cira

Information Security Webinar

Part 1

Webinaire sur la sécurité de l’information

Partie 1

Introduction to principles

Introduction aux principes

Overview

- CIA Triad
- Data security
- Evolution of security operations
- Internal and external threats
- Key security controls

Vue d’ensemble

- Triade CID
- Sécurité des données
- Évolution des opérations de sécurité
- Menaces internes et externes
- Principaux contrôles de sécurité

Introduction to principles

Introduction aux principes

Confidentiality, Integrity, Availability

Availability
Integrity
Security Model
Confidentiality

Confidentialité, Intégrité, Disponibilité

Confidentialité
Triade CID
Intégrité
Disponibilité

Introduction to principles
Introduction aux principes

Data security

- Data in transit
- Data at rest
- Data in use

Sécurité des données

- Données en transit
- Données au repos
- Données utilisées

Introduction to principles

Introduction aux principes

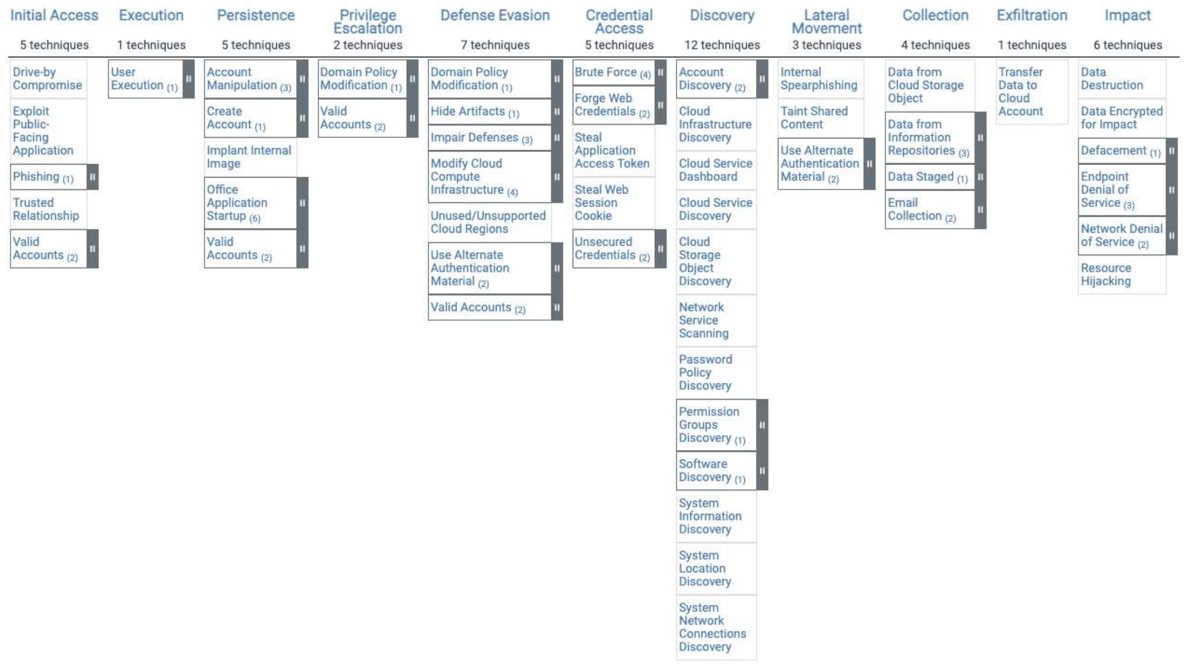
Evolution of security operations

Évolution des opérations de sécurité

Introduction to principles
Introduction aux principes

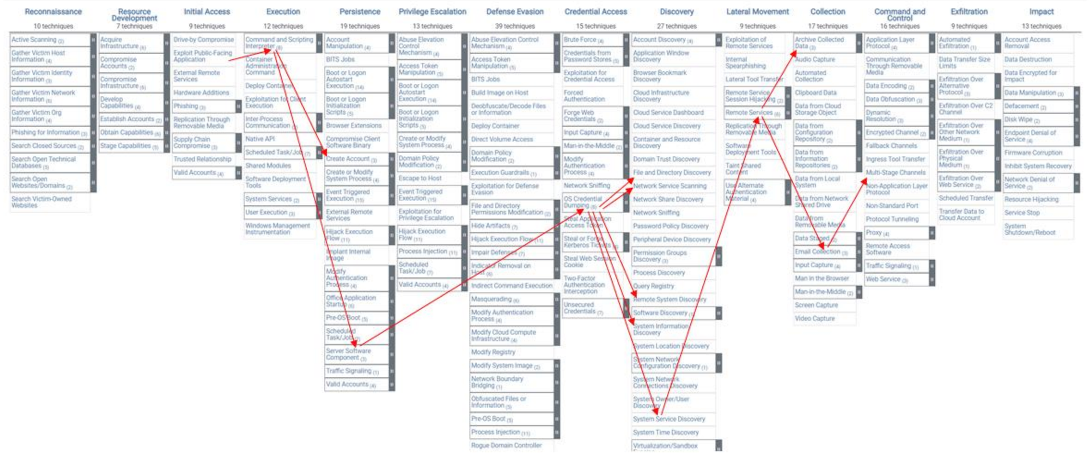
Tactics, Techniques, Procedures

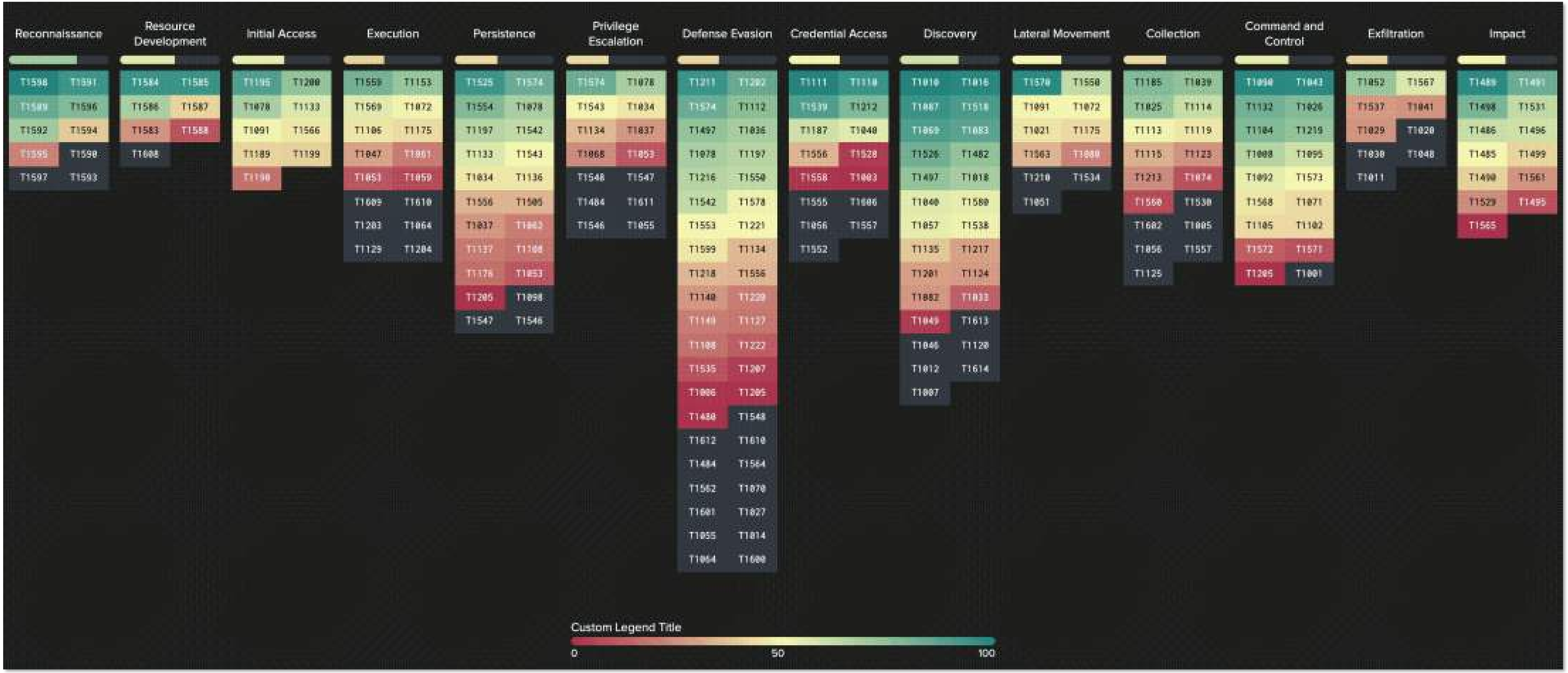
Tactiques, Techniques, Procédures



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Impact
5 techniques	1 techniques	5 techniques	2 techniques	7 techniques	5 techniques	12 techniques	3 techniques	4 techniques	1 techniques	6 techniques
Drive-by Compromise	User Execution (1)	Account Manipulation (3)	Domain Policy Modification (1)	Domain Policy Modification (1)	Brute Force (4)	Account Discovery (2)	Internal Spearphishing	Data from Cloud Storage Object	Transfer Data to Cloud Account	Data Destruction
Exploit Public-Facing Application		Create Account (1)	Valid Accounts (2)	Hide Artifacts (1)	Forge Web Credentials (2)	Cloud Infrastructure Discovery	Taint Shared Content	Data from Information Repositories (3)		Data Encrypted for Impact
Phishing (1)		Implant Internal Image		Impair Defenses (3)	Steal Application Access Token	Cloud Service Dashboard	Use Alternate Authentication Material (2)	Data Staged (1)		Defacement (1)
Trusted Relationship		Office Application Startup (6)		Modify Cloud Compute Infrastructure (4)	Steal Web Session Cookie	Cloud Service Discovery		Email Collection (2)		Endpoint Denial of Service (3)
Valid Accounts (2)		Valid Accounts (2)		Unused/Unsupported Cloud Regions	Unsecured Credentials (2)	Cloud Storage Object Discovery				Network Denial of Service (2)
				Use Alternate Authentication Material (2)		Network Service Scanning				Resource Hijacking
				Valid Accounts (2)		Password Policy Discovery				
						Permission Groups Discovery (1)				
						Software Discovery (1)				
						System Information Discovery				
						System Location Discovery				
						System Network Connections Discovery				

