization should also prioritize the goals, based on the maturity of your cyber security program, with the objective of continuously improving cyber security by implementing as many of the recommended actions as resources allow.

Key characteristics of the CRGs

- **Purpose:** The CRGs are voluntary guidelines to improve CI cyber security and not an exhaustive list of requirements or mandated actions.
- **Scope:** The CRGs are a prioritized subset of foundational cyber security recommendations for both IT and OT. The goals themselves are not sufficient on their own to fully protect against all cyber security risks.
- **Applicability:** The CRGs can be applied across all CI sectors in Canada, as they are not specifically tailored to individual sectors or systems.

Cross-sector CRGs by pillars

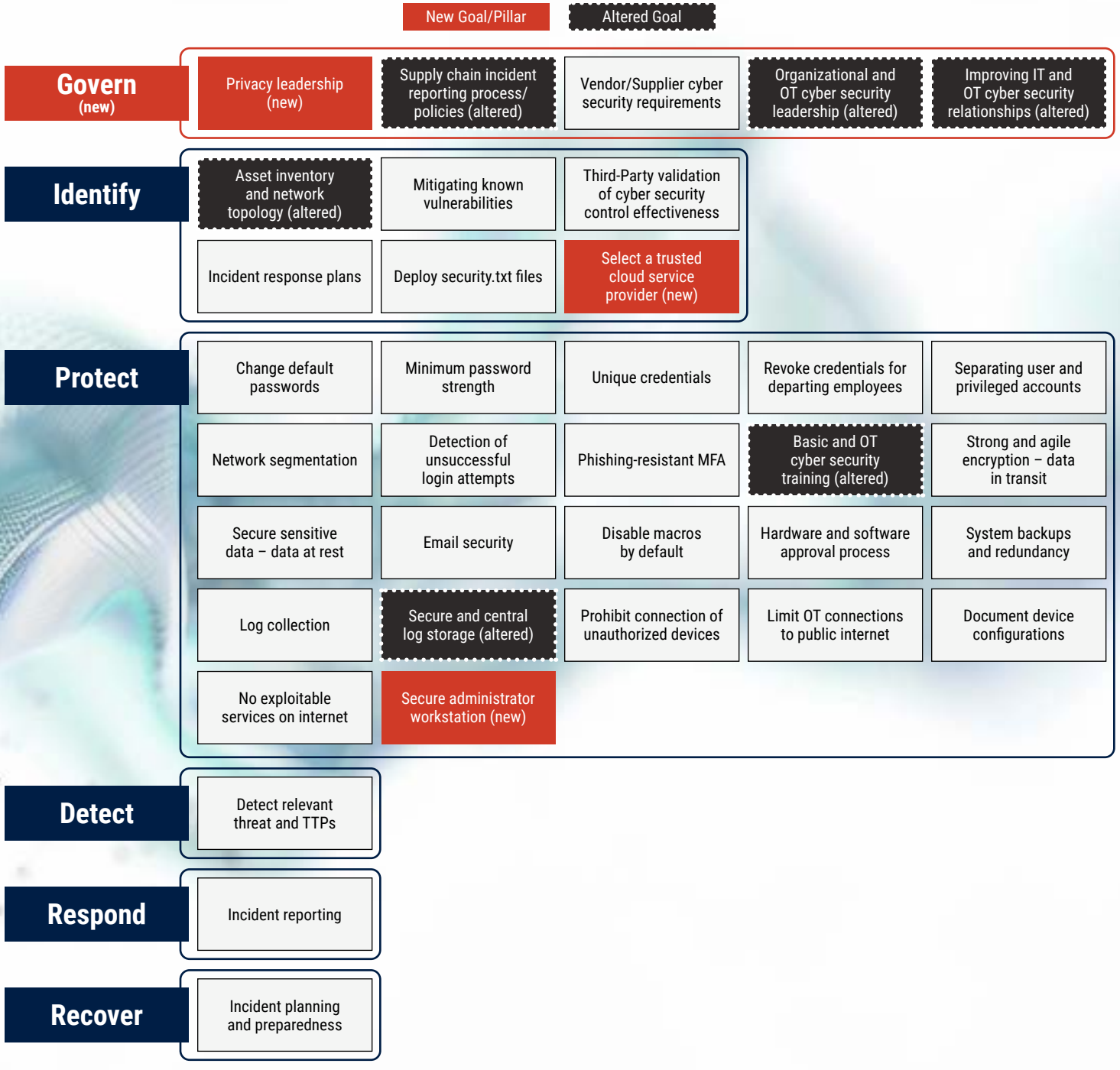
In this guidance, the CRGs are depicted in a condensed visual overlay that compares the Cyber Centre's CRGs and CISA's CPGs (see Figure 1). Where components of the model are shown as "altered" or "new" (marked in dark grey and orange, respectively), these are in comparison to the CPGs. The visual contrast is to illustrate the extent of the similarity to CISA's model, to support cross-border operators, and operators that are already familiar with the CPGs. Refer to Annex A: Differences between CRGs and CPGs for a full description of the differences between the CRGs and CPGs.

