See Something, Say Something

Coordinating the Disclosure of Security Vulnerabilities in Canada

June 2021

Yuan Stevens | Stephanie Tran | Ryan Atkinson | Sam Andrey

cybersecure policy exchange

Powered by RBC®

Cybersecure Policy Exchange

The Cybersecure Policy Exchange (CPX) is an initiative dedicated to advancing effective and innovative public policy in cybersecurity and digital privacy, powered by RBC through Rogers Cybersecure Catalyst and the Ryerson Leadership Lab. Our goal is to broaden and deepen the debate and discussion of cybersecurity and digital privacy policy in Canada, and to create and advance innovative policy responses, from idea generation to implementation. This initiative is sponsored by the Royal Bank of Canada; we are committed to publishing independent and objective findings and ensuring transparency by declaring the sponsors of our work.

Rogers Cybersecure Catalyst

Rogers Cybersecure Catalyst is Ryerson University's national centre for innovation and collaboration in cybersecurity. The Catalyst works closely with the private and public sectors and academic institutions to help Canadians and Canadian businesses tackle the challenges and seize the opportunities of cybersecurity. Based in Brampton, the Catalyst delivers training; commercial acceleration programming; support for applied R&D; and public education and policy development, all in cybersecurity.

Ryerson Leadership Lab

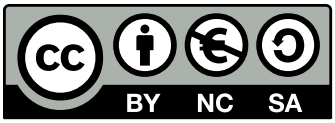
The Ryerson Leadership Lab is an action-oriented think tank at Ryerson University dedicated to developing new leaders and solutions to today's most pressing civic challenges. Through public policy activation and leadership development, the Leadership Lab's mission is to build a new generation of skilled and adaptive leaders committed to a more trustworthy, inclusive society.

Funded by the Government of Canada | Canada

This project is sponsored by the Department of National Defence's Mobilizing Insights in Defence and Security program.

How to Cite this Report
Stevens, Y., Tran, S., Atkinson, R., Andrey, S. (2021, June). *See Something, Say Something: Coordinating the Disclosure of Security Vulnerabilities in Canada*. Retrieved from https://www.cybersecurepolicy.ca/vulnerability-disclosure.

350 Victoria St, Toronto, ON M5B 2K3
ISBN : 978-1-77417-027-4



Contributors
Sam Andrey, Director of Policy & Research, Ryerson Leadership Lab
Ryan Atkinson, Policy Consultant, Cybersecure Policy Exchange
Karim Bardeesy, Executive Director, Ryerson Leadership Lab
Sumit Bhatia, Director of Innovation and Policy, Rogers Cybersecure Catalyst
Zaynab Choudhry, Design Lead
Charles Finlay, Executive Director, Rogers Cybersecure Catalyst
Braelyn Guppy, Marketing and Communications Lead, Ryerson Leadership Lab
Sharan Khela, Research and Policy Intern, Cybersecure Policy Exchange
Mohammed (Joe) Masoodi, Policy Analyst, Cybersecure Policy Exchange
Stephanie Tran, Research and Policy Assistant, Cybersecure Policy Exchange
Yuan Stevens, Policy Lead, Cybersecure Policy Exchange

Our work is guided by these core principles:

- Responsible technology governance is a key to Canadians' cybersecurity and digital privacy.
- Complex technology challenges call for original insights and innovative policy solutions.
- Canadians' opinions matter, and must inform every discussion of technology policy.
- Cybersecurity needs to be explained and made relevant to Canadians, and cannot be relegated to language and concepts accessible only to experts.
- Canadian institutions matter, and must evolve to meet new cybersecurity and digital privacy risks to maintain the public trust.
- Harms, inequities and injustices arising from the unequal use or application of technology must be confronted, wherever they exist or could arise.

For more information, visit: https://www.cybersecurepolicy.ca/

@cyberpolicyx @cyberpolicyx Cybersecure Policy Exchange

Executive Summary

Ill-intentioned actors are rapidly developing the technological means to exploit vulnerabilities in the web assets, software, hardware, and networked infrastructure of governments around the world. Numerous jurisdictions have adopted the policy approach of facilitating **coordinated vulnerability disclosure (CVD)** as one means to better secure the public sector's systems, through which external security researchers are provided a predictable and cooperative process to disclose security flaws for patching before they are exploited. **Canada is falling behind its peers and allies in adopting such an approach.**

A global scan of vulnerability disclosure policy approaches indicates that **60 percent of G20 member countries provide distinct and clear disclosure processes** for vulnerabilities involving government systems, with many providing clarity regarding the disclosure process and expectations for security researchers regarding communication and acceptable activity. The Netherlands and the US are particularly leading the way when it comes to providing comprehensive policy and pragmatic solutions for external vulnerability disclosure, acting as a learning model for Canada. Both countries have also begun to provide explicit legal clarification regarding acceptable security research activity, particularly in the context of coordinated vulnerability disclosure.