MITRE
ATT&CK®





Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
T1598 T1591	T1584 T1585	T1195 T1200	T1559 T1153	T1525 T1574	T1574 T1078	T1211 T1202	T1111 T1110	T1010 T1016	T1570 T1550	T1185 T1039	T1090 T1043	T1052 T1567	T1489 T1491
T1589 T1596	T1586 T1587	T1078 T1133	T1569 T1072	T1554 T1078	T1543 T1034	T1574 T1112	T1539 T1212	T1087 T1518	T1091 T1072	T1025 T1114	T1132 T1026	T1537 T1041	T1498 T1531
T1592 T1594	T1583 T1588	T1091 T1566	T1106 T1175	T1197 T1542	T1134 T1037	T1497 T1036	T1187 T1040	T1069 T1083	T1021 T1175	T1113 T1119	T1104 T1219	T1029 T1020	T1486 T1496
T1595 T1590	T1608	T1189 T1199	T1047 T1061	T1133 T1543	T1068 T1053	T1078 T1197	T1556 T1528	T1526 T1482	T1563 T1080	T1115 T1123	T1008 T1095	T1030 T1048	T1485 T1499
T1597 T1593		T1190	T1053 T1059	T1034 T1136	T1548 T1547	T1216 T1550	T1558 T1003	T1497 T1018	T1210 T1534	T1213 T1074	T1092 T1573	T1011	T1490 T1561
			T1609 T1610	T1556 T1505	T1484 T1611	T1542 T1578	T1555 T1606	T1040 T1580	T1051	T1560 T1530	T1568 T1071		T1529 T1495
			T1203 T1064	T1037 T1062	T1546 T1055	T1553 T1221	T1056 T1557	T1057 T1538		T1602 T1005	T1105 T1102		T1565
			T1129 T1204	T1137 T1108		T1599 T1134	T1552	T1135 T1217		T1056 T1557	T1572 T1571		
				T1176 T1053		T1218 T1556		T1201 T1124		T1125	T1205 T1001		
				T1205 T1098		T1140 T1220		T1082 T1033					
				T1547 T1546		T1149 T1127		T1049 T1613					
						T1108 T1222		T1046 T1120					
						T1535 T1207		T1012 T1614					
						T1006 T1205		T1007					
						T1480 T1548							
						T1612 T1610							
						T1484 T1564							
						T1562 T1070							
						T1601 T1027							
						T1055 T1014							
						T1064 T1600							

Introduction to principles

Introduction aux principes

Internal threats

- Malicious insiders
- Uneducated insiders
- Careless insiders

Menaces internes

- Initiés malveillants
- Initiés incultes
- Initiés négligents

CIRA.CA

Introduction to principles

Introduction aux principes

External threats

- Nation States
- Hacktivists
- Organized crime
- Individuals
- Organizational adversaries
- 3rd-Parties

Menaces externes

- États-nations
- Hacktivistes
- Crime organisé
- Particuliers
- Adversaires organisationnels
- 3èmes Parties

Introduction to principles
Introduction aux principes

Attacks

- Data Exfiltration
- Data Alteration
- Data Loss
- Extortion
- Denial of Service
- Sabotage

Attaques

- Exfiltration des données
- Modification des données
- Perte de données
- Extorsion
- Déni de service
- Sabotage

Introduction to principles

Introduction aux principes

Attacks

- Surveillance
- Privacy Breach
- Financial Theft
- Command & Control

Attaques

- La surveillance
- Atteinte à la vie privée
- Vol financier
- Commande et contrôle

Introduction to principles

Introduction aux principes

Key security controls

- People
- Process
- Technology

Principaux contrôles de sécurité

- Les gens
- Processus
- La technologie

Key security controls

Principaux contrôles de sécurité

People

- Training
- Awareness
- Exercises

Les gens

- Formation
- Sensibilisation
- Exercices

Key security controls
Principaux contrôles de sécurité

Process

- Information security management system
- Incident response plan
- Continuous improvement
- Exercises

Processus

- Système de gestion de la sécurité de l’information
- Plan d’intervention en cas d’incident
- Amélioration continue
- Exercices

Key security controls
Principaux contrôles de sécurité

Technology

- Endpoint, Network, Cloud
- Software
- AI
- Quantum
- Exercises

La technologie

- Point de terminaison, réseau, cloud
- Logiciels
- L’IA
- Quantum
- Exercices

Settlement & Integration
Établissement et intégration

Settlement & Integration
Établissement et intégration

Types of sensitive data

- Usernames and passwords
- Communications
- Social media content
- Financial records
- Health records

Types de données sensibles

- Noms d’utilisateur et mots de passe
- Les communications
- Contenu des médias sociaux
- Documents financiers
- Dossiers de santé

Settlement & Integration
Établissement et intégration

Social engineering

Ingénierie sociale

Phishing

Hameçonnage

Vishing

Hameçonnage vocal

Smishing

Hameçonnage par texto

Introduction to principles

Introduction aux principes

Deepfake

Deepfake

Settlement & Integration
Établissement et intégration

Impacts

- Loss of important documents
- Inability to communicate
- Disqualification
- Theft
- Extortion

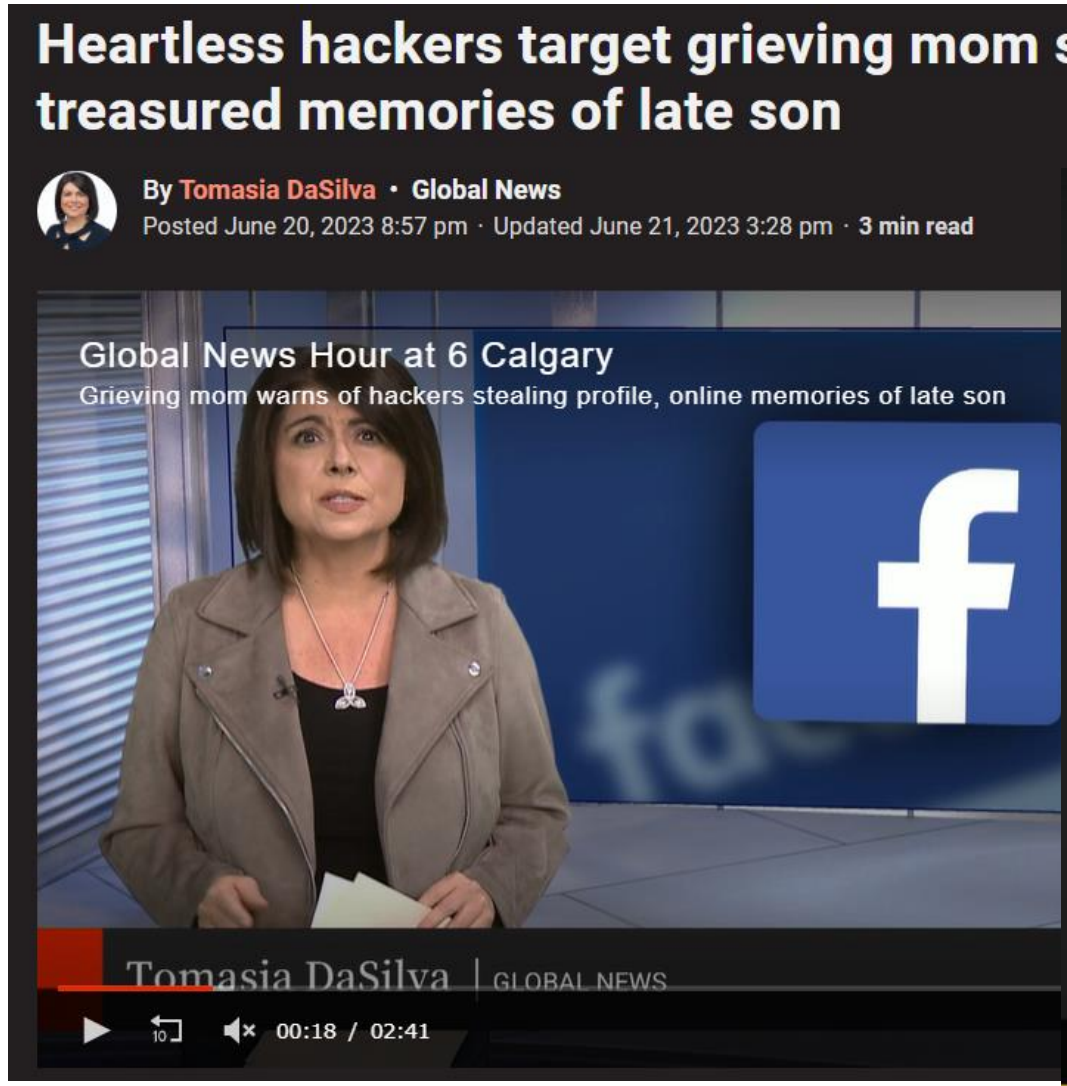
Répercussions

- Perte de documents importants
- Incapacité de communiquer
- Disqualification
- Vol
- Extorsion