The figure shows the 36 cross-sector CRGs organized into 6 pillars. Consult the Cross-Sector Goals Toolkit[6] for the full CRGs.

The CRGs and the Cross-Sector Goals Toolkit are designed for practitioners who can implement the detailed guidance on their systems.

6 https://www.cyber.gc.ca/en/cyber-security-readiness-goals/cross-sector-cyber-security-readiness-goals-toolkit

Figure 1: Cyber Security Readiness Goals by Pillar



THE CRGs MODEL

The CRGs are aligned with existing frameworks and guidance, both in Canada and from our international partners. This section highlights what the CRGs offer for CI in Canada, in addition to the current models.

Alignment with CISA's Cross-Sector Cybersecurity Performance Goals

In many sectors, Canadian companies work closely with U.S.-based counterparts. Some may have infrastructure that spans the international boundary. Given these interdependencies, the Cyber Centre consulted with CISA during the development of the CRGs to ensure the goals could be implemented across North American CI sectors with ease.

Currently, CISA CPG Version 1.0.1 consists of 38 cyber security goals. The Cyber Centre's CRGs contain 36 cyber security goals. The CRGs have some notable differences from the CPGs. To align with the most recent version of the NIST CSF 2.0, the CRGs include a "Govern" pillar, with goals that highlight the value in establishing policies and procedures within an organization. In keeping with other updates to the CSF, the Govern pillar includes a cyber-related privacy goal, along with additional goals to highlight the importance of people, processes and technology needed to execute cyber security decisions. The CRGs include some other goals that are not in the first version of CISA's CPGs, namely, cloud and AI goals. The CRGs also provide a Canadian context to both the references and recommended actions to reflect existing Cyber Centre advice and guidance. Several of CISA's goals with similar outcomes, such as "cyber security leadership" and "OT leadership," are combined and streamlined in the Canadian CRGs .

Lastly, version 1.0 of the CRGs does not include "vulnerability disclosure." Canada does not have Safe Harbour rules, which are common in the U.S. and permit researchers to test for vulnerabilities without risk of legal liability. Nonetheless, disclosing vulnerabilities is a valuable practice. Inclusion of a vulnerability disclosure goal will be considered for future versions of the CRGs.

The Cyber Centre and CISA will continue to engage in information sharing on the baseline cyber security goals for CI. These efforts will ensure harmonization of practices across the U.S. and Canada, as well as allow us to periodically revise the CRGs and create sector-specific goals in the future.

Alignment with Government of Canada publications and tools

The CRGs provide Canadian CI owners and operators with a set of achievable cyber security goals to help them prioritize investments in cyber security and elevate their cyber security posture.

Building on work that has already been done by partners and by the Cyber Centre, the CRGs add further value by covering a wider range of actions for CI owners and operators. In addition to the CRGs, the Cyber Centre offers complementary cyber security guidance and tools to assist CI sectors. These include the:

- Baseline Cyber Security Controls for Small and Medium Organizations[7]
- Top 10 IT Security Actions to Protect Internet-Connected Networks and Information (ITSM.10.089)[8]
- IT Security Risk Management: A Lifecycle Approach (ITSG-33)[9]

All of these resources provide guidance that is aligned with the CRGs. As the CRGs consolidate many of the recommended actions from these other publications and tools, there is notable overlap between the CRGs and these other tools. More than two thirds of the baseline controls and the top 10 IT security actions are captured in the CRGs, while also providing additional, unique recommendations. Similar to the baseline controls, the CRGs are foundational guidance that can be applied in CI organizations, while the top 10 IT security actions apply to all Internet-connected networks. ITSG-33 is intended for a GC audience and supports departments in managing IT security considerations.
All actions described in these resources are voluntary, although there may be additional regulatory requirements depending on a given CI sector.