In Canada, there exists no legal or policy framework regarding security research and vulnerability disclosure done in good faith; that is, done with the intent and in such a way to repair the vulnerability while causing minimal harm. Absent this framework, discovering and disclosing vulnerabilities may result in a security researcher facing liability under the *Criminal Code*, as well as potentially the *Copyright Act*, if exemptions do not apply. Whistleblower legislation in Canada generally would also not apply to vulnerability disclosure except in very limited, specific instances.

Further, Canada's Centre for Cyber Security — and its parent agency the Communications Security Establishment — currently have practices and policies that may discourage people from disclosing vulnerabilities and, on top of this, are also opaque about how such vulnerabilities are handled.

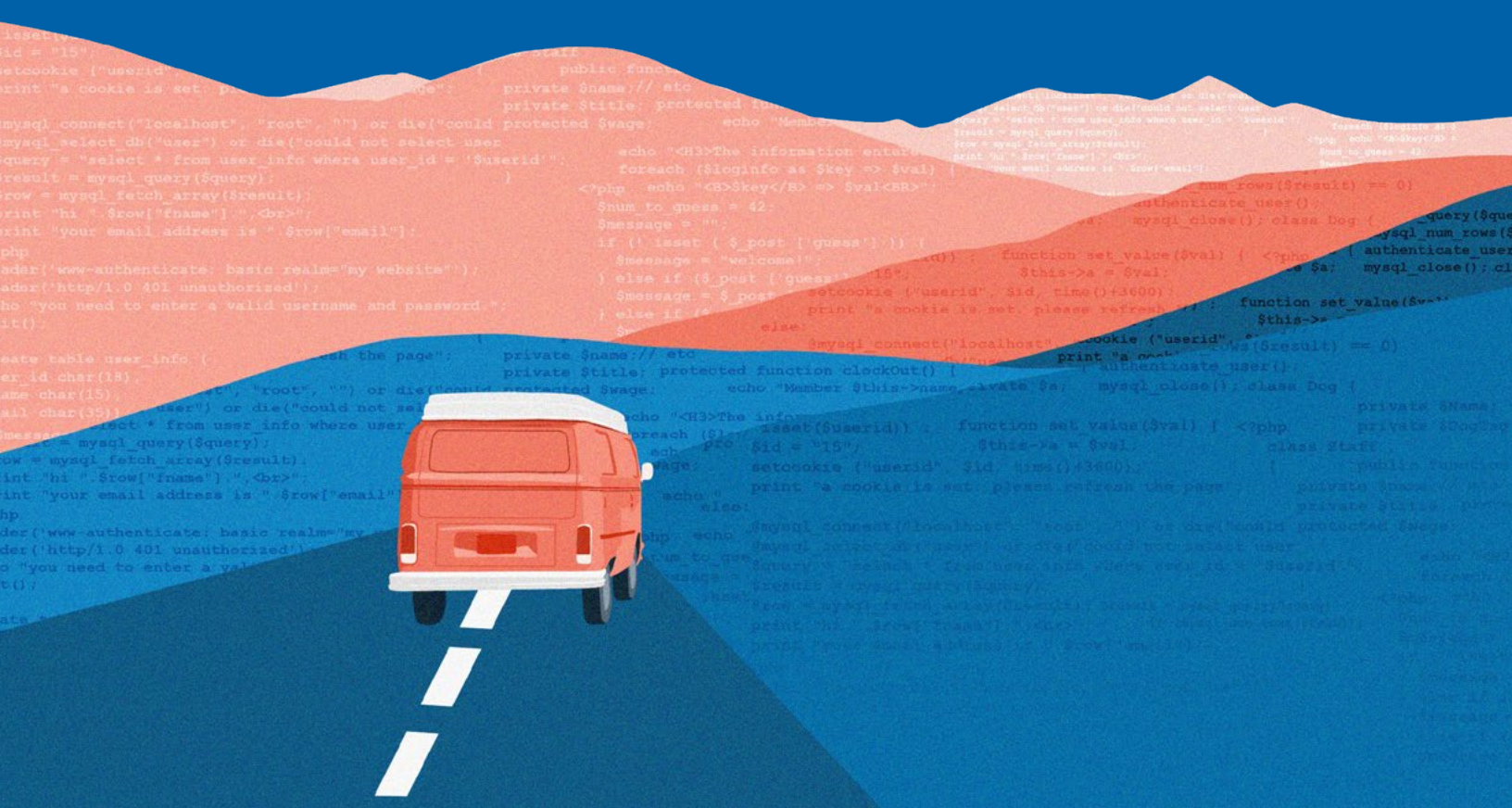
The cumulative effect of this approach in Canada means that there is no straightforward or transparent path for a person wishing to responsibly disclose a security vulnerability found in the computer systems used by the Government of Canada — resulting in possible non-disclosure, public disclosure before remediation, or otherwise enabling the use of security vulnerabilities by attackers in ways that could jeopardize the security of Canada's computer systems and the people that they serve.