Settlement & Integration
Établissement et intégration

In the news

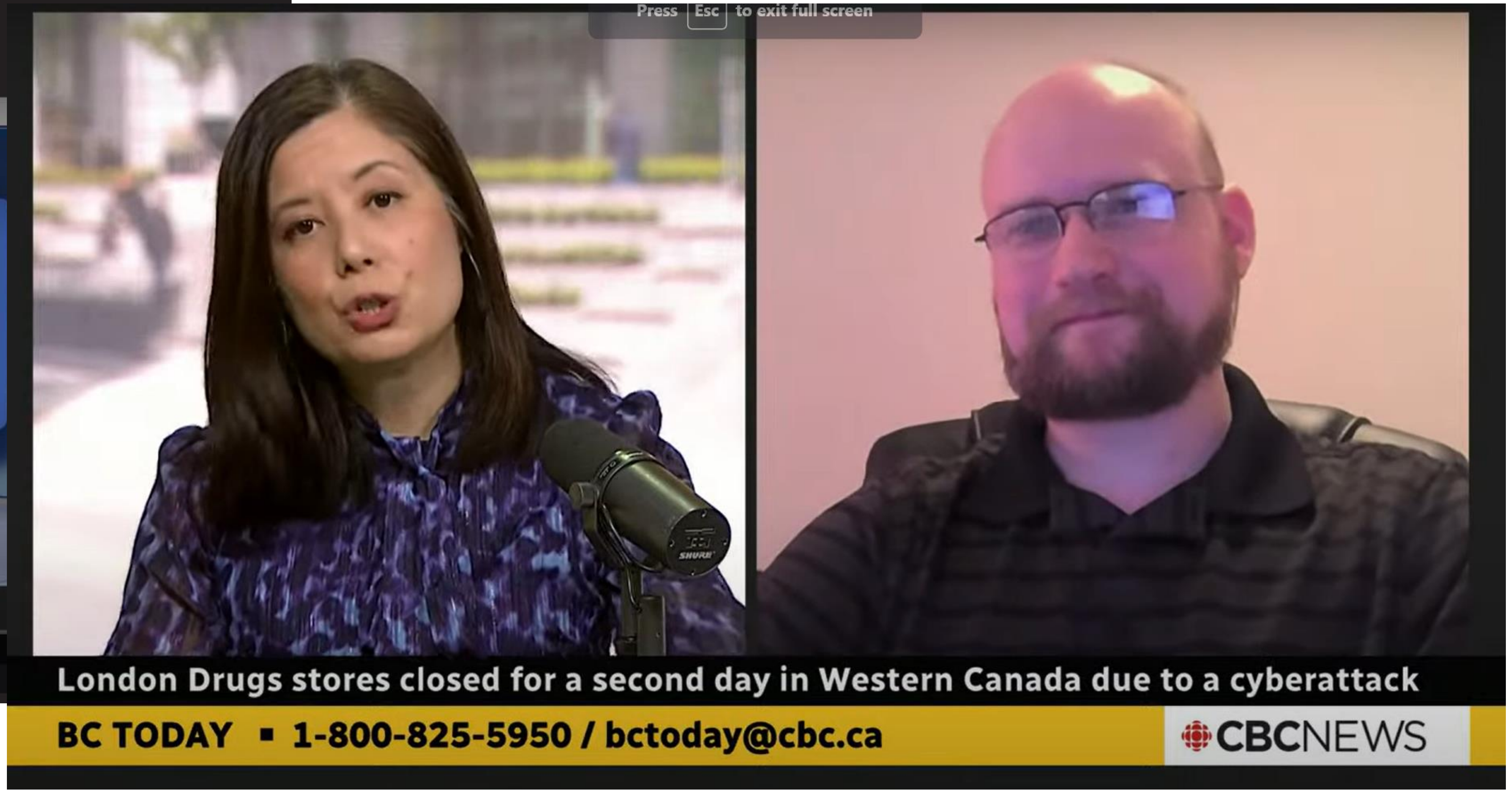
Dans l’actualité



Heartless hackers target grieving mom stealing treasured memories of late son

By Tomasia DaSilva • Global News
Posted June 20, 2023 8:57 pm · Updated June 21, 2023 3:28 pm · 3 min read

Global News Hour at 6 Calgary
Grieving mom warns of hackers stealing profile, online memories of late son



London Drugs stores closed for a second day in Western Canada due to a cyberattack

BC TODAY ▪ 1-800-825-5950 / bctoday@cbc.ca

cira

Information Security Webinar

Part 2

Webinaire sur la sécurité de l’information

Partie 2

Part 2

Partie 2

Topics

- Digital security and privacy: laws, regulations, and frameworks.
- Security program management: policies, incident management, and oversight.

Thèmes

- Sécurité et confidentialité numériques : lois, règlements, et cadre.
- Gestion du programme de sécurité : politiques, gestion des incidents, et surveillance.