7 https://www.cyber.gc.ca/en/guidance/baseline-cyber-security-controls-small-and-medium-organizations
8 https://www.cyber.gc.ca/en/guidance/top-10-it-security-actions-protect-internet-connected-networks-and-information-itsm10089
9 https://www.cyber.gc.ca/en/guidance/it-security-risk-management-lifecycle-approach-itsg-33
IT Security Risk Management: A Lifecycle Approach (ITSG-33) is currently being updated. Changes will be reflected in future versions of the CRG, as required.

HOW TO USE THE CRGs

The Cross-Sector Goals Toolkit[10] elaborates on all 36 CRGs. As noted, each goal is matched with references, including those mentioned in the previous section, that provide more information on how to implement them.

The CRGs in the Cross-Sector Goals Toolkit are available in a clear, structured format to help your organization understand not only the goals, but also the following related aspects:

- **OUTCOME**
  The intended security outcome that each CRG strives to achieve.
- **RECOMMENDED ACTION**
  Example of action(s) an organization can take towards achieving the goal and outcome. These actions will be updated as new threats and defences are identified.
- **TTP/RISK ADDRESSED**
  A risk statement or, where available, relevant reference to MITRE ATT&CK's TTPs. By implementing the recommended action, an organization can reduce the risk of the TTP being used effectively.
- **NIST CSF 2.0 REFERENCE**
  The NIST CSF 2.0 subcategory that most closely relates to the security practice for each goal.
- **SUPPORTING GUIDANCE REFERENCE**
  Supporting Cyber Centre guidance associated with the corresponding goal and outcome, for additional information and resources.

Cyber security practitioners should consult the toolkit and implement the necessary recommended actions.

10 https://www.cyber.gc.ca/en/cyber-security-readiness-goals/cross-sector-cyber-security-readiness-goals-toolkit


002
003
004

CYBER SECURITY READINESS PROGRAM AMBITION

The CRGs are just the beginning of the Cyber Centre's efforts to support cyber security readiness among CI. These goals will serve as the foundation of our future Cyber Security Readiness program and will be essential to strengthening the cyber security posture of Canadian CI.

As part of the program, the Cyber Centre will continue to provide guidance to equip CI owners and operators with the knowledge to better protect their IT and OT from cyber incidents.

Moving forward, the Cyber Centre will update these cross-sector CRGs when necessary, to ensure they remain relevant and applicable against evolving threats and the ever-changing legislative landscape. The cross-sector CRGs will be a core resource for many CI owners and operators in Canada.

Sector-specific goals

The Cyber Centre will expand from the cross-sector CRGs to sector-specific goals. By analyzing each sector's unique cyber maturity and technologies, we will provide tailored recommendations for the sector. As shown in Figure 2, these sector-specific goals will be grounded in the cross-sector foundation. For example, the sector-specific goals for the energy sector will provide a customized view of the baseline goals that recognizes the capabilities of operators in the energy industry and the unique threat landscape they face. Based on consideration of several factors, the Cyber Centre is focused on developing sector-specific goals for the following sectors: energy, finance, telecommunications, and transportation.

Cyber Security Readiness Framework

As a collection, the cross-sector and sector-specific goals will come together as integral parts of the CRF for strengthening cyber security in CI in Canada. The CRF will incorporate all the goals in a comprehensive and cohesive collection of guidance for supporting cyber security requirements. Figure 2 depicts the CRF as an outer shell; this overarching document will package the cross-sector and sector-specific goals with appropriate implementation guidance for system owners and operators.

Figure 2: Cyber Security Readiness Framework for Canadian critical infrastructure

NEXT STEPS

The CRGs are an essential step forward in the Cyber Centre's work to enhance cyber security among CI. In close collaboration with industry, the Cyber Centre will continue to develop sector-specific goals for select CI sectors to provide additional tailored guidance focused on the unique needs of each sector. The goals will be adapted as threats to Canada's CI continue to evolve, ensuring the goals remain applicable and relevant. Feedback from all partners will contribute to improving the CRGs.

The CRGs and sector-specific goals, framed by the CRF, will help CI organizations to continue improving their cyber security posture. The Cyber Centre will continue to work on guidance to support the implementation of the CRGs in CI. Readiness is a collective effort and a shared priority. The CRGs are a starting point to set Canadian CI on a path to a more resilient cyber security posture.