In light of these findings, we advocate for the following three policy solutions in Canada to remedy these gaps:

1. Canada needs a **policy framework** for good faith vulnerability discovery and disclosure;

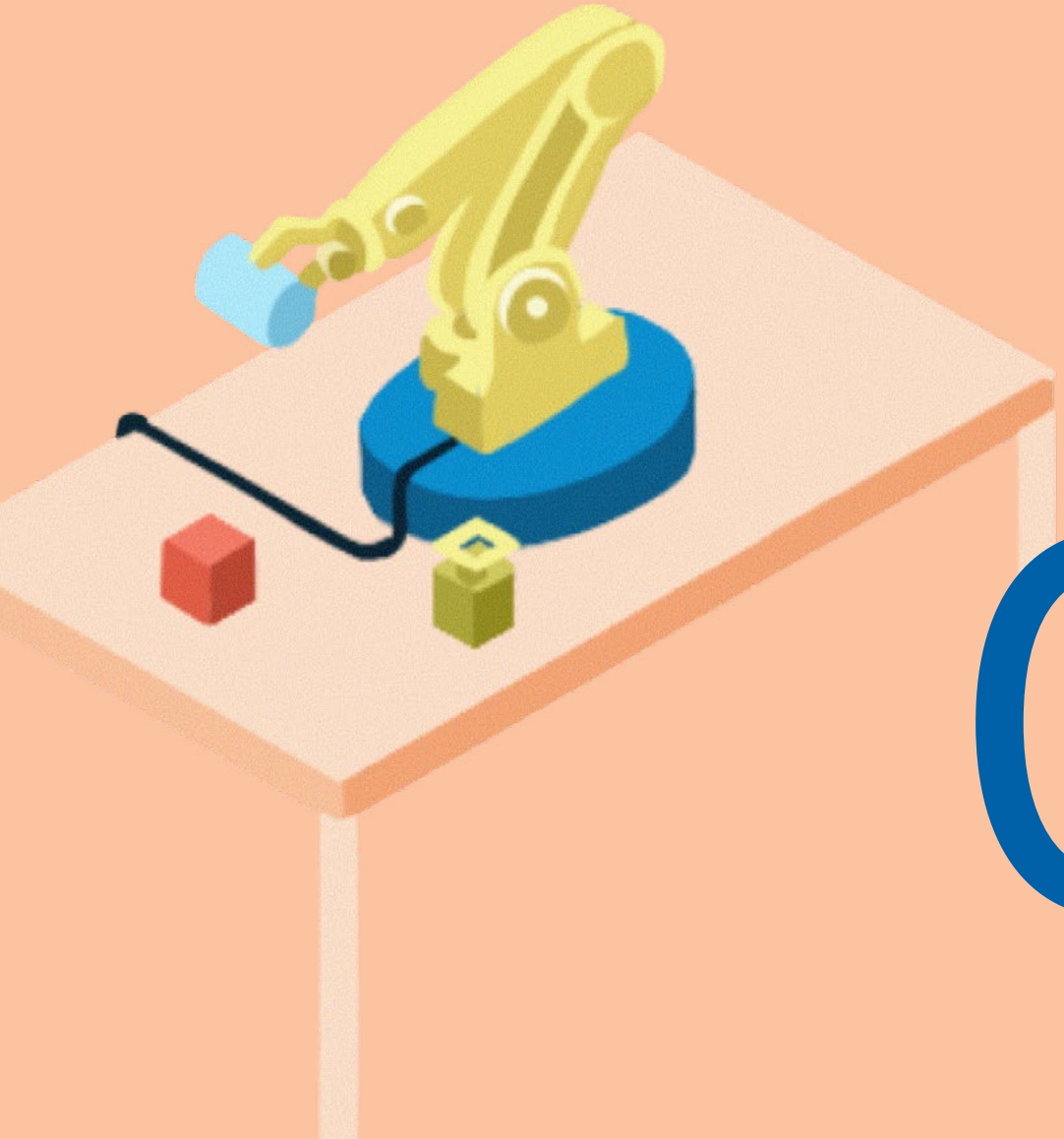
2. Canada should carefully **implement coordinated vulnerability disclosure procedures** for the federal government's computer systems, and draw on emerging **best practices** as it does so; and