cira

Frameworks, Regulations, and Laws

Cadres, Règlements et Lois

Frameworks, Regulations, and Laws

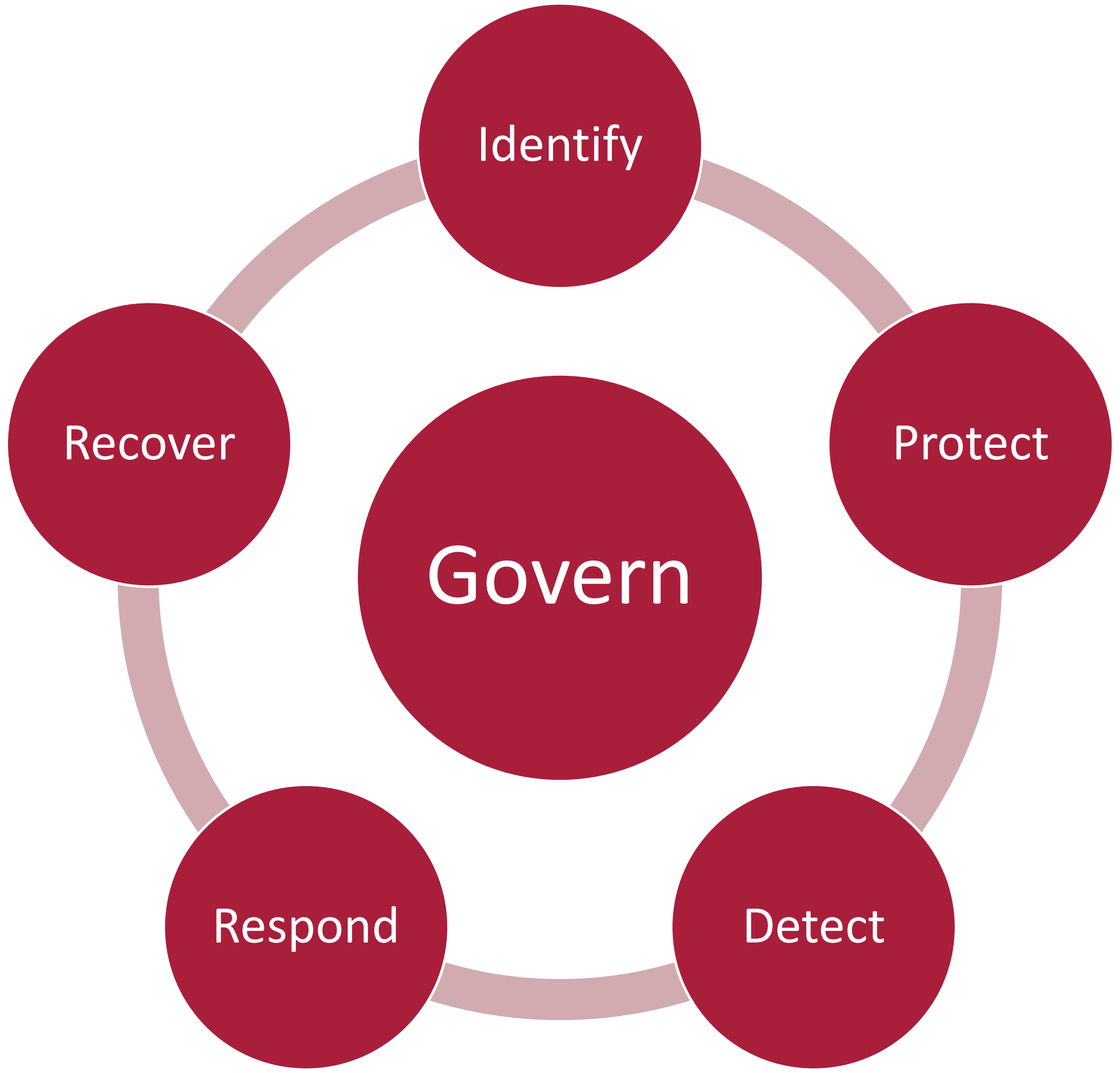
Cadres, Règlements et Lois

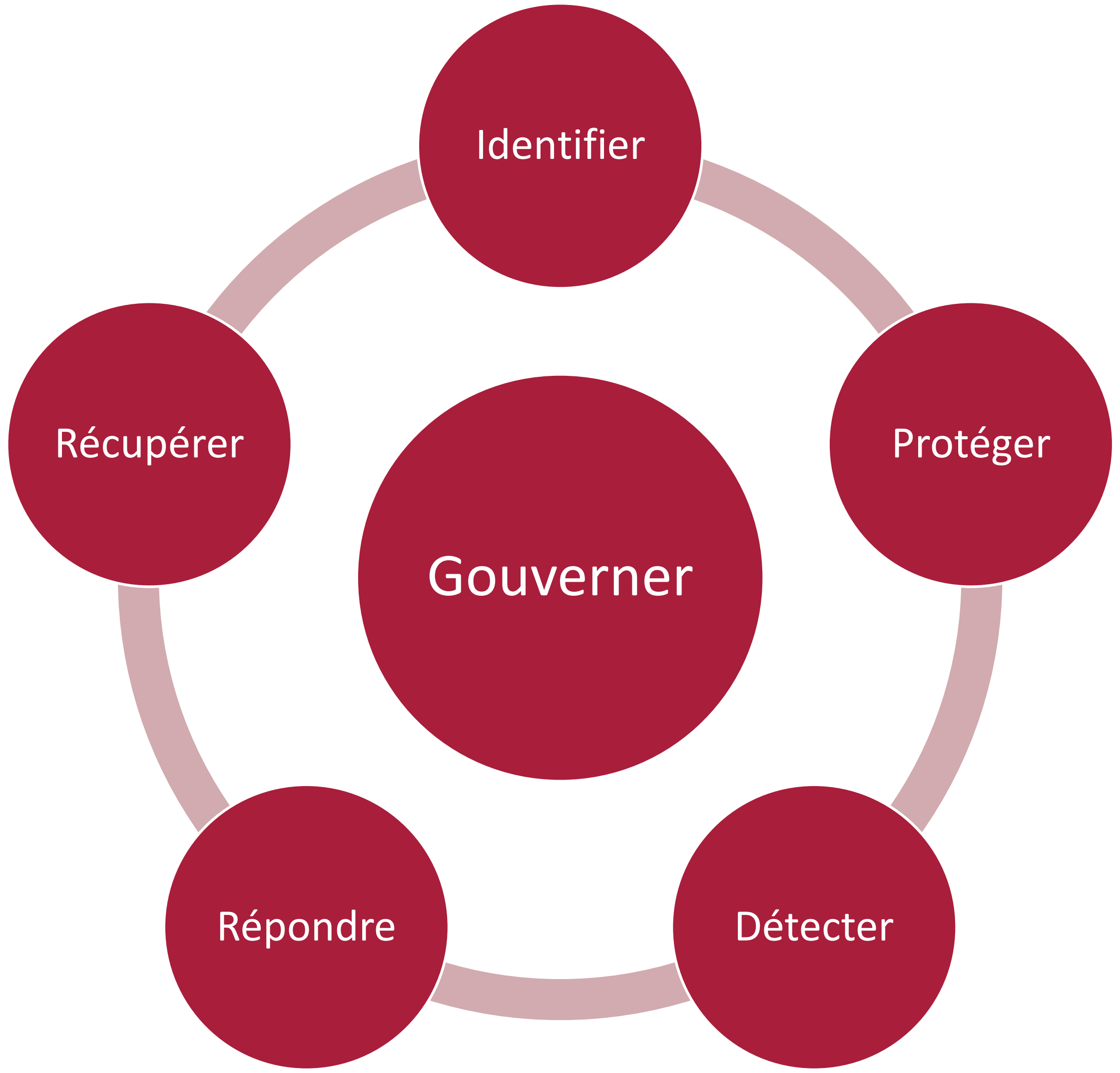
Overview

Vue d’ensemble

NIST CSF 2.0

NIST Cadre de cybersécurité 2.0

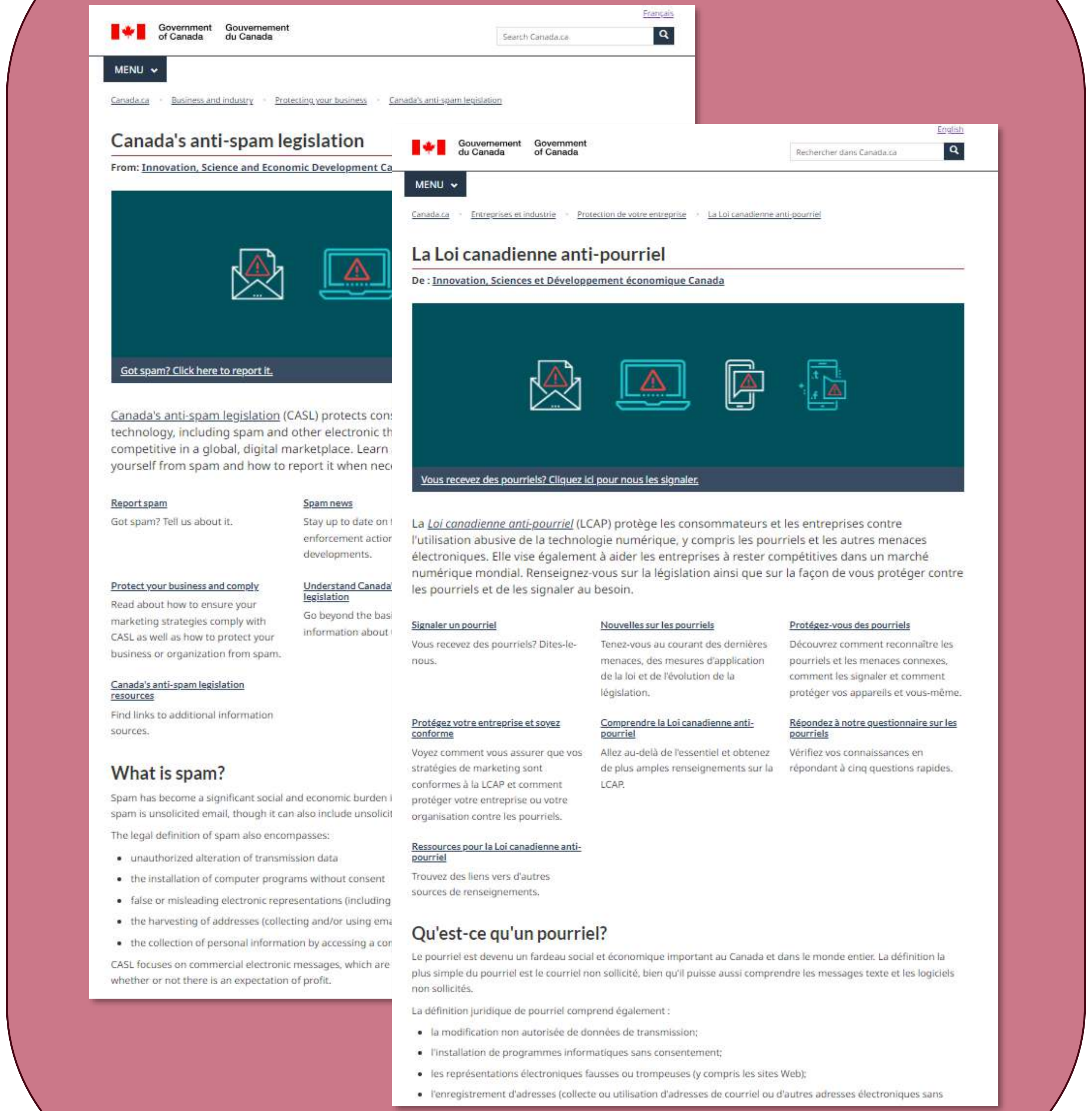




CASL
LCAP

Canada’s anti-spam legislation

La Loi canadienne anti-pourriel



Français

Government of Canada Gouvernement du Canada

Search Canada.ca

MENU

Canada.ca · Business and industry · Protecting your business · Canada's anti-spam legislation

Canada's anti-spam legislation

From: Innovation, Science and Economic Development Ca

Got spam? Click here to report it.

Canada's anti-spam legislation (CASL) protects con
technology, including spam and other electronic th
competitive in a global, digital marketplace. Learn
yourself from spam and how to report it when nec

Report spam
Got spam? Tell us about it.

Spam news
Stay up to date on
enforcement actior
developments.

Protect your business and comply
Read about how to ensure your marketing strategies comply with CASL as well as how to protect your business or organization from spam.

Understand Canada' legislation
Go beyond the basi
information about

Canada's anti-spam legislation resources
Find links to additional information sources.

What is spam?

Spam has become a significant social and economic burden i
spam is unsolicited email, though it can also include unsolicit

The legal definition of spam also encompasses:

- unauthorized alteration of transmission data
- the installation of computer programs without consent
- false or misleading electronic representations (including
- the harvesting of addresses (collecting and/or using ema
- the collection of personal information by accessing a cor

CASL focuses on commercial electronic messages, which are
whether or not there is an expectation of profit.

English

Gouvernement du Canada Government of Canada

Rechercher dans Canada.ca

MENU

Canada.ca · Entreprises et industrie · Protection de votre entreprise · La Loi canadienne anti-pourriel

La Loi canadienne anti-pourriel

De : Innovation, Sciences et Développement économique Canada

Vous recevez des pourriels? Cliquez ici pour nous les signaler.

La *Loi canadienne anti-pourriel* (LCAP) protège les consommateurs et les entreprises contre l'utilisation abusive de la technologie numérique, y compris les pourriels et les autres menaces électroniques. Elle vise également à aider les entreprises à rester compétitives dans un marché numérique mondial. Renseignez-vous sur la législation ainsi que sur la façon de vous protéger contre les pourriels et de les signaler au besoin.

Signaler un pourriel
Vous recevez des pourriels? Dites-le-nous.

Nouvelles sur les pourriels
Tenez-vous au courant des dernières menaces, des mesures d'application de la loi et de l'évolution de la législation.

Protégez-vous des pourriels
Découvrez comment reconnaître les pourriels et les menaces connexes, comment les signaler et comment protéger vos appareils et vous-même.

Protégez votre entreprise et soyez conforme
Voyez comment vous assurer que vos stratégies de marketing sont conformes à la LCAP et comment protéger votre entreprise ou votre organisation contre les pourriels.

Comprendre la Loi canadienne anti-pourriel
Allez au-delà de l'essentiel et obtenez de plus amples renseignements sur la LCAP.

Répondez à notre questionnaire sur les pourriels
Vérifiez vos connaissances en répondant à cinq questions rapides.

Ressources pour la Loi canadienne anti-pourriel
Trouvez des liens vers d'autres sources de renseignements.

Qu'est-ce qu'un pourriel?

Le pourriel est devenu un fardeau social et économique important au Canada et dans le monde entier. La définition la plus simple du pourriel est le courriel non sollicité, bien qu'il puisse aussi comprendre les messages texte et les logiciels non sollicités.

La définition juridique de pourriel comprend également :

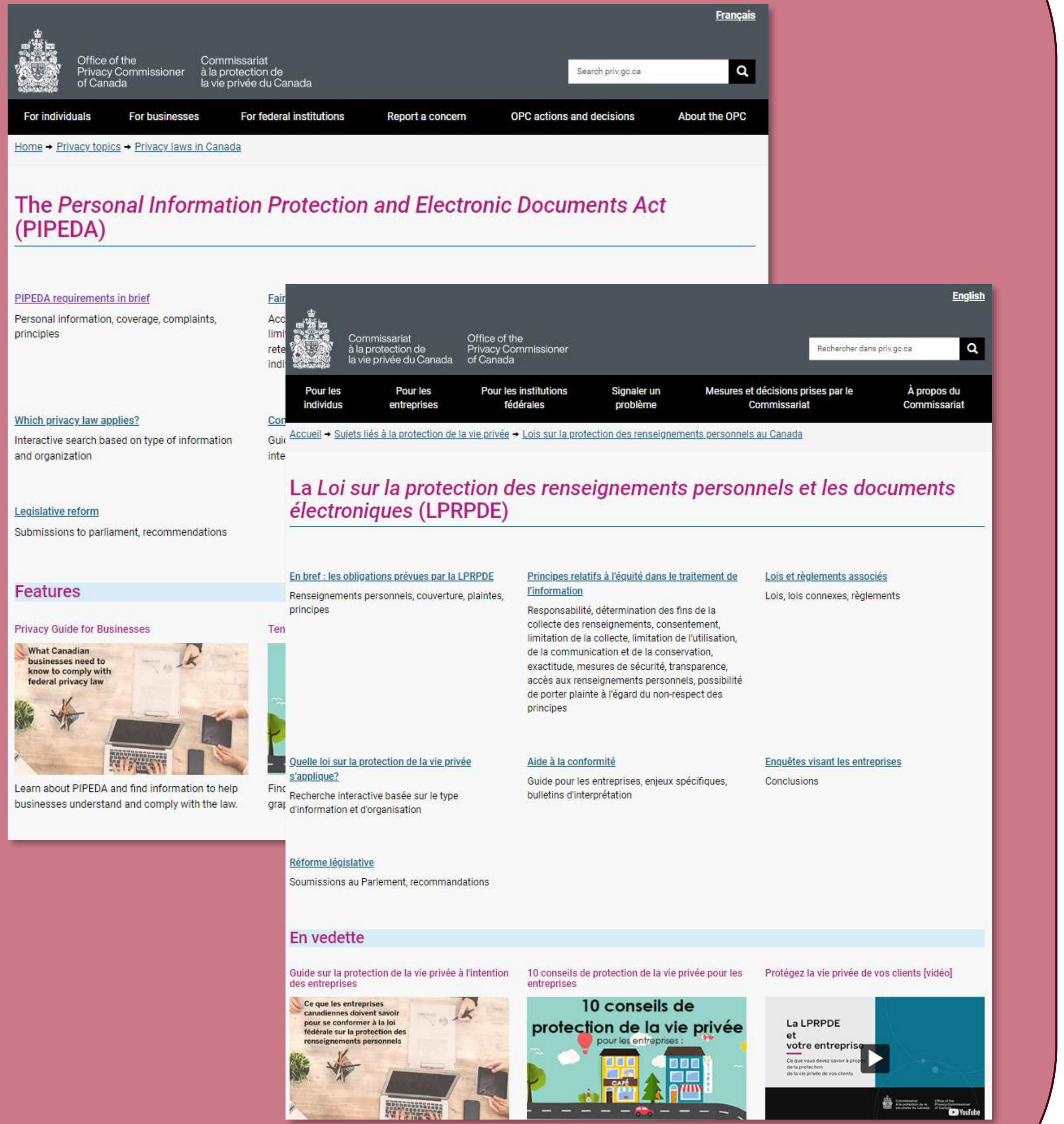
- la modification non autorisée de données de transmission;
- l'installation de programmes informatiques sans consentement;
- les représentations électroniques fausses ou trompeuses (y compris les sites Web);
- l'enregistrement d'adresses (collecte ou utilisation d'adresses de courriel ou d'autres adresses électroniques sans

PIPEDA

LPRPDE

The Personal Information Protection and Electronic Documents Act

La Loi sur la protection des renseignements personnels et les documents électroniques


Français
Office of the Privacy Commissioner of Canada
Commissariat à la protection de la vie privée du Canada
Search priv.gc.ca
For individuals
For businesses
For federal institutions
Report a concern
OPC actions and decisions
About the OPC
Home → Privacy topics → Privacy laws in Canada

The *Personal Information Protection and Electronic Documents Act* (PIPEDA)

PIPEDA requirements in brief

Personal information, coverage, complaints, principles

Which privacy law applies?

