

Cybersecurity in the Government of Quebec

An evolving government

Presentation to the PSCIOC
October 27, 2021

Agenda

CYBERDÉFENSE



- Introduction of the **Government Cybersecurity Policy**
- Introduction of **Bill No. 95 (2021)**
- Introduction of the **Government Cyber Defence Network**
- **Government Cyber Defence Centre's** achievements

Context



“The laws and regulations will need to continue to evolve in order to harness the full potential of digital technology and to meet the government’s transformation targets.”

– Government Digital Transformation Strategy 2019–2023



“Its implementation requires strong and integrated governance based on a legal, administrative, and prescriptive framework adapted to the digital age.”

– Government Cybersecurity Policy

CYBERDÉFENSE



Government Cybersecurity Policy

Adopted in March 2020

- Building on the Government Digital Transformation Strategy
- Developed using a cybersecurity **expert panel**
- Targets public administration, citizens and cybersecurity ecosystem partners
- Translates into **key actions** with action plans tailored to cybersecurity issues and opportunities

Read about the policy and key actions

[Government Cybersecurity policy](#) | [Government of Quebec \(quebec.ca\)](#)

[Key actions](#) | [Government of Quebec \(quebec.ca\)](#)





Government Cybersecurity Policy

Targets spread across four axes

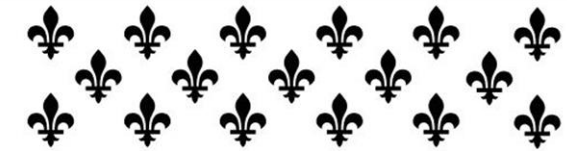
1. Cybersecurity, a government priority
2. Secure public services
3. Confident and knowledgeable citizens
4. Strategic and sustainable partnerships

CYBERDÉFENSE



Bill No. 95

- Bill 95, An Act to amend the Act respecting the governance and management of the information resources of public bodies and government enterprises and other legislative provisions - Assemblée nationale du Québec (assnat.qc.ca)



ASSEMBLÉE NATIONALE DU QUÉBEC

PREMIÈRE SESSION

QUARANTE-DEUXIÈME LÉGISLATURE

Projet de loi n° 95
(2021, chapitre 22)

**Loi modifiant la Loi sur
la gouvernance et la gestion des
ressources informationnelles des
organismes publics et des entreprises
du gouvernement et d'autres
dispositions législatives**

Présenté le 5 mai 2021
Principe adopté le 1^{er} juin 2021
Adopté le 9 juin 2021
Sanctionné le 10 juin 2021

Éditeur officiel du Québec
2021

Purpose

Establish an information resources governance and management framework for public bodies and government enterprises with a particular focus on:

Providing citizens and businesses with **streamlined, integrated, and quality services**

Properly protecting
public body IRs

Establishing optimal governance and management of **government digital data**

Coordinating public body **digital transformation initiatives**

Read Bill No. 95 (2021):

[Bill No. 95](#)

Key changes

CYBERDÉFENSE

The main changes discussed relate to the following chapters:



Chief Information Officer
and Information Officer

AGMIR, chapter II



Information Security

AGMIR, chapter II.4



Government Digital Data

AGMIR, chapter II.2



Digital transformation

AGMIR, chapter II.3



Planning and management
for public bodies

AGMIR, chapter III



Other provisions

AELFIT, chapter V



Chief Information Officer

New functions

CYBERDÉFENSE

9



**Chief Information Officer
(CIO)***

New functions

AGMIR, section 7.1

**Head of Government
Information Security**

**Government Digital
Data Manager**

**Head of Government
Digital Transformation**

*They may delegate the exercise of any of their responsibilities—in writing—to a person under their management.



Chief Information Officer

New functions

CYBERDÉFENSE

10

Overall vision

Develop and submit a comprehensive IR vision, including the **digital transformation of Public Administration**, and propose ways to implement it

Application guidance

Any written instructions, relating to

- Carrying out activities,
- Fulfilling responsibilities
- Applying IR measures

Public agencies must comply with them

Developing IR expertise

To provide public bodies with services, advice, or support and to strengthen the Crown's expertise, including by:

Information security

Digital transformation

Information technologies

AGMIR, chapter 7



Information Officer

New functions and terms and conditions
for appointing the IO





Information security

Summary of key changes

CYBERDÉFENSE

12

Purpose

Establish a **comprehensive and coordinated** information security governance and **monitor** the implementation of requirements in public bodies

AGMIR, chapter II.2

- Create the functions of the **Government Chief Information Security Officer** and the **Deputy Chief Information Security Officer**.
- Allow for the timely sharing of certain pieces of information when compromising the confidentiality, availability, or integrity of an IR or information.
- Help the CIO, the Government Chief Information Security Officer and IOs formulate security information **application guidance**.
- Maintain a specialized information security administrative unit within TBS.