3. **Vulnerabilities disclosed** to the government from external actors should be **kept separate** from the government's handling of vulnerabilities uncovered internally in the course of Canada's **defensive and offensive intelligence efforts.**



INTRODUCTION

The Need for Coordinated Vulnerability Disclosure



01

The Need for Coordinated Vulnerability Disclosure

In 2008, the Dutch court faced a difficult decision. Academic researchers at Radboud University decided to examine the security of a smart card, which was being rolled out on a mass scale for use across the country's transit system.[1] The contactless card reader used the MIFARE Classic chip by Dutch manufacturer NXP. The chip was already in use for major transit systems, including London,[2] Hong Kong and Boston,[3] and for government buildings in the Netherlands and elsewhere.[4] In their work, the security researchers discovered that the chip's encryption algorithm was using a random number generator to protect the card's memory that was not, in fact, random at all.[5] The result was that the research team was able to access the chip's encryption protocol, enabling them to use cloned smartcards for limitless transit trips and unauthorized entry into government buildings.

The researchers informed NXP, the Dutch Ministry of the Interior, and the Dutch transit agency not long after discovering the flaw in early March 2008, in hopes that the security flaw could be patched.[6] The researchers sought to give the government and NXP at least six months to remediate the issue before releasing the results of their research at an academic conference in October 2008.[7] The six-month embargo was not an issue for the Dutch intelligence and security agency, which saw the timing as reasonable and beneficial for the government.[8] But in June that year, NXP sought a restraining order against the researchers, hoping to prevent them from publishing their research in October. The judge carefully weighed the interests at stake when security researchers disclose vulnerabilities — including corporate intellectual property rights, human rights such as freedom of expression, and the motivation and impact of security research and hacking activity.[9]

The court rendered its decision in July 2008. In short, the court rejected NXP's request to suppress the information largely on the basis of copyright law and freedom of expression.[10] It held that the chip's algorithm, a mathematical formula, was not a copyrighted work and had never been made public. The court also found that the researchers lacked the element of intention needed for criminal liability, given that their work "sought only to raise the issue of social wrongdoing and promote scientific research on encryption."[11]

More than this, the court concluded that the risk of misuse of the chip emanated not from the researchers' activity, but due to the chip design itself. NXP had also provided an assessment of harm that was far too general and oversimplified to justify the limitations they sought on the researchers' freedom of expression. In the end, a student at the centre of the Radboud research project won numerous awards for his contributions to the field of security,[12] the professors involved continued their illustrious careers, and NXP continued to release improved smartcard chips in which security researchers invariably found vulnerabilities.

The case is significant for the way it has shaped policy discourse and solutions in the Netherlands regarding **coordinated vulnerability disclosure (CVD)**, a policy approach that provides external security researchers a predictable and cooperative process to disclose security flaws for patching before they are exploited.[13] Since 2008, security

researchers in the Netherlands have been able to rely on this legal decision to support the claim that disclosing vulnerabilities responsibly and in a coordinated fashion is indeed possible and is, in fact, often desirable in pursuit of better ensuring the security of the government's computer systems and critical infrastructure.

After numerous other significant hacks of government systems, the Dutch government released two documents in 2013 that explained how coordinated vulnerability disclosure should be treated by organizations, prosecutors in the Netherlands, and the Dutch National Cyber Security Centre, both of which are described in detail below.

The case also illustrates the need for governments to consider facilitating disclosure of vulnerabilities found in their systems (of vital importance) as one solution among many in the pursuit of more secure infrastructure. This is because software and hardware will always contain latent vulnerabilities that have the potential to be exploited,[14] regardless of how much testing is done prior to deployment.[15]

Cyberattacks on critical infrastructure are also now the norm[16] and come at alarming costs. Indeed, cyberattacks are significantly disrupting digital infrastructure and operations in Canada at an increasing rate, with annual economic losses estimated at more than $3 billion.[17] A recent report estimated that Canada experienced more than 4,000 ransomware incidents in 2020 — with costs to organizations exceeding $1 billion.[18] Statistics Canada also found that more than one-fifth of Canadian businesses reported being impacted by cybersecurity incidents in 2019.[19] Indeed, the rapidness of technological development has resulted in calls for internationally coordinated responses to cyberattacks[20] and the vulnerabilities that can enable them.[21]