Supporting content

List of abbreviations

AI	Artificial intelligence
CI	Critical infrastructure
CISA	Cybersecurity Infrastructure Security Agency
CPGs	Cross-Sector Cybersecurity Performance Goals
CRF	Cyber Security Readiness Framework
CRGs	Cyber Security Readiness Goals
CSF	Cybersecurity Framework
GC	Government of Canada
ICS	Industrial control systems
IT	Information technology
MFA	Multi-factor authentication
NIST	National Institute of Standards and Technology
OT	Operational technology
SAW	Secure administrator workstation
TTPs	Tactics, techniques, and procedures

Glossary

Anti-virus software
Software that defends against viruses, trojans, worms, and spyware. Anti-virus software uses a scanner to identify programs that may be malicious. Scanners can detect known viruses, previously unknown viruses, and suspicious files.

Artificial intelligence
A subfield of computer science that develops intelligent computer programs to behave in a way that would be considered intelligent if observed in a human (e.g., solve problems, learn from experience, understand language, interpret visual scenes).

Compromise
The intentional or unintentional disclosure of information, which adversely impacts its confidentiality, integrity, or availability.

Critical infrastructure
Processes, systems, facilities, technologies, networks, assets, and services essential to the health, safety, security, or economic well-being of Canadians and the effective functioning of government. Critical infrastructure (CI) can be stand-alone or interconnected and interdependent within and across provinces, territories, and national borders. Disruptions of critical infrastructure could result in catastrophic loss of life, adverse economic effects, and significant harm to public confidence.

Cyber attack
The use of electronic means to interrupt, manipulate, destroy, or gain unauthorized access to a computer system, network, or device.

Cyber incident
Any unauthorized attempt, whether successful or not, to gain access to, modify, destroy, delete, or render unavailable any computer network or system resource.

Cyber security
The protection of digital information, as well as the integrity of the infrastructure housing and transmitting digital information. More specifically, cyber security includes the body of technologies, processes, practices and response and mitigation measures designed to protect networks, computers, programs and data from attack, damage or unauthorized access, so as to ensure confidentiality, integrity, and availability.

Cyber threat
A threat actor, using the Internet, who takes advantage of a known vulnerability in a product for the purposes of exploiting a network and the information the network carries.

Detection
The monitoring and analyzing of system events in order to identify unauthorized attempts to access system resources.

Encryption
Converting information from one form to another to hide its content and prevent unauthorized access.

Firewall
A security barrier placed between two networks that controls the amount and kinds of traffic that may pass between the two. This protects local system resources from being accessed from the outside.

Intrusion detection
A security service that monitors and analyzes network or system events to warn of unauthorized access attempts. The findings are provided in real-time or near real-time.

Multi-factor authentication
A tactic that can add an additional layer of security to your devices and account. Multi-factor authentication (MFA) requires additional verification (like a PIN or fingerprint) to access your devices or accounts. Two-factor authentication is a type of MFA.

Malware
Malicious software designed to infiltrate or damage a computer system, without the owner's consent. Common forms of malware include computer viruses, worms, trojans, spyware, and adware.

Ransomware
A type of malware that denies a user's access to a system or data until a sum of money is paid.

Vulnerability
A flaw or weakness in the design or implementation of an information system or its environment that could be exploited to adversely affect an organization's assets or operations.

References

1 Canadian Centre for Cyber Security. Baseline cyber threat assessment: Cybercrime. (https://www.cyber.gc.ca/en/guidance/baseline-cyber-threat-assessment-cybercrime) August 28, 2023.

2 Global Affairs Canada. Statement on Russia's malicious cyber activity affecting Europe and Ukraine. (https://www.canada.ca/en/global-affairs/news/2022/05/statement-on-russias-malicious-cyber-activity-affecting-europe-and-ukraine.html) May 10, 2022.

3 Communications Security Establishment. "Since Russia's brazen and unjustifiable invasion of Ukraine, CSE continues to observe numerous Russia-backed #disinformation campaigns online". (https://x.com/cse_cst/status/1514246874890395654?s=20) X (Twitter). April 13, 2022.

4 Cybersecurity and Infrastructure Security Agency. People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection. (https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a) May 24, 2023.

5 Cybersecurity and Infrastructure Security Agency. PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure. (https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a) February 7, 2024.

6 Lionel Sujay Vailshery. "Industrial IoT – market size worldwide 2020-2030." (https://www.statista.com/statistics/611004/global-industrial-internet-of-things-market-size/#statisticContainer) Statista. February 13, 2024.

7 Dee-ann Durbin. "Meat company JBS Foods confirms it paid U.S.$11M ransom in cyberattack". (https://globalnews.ca/news/7936930/jbs-foods-ransomware-attack-paid) Global News. June 9, 2021.