Information Security

CYBERDÉFENSE

13

AGMIR, section 12.6



Government Chief Information Security Officer

(function assigned to the CIO that may be delegated)

Responsibilities

- Leading government action in terms of information security;
- Recommend to the Conseil du Trésor rules for information security, including those related to authentication and identification and recommend performance targets for public bodies in terms of information security to the Chair of the Conseil du Trésor;
- Establish the security classification model for government digital data based on its nature, characteristics, use, and rules that administer them, and have it approved by the Conseil du Trésor;
- Notify public bodies of information security expectations and formulate application guidance for them;
- Monitor public bodies' implementation of information security obligations arising from the application of this Act, ensure they are enforced and assess action taken by public bodies in this regard;
- Report to the Chair of the Conseil du Trésor, on terms and conditions as determined by the Chair, on performance target results and on compliance with obligations and make any necessary recommendations to the Chair;
- Performs any other duties assigned by the Chair of the Conseil du Trésor or the Government.



Information Security

CYBERDÉFENSE

14

AGMIR, section 12.7



Deputy Chief Information Security Officer

(function assigned to IOs under the functional authority of the Government Chief Information Security Officer)

Responsibilities

- Support the Government Chief Information Security Officer in supporting government action on information security;
- Apply, under the direction of the Government Chief Information Security Officer, standards, directives, rules or application guidance related to information security developed under this Act;
- Ensure the protection of information resources and information, including through risk and vulnerability management and by implementing measures to protect them from any form of breach, such as threats or cyberattacks;
- Take any action required in the event of a breach of the protection of information resources and information;
- Formulate specific information security application guidance for these bodies;
- Monitor public bodies' implementation of information security obligations arising from the application of this Act, ensure they are enforced and assess action taken by public bodies in this regard;
- Report to the Government Chief Information Security Officer on his management and provide him with any requested information, according to the terms and conditions determined by the Chair of the Conseil du Trésor.



Information Security

Implementing
regulations
forthcoming

Quick sharing of certain pieces of information*

AGMIR, sections 12.2, 12.3, and 12.4

- Actions to be taken by a public body when it finds that an IR or information under its responsibility is or has been the subject of a breach of its confidentiality, availability, or integrity
- Measures that the body can take to prevent or reduce these risks of breaches;

Information security application guidance

Forthcoming

AGMIR, sections 12.6 and 12.7

Application guidance issued by the Government Chief or specific application guidance by the Deputy Chief to the associated public bodies

Administrative unit specializing in information security

AGMIR, section 12.5

- Duty to maintain within the secretariat of the Conseil du Trésor
- Under the direction of the Government Chief Information Security Officer
- Currently the Government Cyber Defence Centre

*Provisions that will come into force on the date of the first regulation made under new section 22.1.1. scheduled for fall 2021