On top of this, approximately 28% of organizations have reported an increase in cyberattacks, insider threats or data breaches since the COVID-19 pandemic began.[22] Another report found that the average cost of data breaches in Canada has risen 7% since 2019,[23] while the average ransom demand increased by 33% since Q4 2019.[24] Internet-connected (Internet of Things or IoT) devices procured by federal governments warrant particular attention when it comes to security considerations, given their interconnected nature and the supply chain risks that insecure devices pose to the government.[25] The 2020 National Cyber Threat Assessment issued by the Canadian Centre for Cyber Security found that the targeting of critical infrastructure industrial control systems will very likely increase in the next two years, as attackers attempt to place increased pressure to promptly accede to ransom demands.[26]

Governments, organizations, and individuals all benefit when security researchers are encouraged and enabled to disclose vulnerabilities in "good faith"[27] — a term used throughout this report referring to vulnerability disclosure done with the intent and in such a way to repair the vulnerability while causing minimal harm. Good faith need not be the only way to understand such activity; disclosure may also be done in the public interest and, for those who prefer such terminology, may constitute "ethical hacking."[28] In any case, providing responsible and predictable vulnerability disclosure procedures in turn allows researchers to responsibly disclosure vulnerabilities for remediation before malicious attackers exploit such weaknesses.

Coordinated Vulnerability Disclosure as Global Best Practice

Facilitating coordinated vulnerability disclosure is becoming a policy standard and best practice for organizations and governments around the globe.[29] Beyond the Netherlands, the US[30] and the UK,[31] as well as the EU,[32] are among the jurisdictions that have begun providing legal clarification and procedures for facilitating coordinated vulnerability disclosure as one means to better secure the public sector's systems. However, the topic remains understudied and underutilized in the Canadian context, leaving Canada's federal institutions potentially more vulnerable in the face of threat actors.[33]

To this end, we engaged in a review of interdisciplinary academic literature, government policies and procedure, as well as legislation, to provide a scan of current CVD approaches in Canada and around the globe, with a particular focus on countries that are members of the G20 and a few select countries elsewhere with noteworthy policy developments that add to the diversity of countries analyzed (see **Appendix A**). Limiting this report's scope of analysis to focus primarily on the CVD policy approaches of G20 members was logical given the group's emphasis since at least 2017 on reducing vulnerabilities in internet infrastructure, as well as implementing norms regarding cyberattacks,[34] an emphasis which has been of heightened importance during the COVID-19 pandemic.[35]

This report also draws on two workshops held in early 2021, which brought together computer security experts hailing from industry,

Intent of Report

This report seeks to help the Government of Canada adapt to meet the challenges posed by digital transformation, and the security threats that come with rapid technological development and deployment. While far from providing exhaustive solutions, this report begins to identify both policy gaps and pragmatic solutions that can harness the skillset of security researchers and professionals who find and responsibly disclose security flaws in government websites, software, hardware, IoT devices, and critical infrastructure before attackers do.

government, academia, civil society, and computer security incident response teams who offered expertise on the benefits, risks, and best practices for CVD frameworks that could be implemented in the Canadian context (see list of participants in **Appendix B**, whose names are listed with permission). The workshops were held under the Chatham House Rule, in order to facilitate productive dialogue on such a critical public policy topic without the need to represent certain organizations' interests.

While this project received financial support from the Department of National Defence's Mobilizing Insights in Defence and Security program, this report's findings have implications for the security of computer systems across all government bodies — not only at the federal level, but also at the provincial and municipal levels — and additionally implicates the systems provided by third-party software and hardware vendors for government use.

The Global State of Coordinated Vulnerability Disclosure Processes

Governments around the globe have begun providing vulnerability disclosure procedures for their digital systems. The full result of our jurisdictional scan is included in **Appendix A**, which provides information for all G20 member countries, including Spain as a permanent non-member invitee of the G20; and New Zealand, which we included due to its membership in the Five Eyes intelligence alliance; as well as Latvia, the Netherlands and Singapore, whose policy approaches we particularly gained knowledge about through the expert workshops we held in early 2021.

We used a modified version of the standards enumerated by Woszczynski et al.[36] to assess the number of G20 member countries that meet best practices for coordinated vulnerability disclosure, which Canada does not (see **Figure 1**).