8 Christina Wilkie. "Colonial Pipeline paid $5 million ransomware one day after cyberattack, CEO tells Senate". (https://www.cnbc.com/2021/06/08/colonial-pipeline-ceo-testifies-on-first-hours-of-ransomware-attack.html) CNBC. June 9, 2021.

9 Government of Newfoundland and Labrador. Cyberattack on the Newfoundland and Labrador Heath Care System. (https://www.gov.nl.ca/hcs/files/OVERVIEW-NL-Health-Cyber-Incident-March-2023.pdf) March 2023.

10 Rob Antle. "N.L. says Hive ransomware group was behind 2021 cyberattack on health systems". (https://www.cbc.ca/news/canada/newfoundland-labrador/nl-cyberattack-hive-ransomware-group-1.6778579) CBC News. March 14, 2023.

11 The Hospital for Sick Children (SickKids). "SickKids lifts Code Grey with 80 per cent of priority systems restored". (https://www.sickkids.ca/en/news/archive/2023/sickkids-lifts-code-grey-with-80-per-cent-of-priority-systems-restored) January 5, 2023.

12 Jonathan Greig. "Canadian banking tech giant Moneris says it prevented ransomware attack". (https://therecord.media/moneris-canada-ransomware-attack-prevented) The Record from Recorded Future News. November 13, 2023.

13 Public Safety Canada. Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada. (https://publications.gc.ca/collections/collection_2010/sp-ps/PS4-102-2010-eng.pdf) 2010.

14 Public Safety Canada. National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age. (https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf) 2018.

Annex A: Differences between CRGs and CPGs

New pillar and goals

- **Govern pillar**
  - **Type**: Pillar
  - **Rationale**: A new Govern pillar was added to the 5 existing pillars to reflect the new NIST CSF 2.0 guidance. The Govern pillar enables organizations to emphasize the importance of cyber security governance. This new pillar guides organizations to focus on the processes, people, and technology required to execute cyber security practices successfully.
- **Privacy leadership**
  - **Type**: Goal **Pillar**: Govern
  - **Rationale**: Under the new Govern pillar, the CRGs added a Privacy leadership goal for organizations to achieve. Data breaches of personal information are increasingly common among CI sectors that experience a cyber incident. Implementing the proper teams and procedures can help prevent and mitigate these breaches. Additionally, cyber-related privacy controls have been added to NIST CSF 2.0.
- **Select a trusted cloud service provider (CSP)**
  - **Type**: Goal **Pillar**: Identify
  - **Rationale**: A trusted CSP that is mature and technically capable is essential for organizations to confidently adopt cloud services technologies.
- **Secure administrator workstation (SAW)**
  - **Type**: Goal **Pillar**: Protect
  - **Rationale**: A SAW is a hardened workstation dedicated to sensitive tasks performed by administrators. It separates sensitive tasks and accounts from non-administrative use to protect the organization's network from cyber security risks like malware, phishing, and pass-the-hash attacks.

Altered goals

- **Organizational and OT cyber security leadership**
  - **Type**: Goal **Pillar**: Govern
  - **Rationale**: Combines leadership for cyber security and OT role/title.
- **Supply chain incident reporting process/policies**
  - **Type**: Goal **Pillar**: Govern
  - **Rationale**: Adds processes and policy to the existing supply chain incident reporting goal. Focuses the organization's supply chain risk management program to require that vendors and suppliers notify the procuring customer of incidents.
- **Asset inventory and network topology**
  - **Type**: Goal **Pillar**: Identify
  - **Rationale**: Asset inventory now includes a cloud component to ensure, if applicable, an organization documents all assets that pertain to the cloud ecosystem.
- **Basic and OT cyber security training**
  - **Type**: Goal **Pillar**: Protect
  - **Rationale**: Combines cyber security and OT training into one goal and includes privacy concepts and privacy breaches in training to increase awareness of privacy-related incidents.
- **Secure and central log storage**
  - **Type**: Goal **Pillar**: Protect
  - **Rationale**: Organizations should keep log storage in a secure and central storage space.

Removed goals

- **Vulnerability disclosure**
  - **Type**: Goal **Pillar**: Respond
  - **Rationale**: Canada does not have Safe Harbour rules, which are common in the U.S. and permit researchers to test for vulnerabilities without risk of legal liability. Inclusion of a vulnerability disclosure goal will be considered for future versions of the CRGs.

Notes