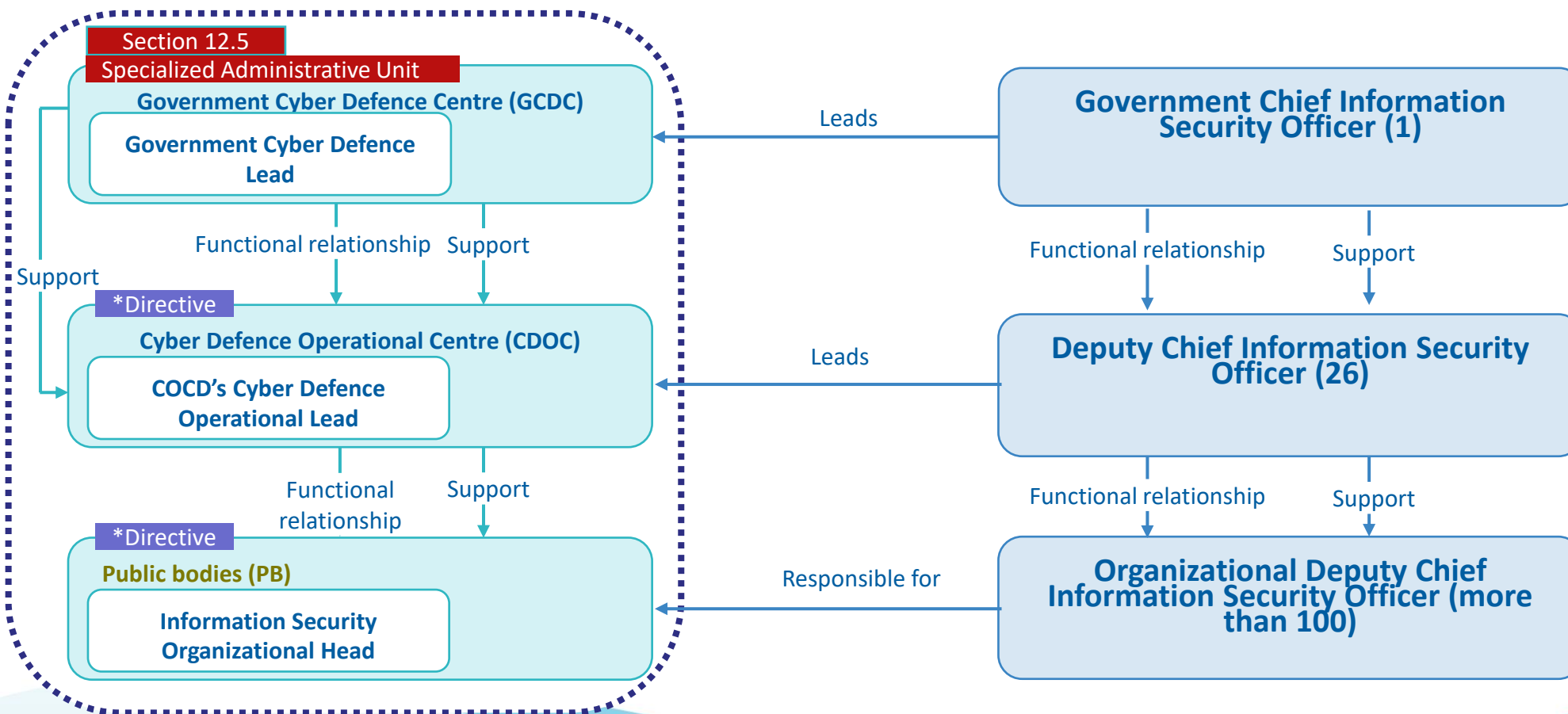


Government Cyber Defence Network

Structure

CYBERDÉFENSE

16



*The Government Directive on Information Security is not yet adopted by the Council of Ministers; provisions subject to change



Government Cyber Defence Network (cont'd)

Proactivity, collaboration, sharing, exchanges, and education

CYBERDÉFENSE

17

Mission

Strengthen cyberthreat **prevention** and **response**

*Government Directive on Information Security

*The Government Directive on Information Security is not yet adopted by the Council of Ministers; provisions subject to change

- Ensure common support for cybersecurity incidents
- Ensure ongoing cyberthreat monitoring
- Enable government authorities to respond quickly and in a coordinated manner to cyberthreats
- Ensure best practices for cyber defence in public administration
- Be the point of contact for public bodies for obtaining cybersecurity advice
- Contribute to enhancing cybersecurity skills among public bodies



Government Cyber Defence Centre

A leader in cyber defence

CYBERDÉFENSE

18

Mission

Protecting the Government of Quebec's information resources from **cyber attacks**

- Provide centralized security services
- Build the capacity of the Government Cyber Defence Network
- Develop and disseminate specialized cyber defence technologies and tools that strengthen cybersecurity
- Act as a coordination centre when managing security incidents
- Advise authorities on positions to take in terms of cyber risk management



Government Cyber Defence Centre (continued)

Multiple Accomplishments

CYBERDÉFENSE

19

GCDC's structure

Direction de la prévention et de la gestion
des incidents

Direction des pratiques et du
développement des compétences en
cyberdéfense

Direction du développement du Réseau
gouvernemental de cyberdéfense

- Deploying a minimum of 15 security measures at the government level
- Conducting a government-wide phishing campaign
- Conducting over 75 intrusion tests on government digital services
- Government Asset Scanning Service and ongoing dark web monitoring
- Implementing a training offer for information security stakeholders