Vulnerability Disclosure Procedure	G20	Canada
Has a distinct and clear disclosure process for vulnerabilities involving government systems	12/20 60%	✗
Describes the vulnerability submission and verification process	7/20 35%	✗
Provides terms and rules for disclosers (e.g., limiting what is in scope)	9/20 45%	✗
Publicly disseminates information about vulnerabilities disclosed through coordinated process	7/20 35%	✗
Publicly give acknowledgment or credit after disclosure	5/20 25%	✗

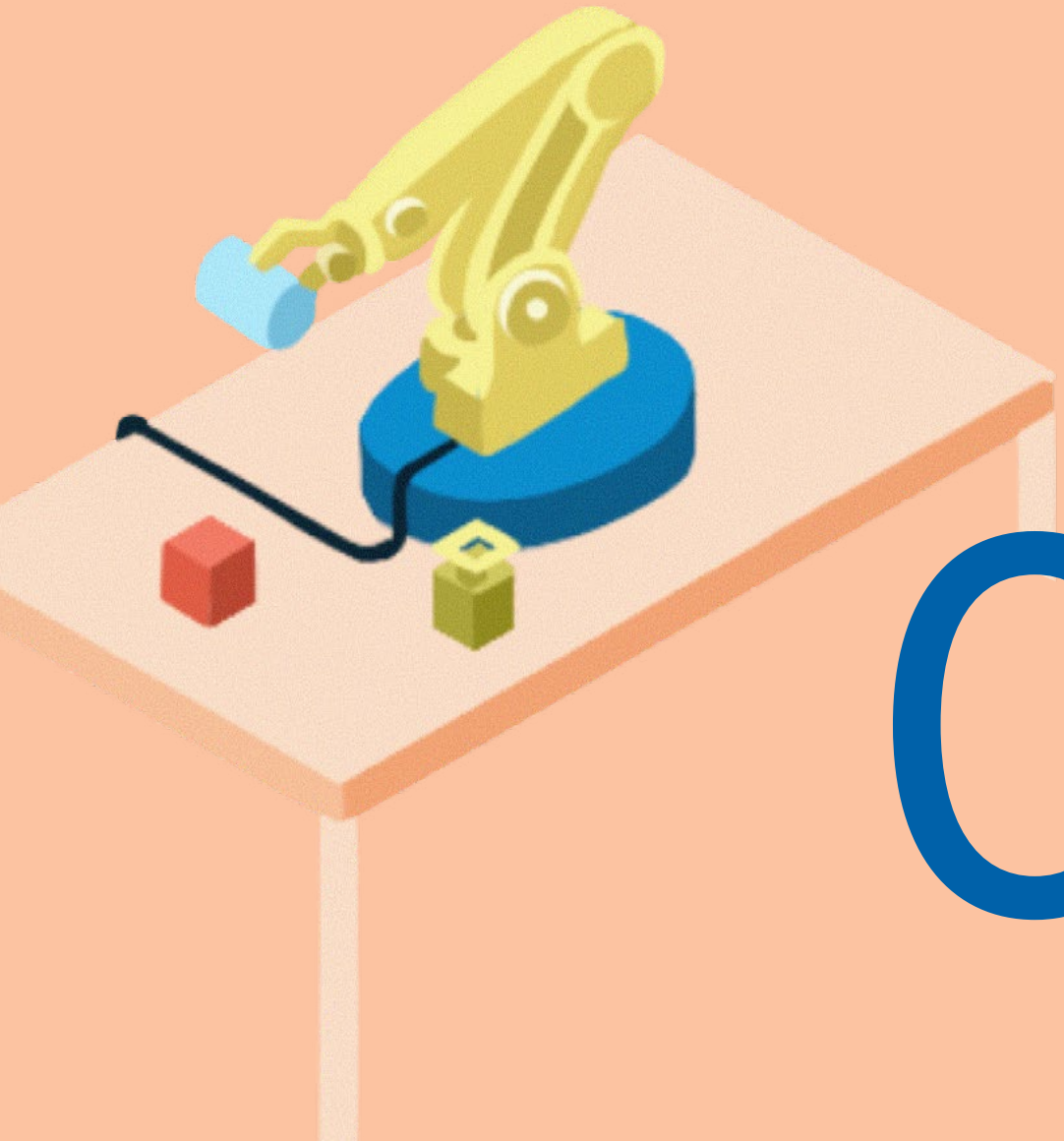
Figure 1: G20 member countries that meet best practices for CVD, which Canada does not

This report demonstrates that Canada appears to be falling behind several of its global peers and allies when it comes to providing a policy framework for good faith security vulnerability discovery and disclosure in respect of government computer systems. Various federal laws, as described below, may have a chilling effect on good faith vulnerability discovery and disclosure in Canada. Despite Canada having a fairly robust system in place for handling "cyber security events" known to the public, Canada's Centre for Cyber Security (CCCS) and its parent agency the Communications Security Establishment (CSE) currently have vulnerability handling practices and procedures generally marked by under-inclusion and opacity.