Interactive search based on type of information and organization

Legislative reform

Submissions to parliament, recommendations

Features

Privacy Guide for Businesses

What Canadian businesses need to know to comply with federal privacy law

Learn about PIPEDA and find information to help businesses understand and comply with the law.

English
Commissariat à la protection de la vie privée du Canada
Office of the Privacy Commissioner of Canada
Rechercher dans priv.gc.ca
Pour les individus
Pour les entreprises
Pour les institutions fédérales
Signaler un problème
Mesures et décisions prises par le Commissariat
À propos du Commissariat
Accueil → Sujets liés à la protection de la vie privée → Lois sur la protection des renseignements personnels au Canada

La *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE)

En bref : les obligations prévues par la LPRPDE

Renseignements personnels, couverture, plaintes, principes

Principes relatifs à l'équité dans le traitement de l'information

Responsabilité, détermination des fins de la collecte des renseignements, consentement, limitation de la collecte, limitation de l'utilisation, de la communication et de la conservation, exactitude, mesures de sécurité, transparence, accès aux renseignements personnels, possibilité de porter plainte à l'égard du non-respect des principes

Lois et règlements associés

Lois, lois connexes, règlements

Quelle loi sur la protection de la vie privée s'applique?

Recherche interactive basée sur le type d'information et d'organisation

Aide à la conformité

Guide pour les entreprises, enjeux spécifiques, bulletins d'interprétation

Enquêtes visant les entreprises

Conclusions

Réforme législative

Soumissions au Parlement, recommandations

En vedette

Guide sur la protection de la vie privée à l'intention des entreprises

Ce que les entreprises canadiennes doivent savoir pour se conformer à la loi fédérale sur la protection des renseignements personnels

10 conseils de protection de la vie privée pour les entreprises

10 conseils de protection de la vie privée pour les entreprises :
CAFÉ

Protégez la vie privée de vos clients [vidéo]

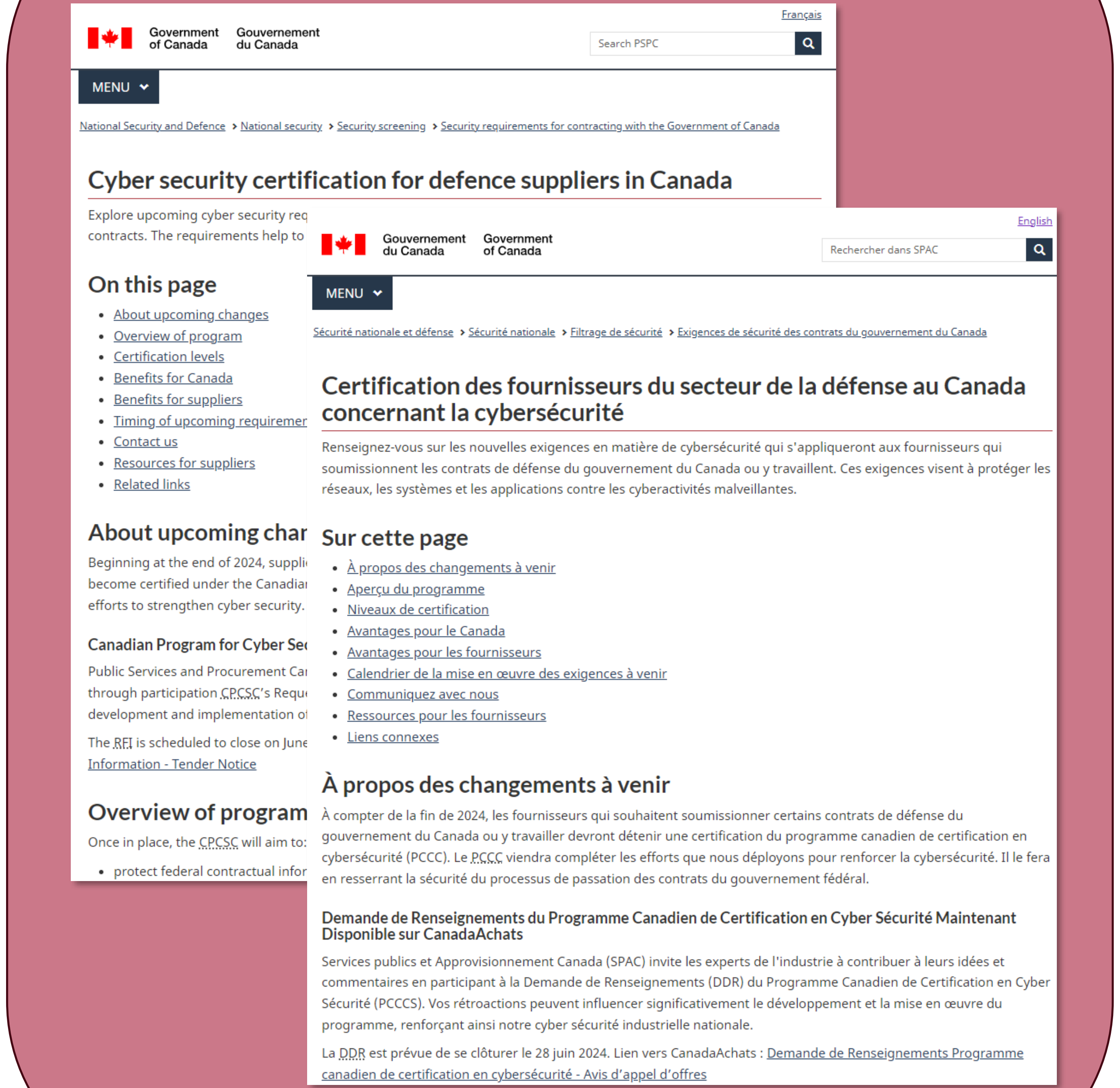
La LPRPDE et votre entreprise
Ce que vous devez savoir à propos de la protection de la vie privée de vos clients
YouTube

CPCSC

PCCC

Canadian program for cyber security certification

Programme canadien de certification en cybersécurité



National Security and Defence > National security > Security screening > Security requirements for contracting with the Government of Canada

Cyber security certification for defence suppliers in Canada

Explore upcoming cyber security req
contracts. The requirements help to

On this page

- About upcoming changes
- Overview of program
- Certification levels
- Benefits for Canada
- Benefits for suppliers
- Timing of upcoming requiremer
- Contact us
- Resources for suppliers
- Related links

About upcoming char

Beginning at the end of 2024, suppli
become certified under the Canadia
efforts to strengthen cyber security.

Canadian Program for Cyber Sec

Public Services and Procurement Ca
through participation CPCSC's Requ
development and implementation o

The RFI is scheduled to close on June
Information - Tender Notice

Overview of program

Once in place, the CPCSC will aim to:

- protect federal contractual infor

Sécurité nationale et défense > Sécurité nationale > Filtrage de sécurité > Exigences de sécurité des contrats du gouvernement du Canada

Certification des fournisseurs du secteur de la défense au Canada concernant la cybersécurité

Renseignez-vous sur les nouvelles exigences en matière de cybersécurité qui s'appliqueront aux fournisseurs qui soumissionnent les contrats de défense du gouvernement du Canada ou y travaillent. Ces exigences visent à protéger les réseaux, les systèmes et les applications contre les cyberactivités malveillantes.

Sur cette page

- À propos des changements à venir
- Aperçu du programme
- Niveaux de certification
- Avantages pour le Canada
- Avantages pour les fournisseurs
- Calendrier de la mise en œuvre des exigences à venir
- Communiquez avec nous
- Ressources pour les fournisseurs
- Liens connexes

À propos des changements à venir

À compter de la fin de 2024, les fournisseurs qui souhaitent soumissionner certains contrats de défense du gouvernement du Canada ou y travailler devront détenir une certification du programme canadien de certification en cybersécurité (PCCC). Le PCCC viendra compléter les efforts que nous déployons pour renforcer la cybersécurité. Il le fera en resserrant la sécurité du processus de passation des contrats du gouvernement fédéral.

Demande de Renseignements du Programme Canadien de Certification en Cyber Sécurité Maintenant Disponible sur CanadaAchats

Services publics et Approvisionnement Canada (SPAC) invite les experts de l'industrie à contribuer à leurs idées et commentaires en participant à la Demande de Renseignements (DDR) du Programme Canadien de Certification en Cyber Sécurité (PCCCS). Vos rétroactions peuvent influencer significativement le développement et la mise en œuvre du programme, renforçant ainsi notre cyber sécurité industrielle nationale.