These organizational practices by the CCCS and CSE — in tandem with a lack of an adequate policy framework in Canada that draws on best practices regarding CVD — operate to dissuade good faith security researchers from discovering or disclosing vulnerabilities that affect the federal government's systems. Canada's current approach to security research activity, or otherwise enable the use of security vulnerabilities by attackers in ways (for example, including but not limited to, selling information on illicit markets) that could jeopardize the security of Canada's computer systems and the people that they serve. It is important to recognize that facilitating coordinated *external* vulnerability disclosure is just one aspect of an organization's (including the government's) security posture and maturity when it comes to addressing the vulnerabilities that exist in software and hardware systems. This is because vulnerabilities can (and should) be discovered and remediated *internally* using various mechanisms through the product development process or after the product has been released.[37] Vulnerabilities may also be disclosed to the *public*, which may occur particularly when no vulnerability disclosure process exists and is often done in hopes that the entity that owns or manages the software will quickly remediate the flaw.[38]

As we describe in the following section, coordinated vulnerability disclosure therefore specifically addresses the "wicked" problems of external vulnerability discovery and disclosure — for which there are no right or perfect solutions, only better or worse solutions in a given context.[39] Indeed, facilitating coordinated vulnerability disclosure may bring with it the risk of perpetuating organizational reliance on systems marked by insecurity,[40] rather than expecting more secure systems up front. Enabling the good faith external disclosure of vulnerabilities is nonetheless one way to reduce the harm associated with the now routine exploitation of security flaws and serves as one method among many that Canada could use in the process of ensuring the improved security of the federal government's digital systems.

Defining Coordinated Vulnerability Disclosure



02

Defining Coordinated Vulnerability Disclosure

It is important to understand how vulnerability disclosure works in order to provide effective policy solutions in respect of this topic. In sum, security vulnerabilities in the context of computing are a set of **conditions** or **behaviours** that allow for the violation of an explicit or implicit security policy.[41] In other words, vulnerabilities are weaknesses that can be exploited, allowing attackers to perform unauthorized and/or undesirable actions. The weakness can be found in hardware or software code, "in an information system, system security procedures, internal controls, or implementation."[42]

This report focuses specifically on vulnerabilities found in computer code and systems. **Code vulnerabilities** involve the written code embedded in a product's software and/or firmware components embedded in hardware.[43] All computer code contains latent or undiscovered vulnerabilities. A vulnerability is often described as a "zero day" vulnerability as soon as it's first been discovered, but before a mitigation becomes available.[44] Sometimes a vulnerability will always remain, but often the risk can be eliminated or reduced.

System vulnerabilities involve the implementation or configuration of an information system, with a major source of vulnerabilities in this context involving the maintenance of up-to-date software or system configurations.[45] The Equifax incident, involving 19,000 Canadians,[46] is an excellent example of a company's failure to patch vulnerable systems, leading to a massive security breach.[47]

Malicious actors can develop software or code to **exploit** these vulnerabilities, using these weaknesses to "steal and extort money and data, disrupt processes, or spy on organisations and individuals."[48] However, organizations can consent to having their code or systems exploited in order to test the current status of their security measures and system configurations through network 'penetration' testing or 'red-team' work that mimics the activity of an organization's threat actors.[49]

Vulnerability discovery and disclosure can take many forms. As mentioned, vulnerability discovery and disclosure occur internally in the development process. Vulnerabilities can also be discovered externally from an entity not responsible for maintaining the code or system. Security researchers can intentionally set out to test systems for vulnerabilities or may stumble upon them in the course of their work or spare time. Someone who discovers a vulnerability, but takes no action, withholds that information; this is an instance of **non-disclosure**. For decades, security researchers have routinely disclosed vulnerability information **to the public** in order to push software vendors to improve their security, which can problematically enable attackers to use this information before the vulnerability has been patched or remediated.[50] They can also **sell the information on a potentially illicit market** or **directly to governments** (often called the "grey market").[51]