La DDR est prévue de se clôturer le 28 juin 2024. Lien vers CanadaAchats : Demande de Renseignements Programme canadien de certification en cybersécurité - Avis d'appel d'offres

ISO 27001 : 2022

Information Security Management System (ISMS)

- Policies
- Procedures
- Standards
- Guidelines

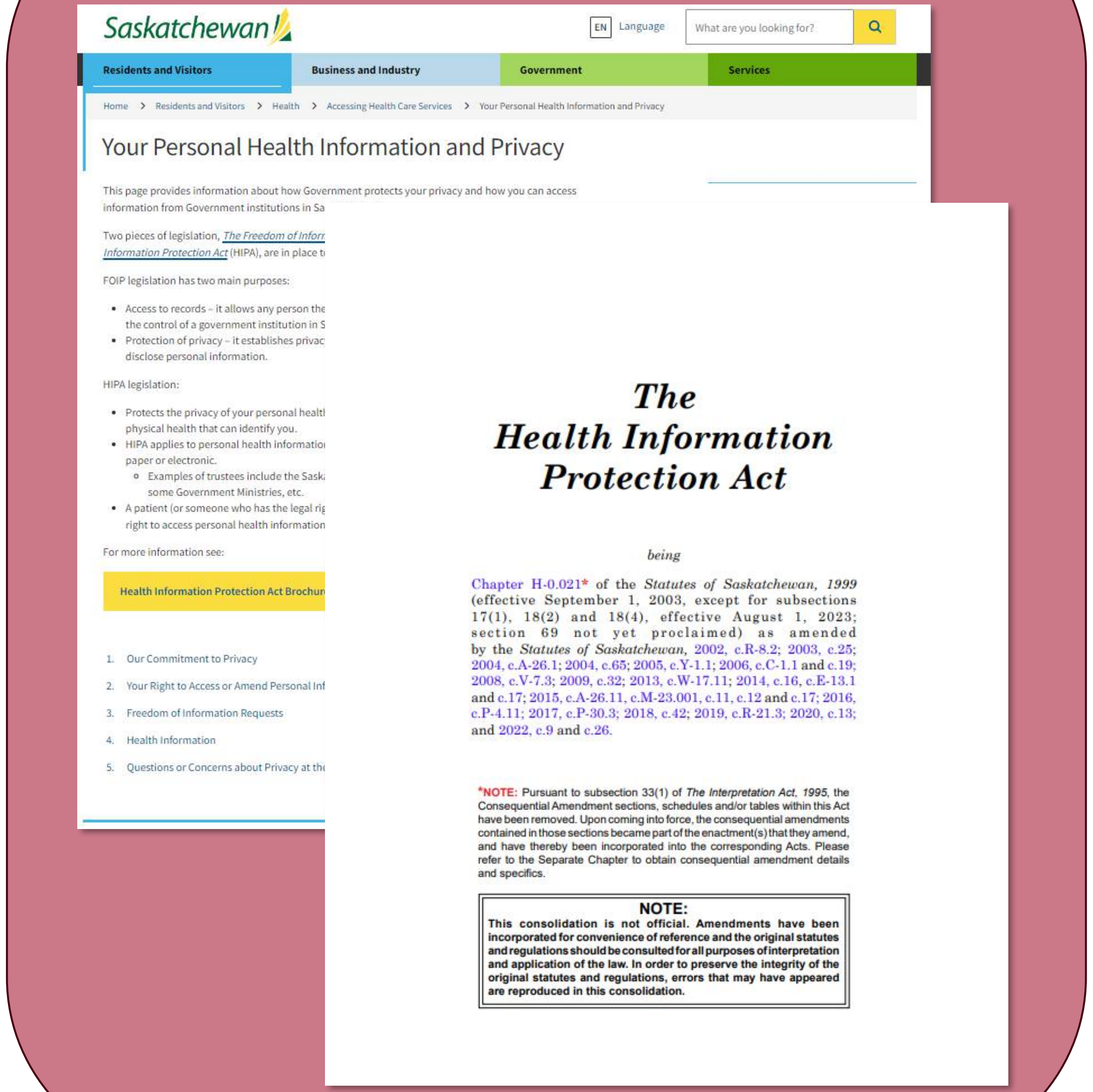
Système de gestion de la sécurité de l’information (SGSI)

- Politiques
- Procédures
- Normes
- Lignes directrices

HIPA

The Health Information Protection Act

La loi sur la protection des renseignements personnels


Saskatchewan
EN Language
What are you looking for?
Residents and Visitors
Business and Industry
Government
Services
Home > Residents and Visitors > Health > Accessing Health Care Services > Your Personal Health Information and Privacy

Your Personal Health Information and Privacy

This page provides information about how Government protects your privacy and how you can access information from Government institutions in Sa

Two pieces of legislation, *The Freedom of Inforr* *Information Protection Act* (HIPA), are in place t

FOIP legislation has two main purposes:

- Access to records – it allows any person the the control of a government institution in S
- Protection of privacy – it establishes privac disclose personal information.

HIPA legislation:

- Protects the privacy of your personal healt physical health that can identify you.
- HIPA applies to personal health informatio paper or electronic.
  - Examples of trustees include the Sask some Government Ministries, etc.
- A patient (or someone who has the legal rig right to access personal health information

For more information see:

1. Our Commitment to Privacy
2. Your Right to Access or Amend Personal Inf
3. Freedom of Information Requests
4. Health Information
5. Questions or Concerns about Privacy at the

The Health Information Protection Act

being

Chapter H-0.021* of the *Statutes of Saskatchewan, 1999* (effective September 1, 2003, except for subsections 17(1), 18(2) and 18(4), effective August 1, 2023; section 69 not yet proclaimed) as amended by the *Statutes of Saskatchewan*, 2002, c.R-8.2; 2003, c.25; 2004, c.A-26.1; 2004, c.65; 2005, c.Y-1.1; 2006, c.C-1.1 and c.19; 2008, c.V-7.3; 2009, c.32; 2013, c.W-17.11; 2014, c.16, c.E-13.1 and c.17; 2015, c.A-26.11, c.M-23.001, c.11, c.12 and c.17; 2016, c.P-4.11; 2017, c.P-30.3; 2018, c.42; 2019, c.R-21.3; 2020, c.13; and 2022, c.9 and c.26.

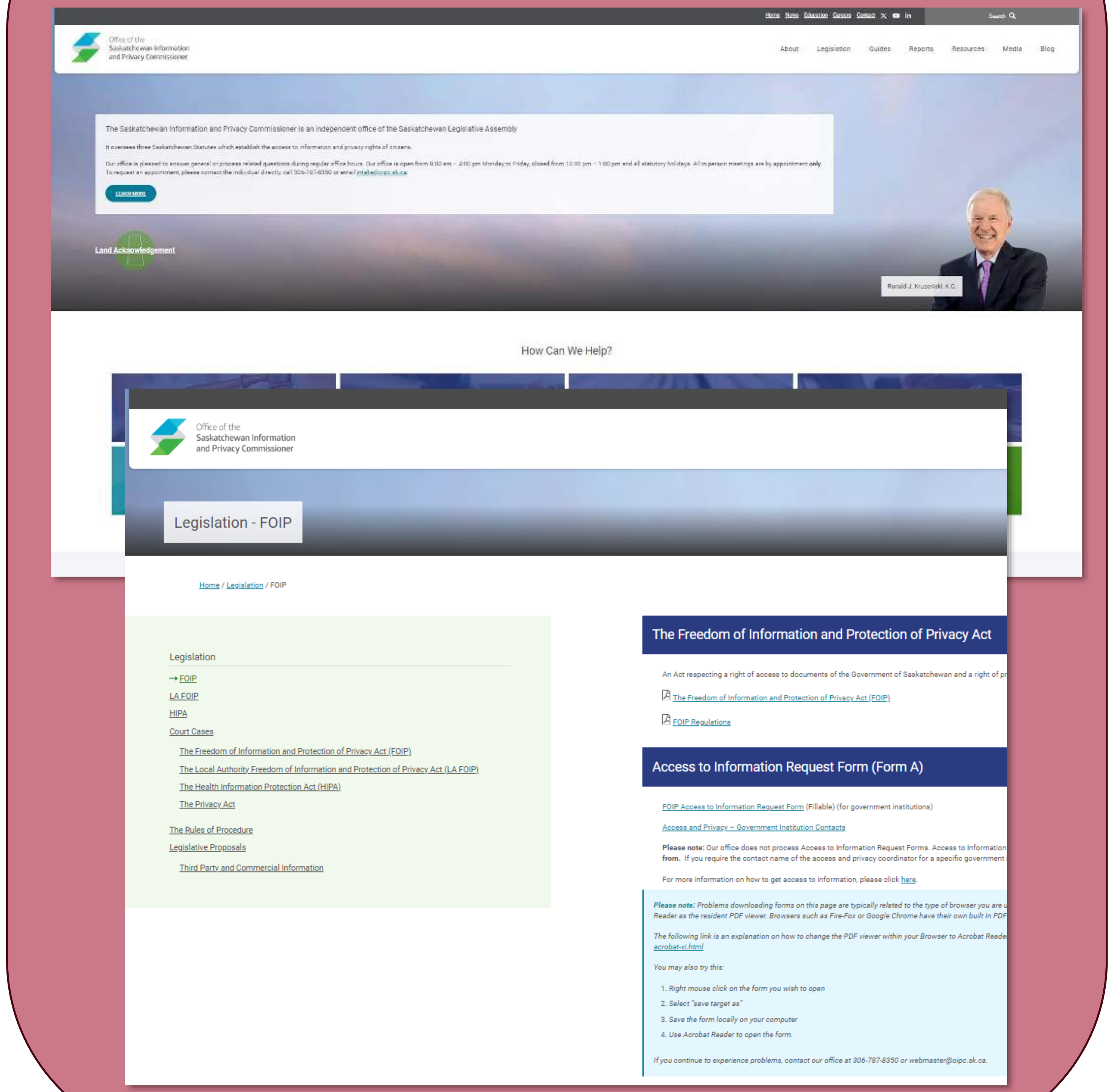
*NOTE: Pursuant to subsection 33(1) of *The Interpretation Act, 1995*, the Consequential Amendment sections, schedules and/or tables within this Act have been removed. Upon coming into force, the consequential amendments contained in those sections became part of the enactment(s) that they amend, and have thereby been incorporated into the corresponding Acts. Please refer to the Separate Chapter to obtain consequential amendment details and specifics.

NOTE:
This consolidation is not official. Amendments have been incorporated for convenience of reference and the original statutes and regulations should be consulted for all purposes of interpretation and application of the law. In order to preserve the integrity of the original statutes and regulations, errors that may have appeared are reproduced in this consolidation.

SK FIPPA

Freedom of Information and Protection of Privacy Act

La loi sur la protection des renseignements personnels


Home News Education Careers Contact
Search
Office of the Saskatchewan Information and Privacy Commissioner
About
Legislation
Guides
Reports
Resources
Media
Blog
LEARN MORE
Land Acknowledgement
Ronald J. Kruzeniski, K.C.
How Can We Help?

The Saskatchewan Information and Privacy Commissioner is an independent office of the Saskatchewan Legislative Assembly

It oversees three Saskatchewan Statutes which establish the access to information and privacy rights of citizens.

Our office is pleased to answer general or process related questions during regular office hours. Our office is open from 8:00 am – 4:00 pm Monday to Friday, closed from 12:00 pm – 1:00 pm and all statutory holidays. All in person meetings are by appointment **only**. To request an appointment, please contact the individual directly, call 306-787-8350 or email intake@oipc.sk.ca.

Legislation - FOIP

Home / Legislation / FOIP

Legislation

- → FOIP
- LA FOIP
- HIPA
- Court Cases
  - The Freedom of Information and Protection of Privacy Act (FOIP)
  - The Local Authority Freedom of Information and Protection of Privacy Act (LA FOIP)
  - The Health Information Protection Act (HIPA)
  - The Privacy Act
- The Rules of Procedure
- Legislative Proposals
  - Third Party and Commercial Information

The Freedom of Information and Protection of Privacy Act

An Act respecting a right of access to documents of the Government of Saskatchewan and a right of pr

The Freedom of Information and Protection of Privacy Act (FOIP)

FOIP Regulations

Access to Information Request Form (Form A)

FOIP Access to Information Request Form (Fillable) (for government institutions)

Access and Privacy – Government Institution Contacts

Please note: Our office does not process Access to Information Request Forms. Access to Information **from.** If you require the contact name of the access and privacy coordinator for a specific government

For more information on how to get access to information, please click here.

Please note: *Problems downloading forms on this page are typically related to the type of browser you are u Reader as the resident PDF viewer. Browsers such as Fire-Fox or Google Chrome have their own built in PDF*

The following link is an explanation on how to change the PDF viewer within your Browser to Acrobat Reade acrobat-xi.html

You may also try this:

1. *Right mouse click on the form you wish to open*
2. *Select "save target as"*
3. *Save the form locally on your computer*
4. *Use Acrobat Reader to open the form.*

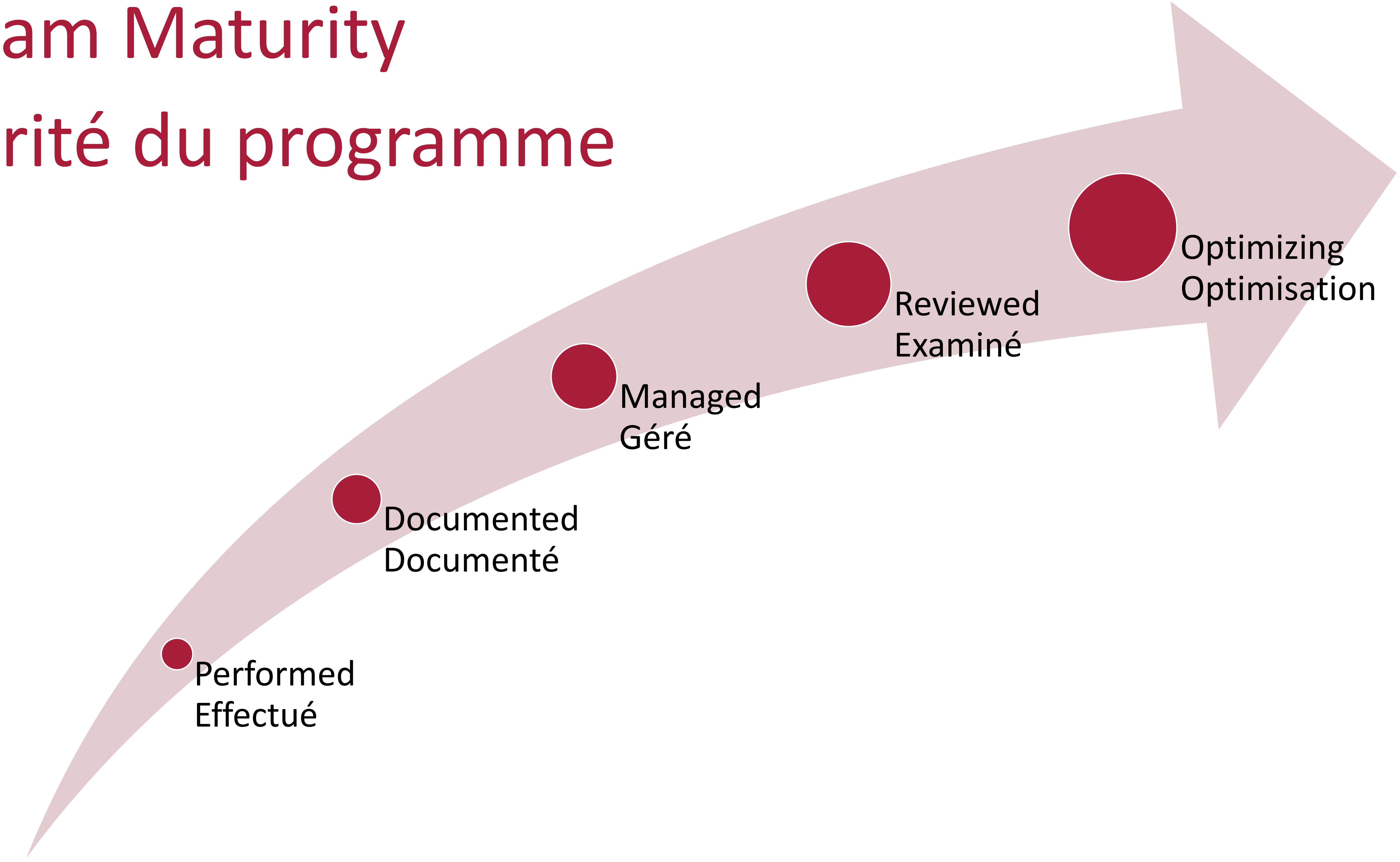
If you continue to experience problems, contact our office at 306-787-8350 or webmaster@oipc.sk.ca.

Data Security Policies

Politiques de sécurité des données

Program Maturity

Maturité du programme



ISO 27001 : 2022

Information Security Management System (ISMS)

- Policies
- Procedures
- Standards
- Guidelines

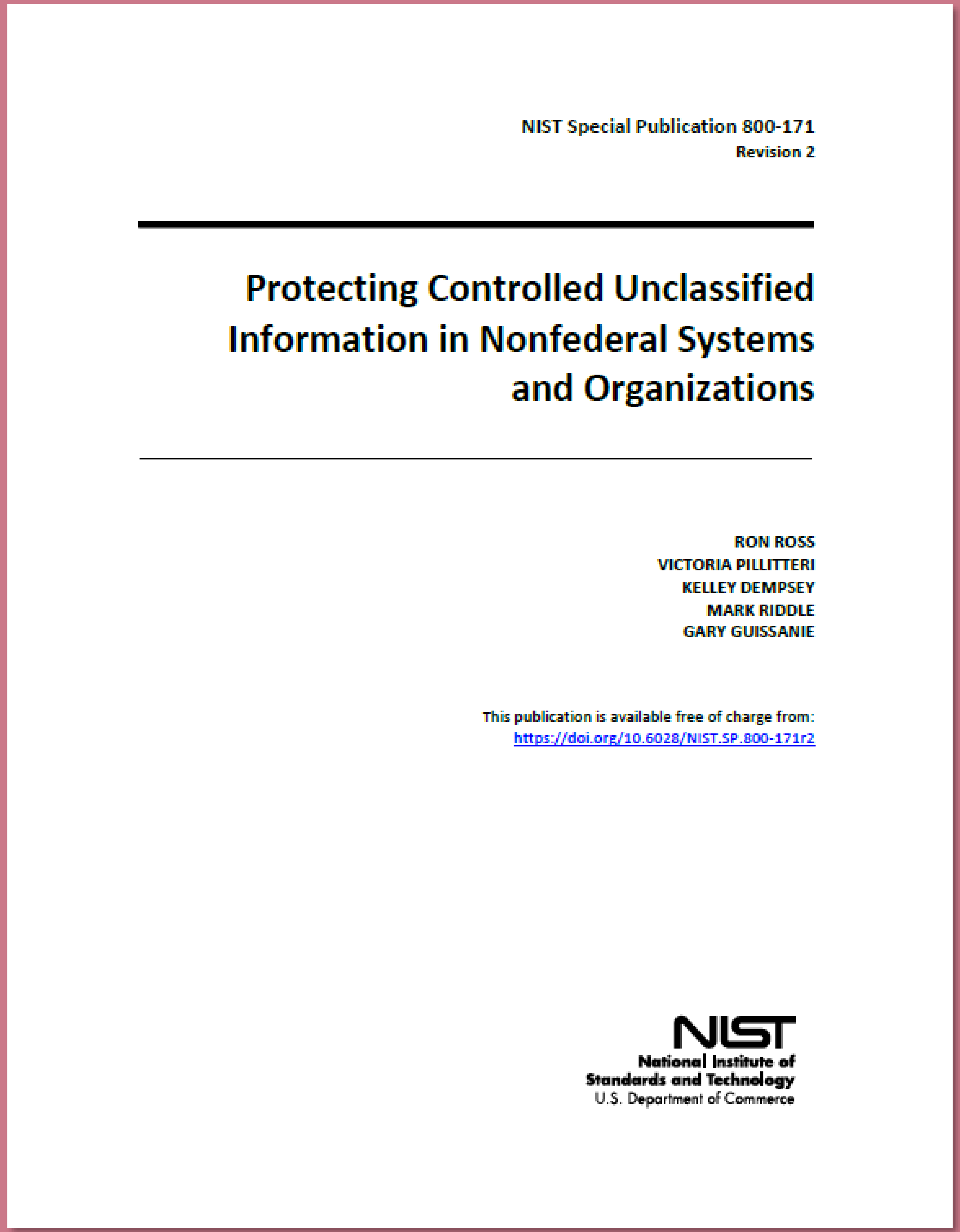
Système de gestion de la sécurité de l'information (SGSI)

- Politiques
- Procédures
- Normes
- Lignes directrices

NIST SP 800-171 r2

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

Protection des informations non classifiées contrôlées dans les systèmes et organisations non féderaux



NIST Special Publication 800-171
Revision 2

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

RON ROSS
VICTORIA PILLITTERI
KELLEY DEMPSEY
MARK RIDDLE
GARY GUISSANIE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-171r2

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

cira

Incident Management
Gestion des incidents

Before

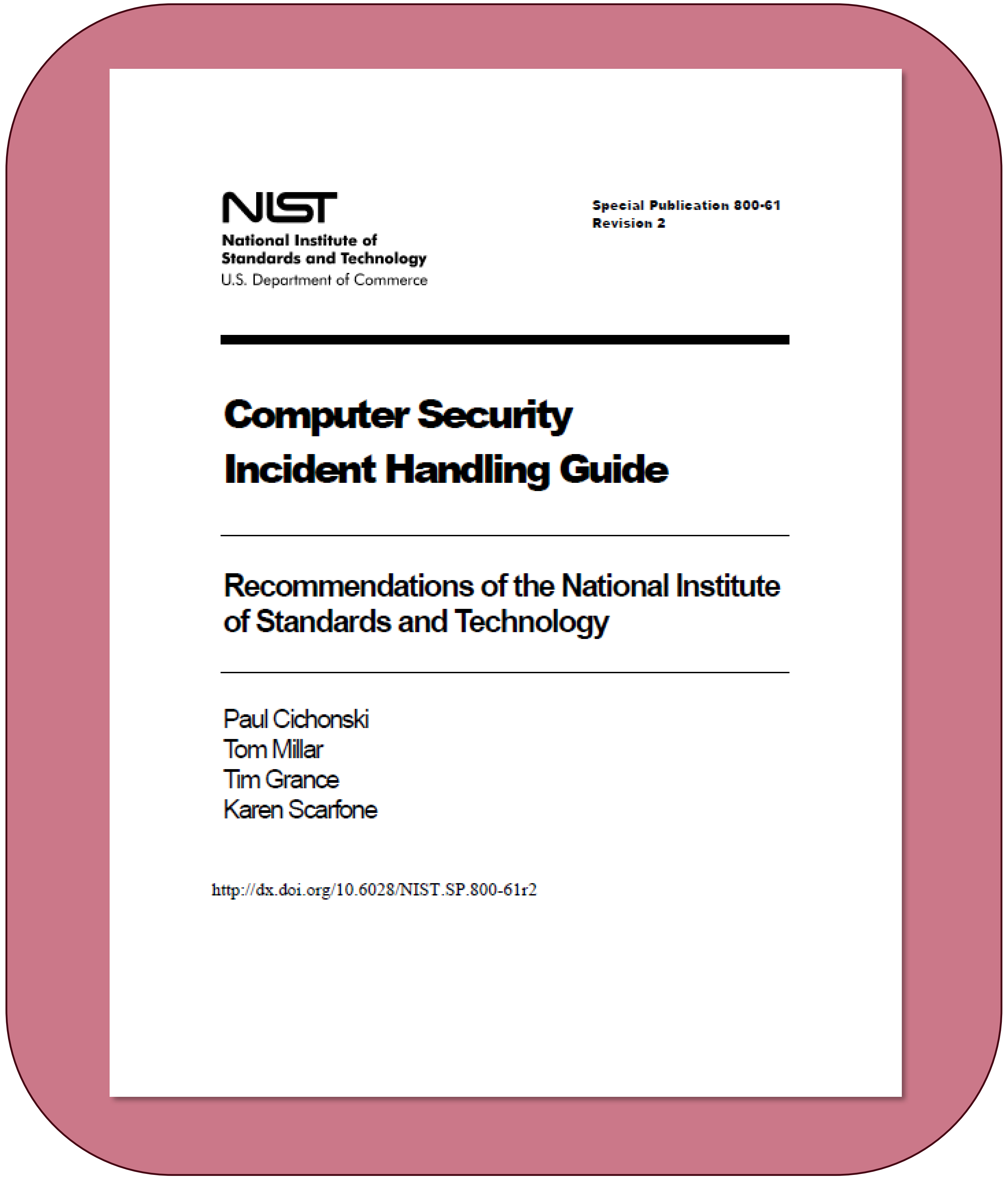
Avant

Incident Response Plan	Plan d’intervention en cas d’incident
• Assess	• Évaluer
• Develop	• Développer
• Educate	• Éduquer
• Communicate	• Communiquer
• Exercise	• Exercice
• Optimize	• Optimiser

NIST SP 800-61 r2

Cyber Security Incident Handling Guide

Guide de traitement des incidents de cybersécurité



NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Special Publication 800-61
Revision 2

Computer Security
Incident Handling Guide

Recommendations of the National Institute of Standards and Technology

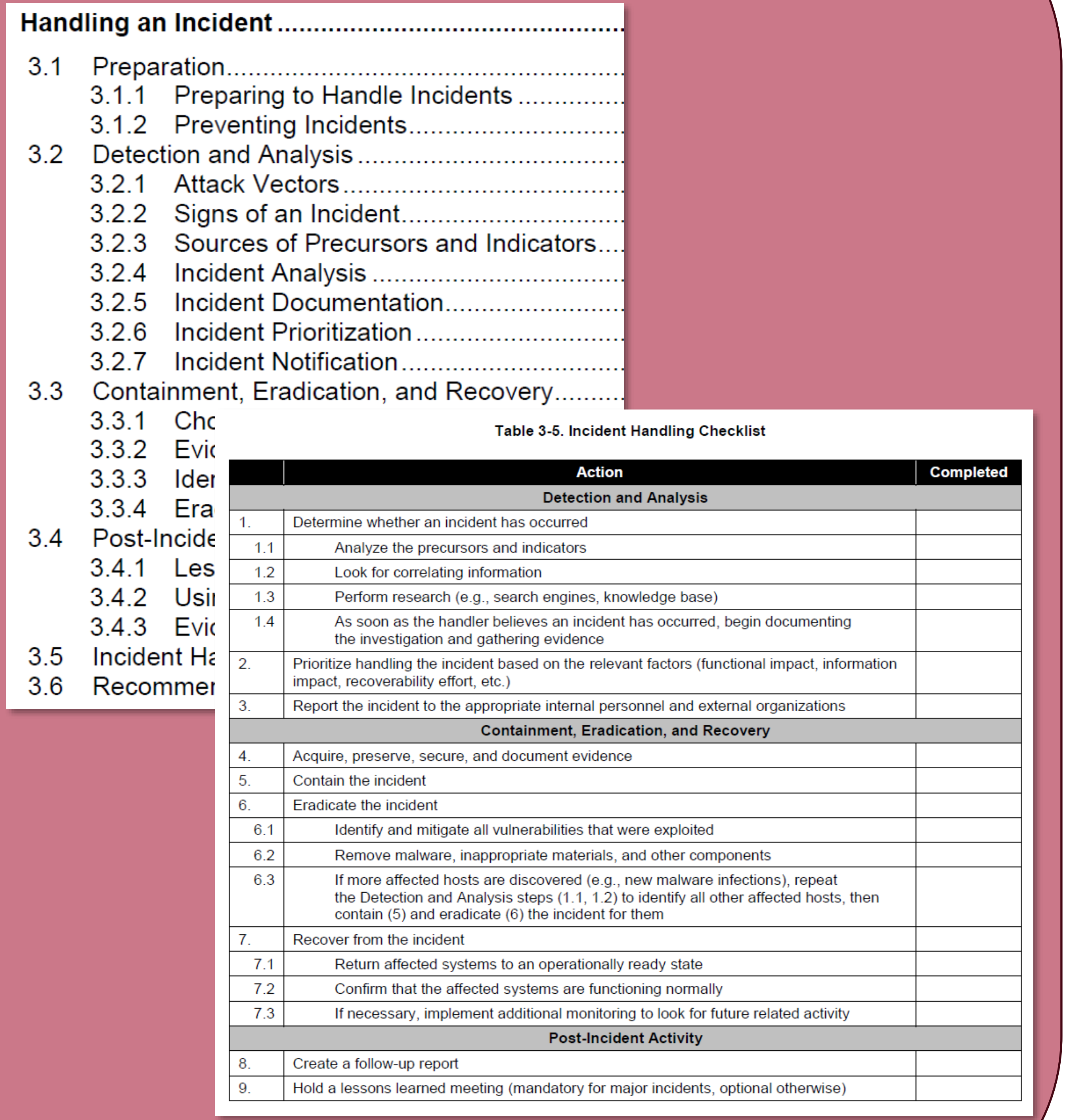
Paul Cichonski
Tom Millar
Tim Grance
Karen Scarfone

http://dx.doi.org/10.6028/NIST.SP.800-61r2

NIST SP 800-61 r2

Cyber Security Incident Handling Guide

Guide de traitement des incidents de cybersécurité



Handling an Incident

Table 3-5. Incident Handling Checklist

	Action	Completed
	Detection and Analysis	
1.	Determine whether an incident has occurred	
1.1	Analyze the precursors and indicators	
1.2	Look for correlating information	
1.3	Perform research (e.g., search engines, knowledge base)	
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence	
2.	Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)	
3.	Report the incident to the appropriate internal personnel and external organizations	
	Containment, Eradication, and Recovery	
4.	Acquire, preserve, secure, and document evidence	
5.	Contain the incident	
6.	Eradicate the incident	
6.1	Identify and mitigate all vulnerabilities that were exploited	
6.2	Remove malware, inappropriate materials, and other components	
6.3	If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them	
7.	Recover from the incident	
7.1	Return affected systems to an operationally ready state	
7.2	Confirm that the affected systems are functioning normally	
7.3	If necessary, implement additional monitoring to look for future related activity	
	Post-Incident Activity	
8.	Create a follow-up report	
9.	Hold a lessons learned meeting (mandatory for major incidents, optional otherwise)	

During
Au cours de

Keys to Success

1. Make a formal declaration
2. Engage stakeholders and partners
3. Follow the plan
4. Document everything

Les clés du succès

1. Faites une déclaration formelle
2. Engagez les partenaires
3. Suivez le plan
4. Documentez tout

After

Après

Recovery

- People
- Process
- Technology
- Data
- Reputation

Récupération

- Les gens
- Processus
- La technologie
- Données
- Réputation

Cyber Risk Insurance

Assurance contre les cyberrisques

Challenges

- New, more rigorous requirements
- Limited list of acceptable security partners
- New scrutiny and limitations on payouts

Problèmes

- De nouvelles exigences plus rigoureuses
- Liste limitée de partenaires de sécurité acceptables
- Nouvel examen et limites sur les paiements

Partners for Government Agencies

Partenaires pour les organismes gouvernementaux

CANADIAN CENTRE FOR
CYBER SECURITY

CENTRE CANADIEN POUR LA
CYBERSÉCURITÉ

cira

CIRA.CA

Thank you.

JAMIE HARI | Director / Directeur, CyberDNS
Jamie.hari@cira.ca

CIRA.CA

FACEBOOK	/cira.ca	TIKTOK	/@cira.ca
INSTAGRAM	/ciradotca	YOUTUBE	/ciranews
MASTODON	/@cira	LINKEDIN	/company/canadian-internet-registration-authority
X	/ciranews		