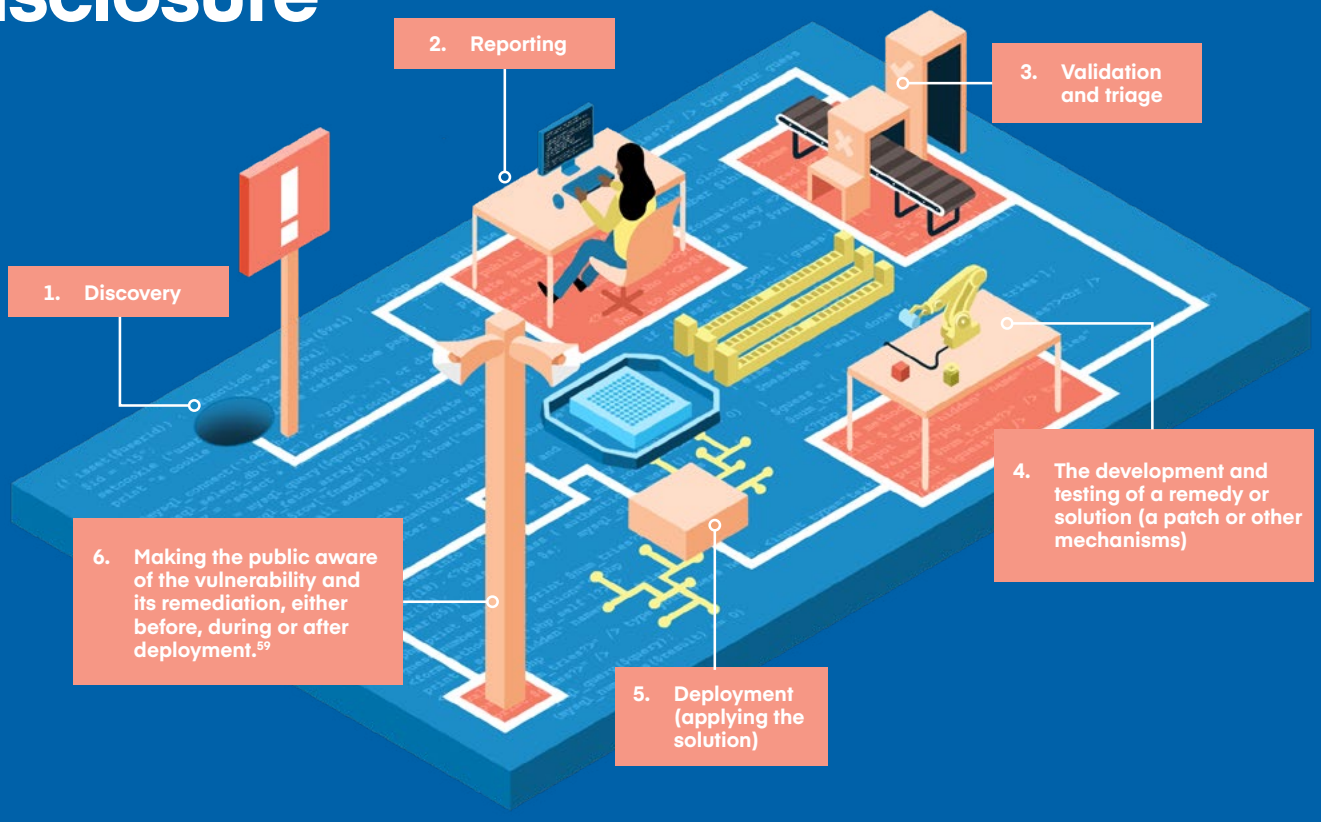
In many ways, **coordinated vulnerability disclosure stands in contrast to these vulnerability disclosure methods**. It involves **researchers contacting systems providers** in order for the vulnerability to be patched before the public learns about the vulnerability, and to reduce the risk of it being exploited.[52] Coordinated vulnerability disclosure is not an

event, but an ongoing process for reducing the risk associated with the existence of vulnerabilities that have been discovered, but not yet remediated or patched.[53] The principles of CVD include:

- Reducing harm;[54]
- Presuming benevolence;[55]
- Avoiding surprise;
- Incentivizing desired behaviour;
- Process improvement; and
- Addressing the "wicked problem" of vulnerability disclosure, which is a multifaceted problem for which there are no "right" answers, only "better" or "worse" solutions in a given context.[56]

There are various roles in coordinated vulnerability procedures.[57] There are the **finder/discoverers**, the **reporter** (which may overlap with the finder), **system providers** (software or hardware vendors, including institutions that develop products for their own use), the **deployer** (which must deploy a patch or take remediation action, and which may overlap with the system provider), and the **coordinator** that facilitates coordinated responses. Other stakeholders in the CVD process include users, integrators, cloud and application service providers, IoT and mobile vendors, and governments.[58]

Phases of Vulnerability Disclosure



There is the possibility for significant variation in the coordinated vulnerability disclosure process.[60] There can be variation in the elements of the disclosure policy, coordination across multiple parties (e.g., the system providers, vulnerability finders or discoverers, vendors, supply chains or service providers affected, etc.). There also can be variation in the pacing and synchronization of CVD frameworks. The coordination aspects of CVD can specifically vary in terms of:

- Requirements to disclose to the software and hardware vendors, or to the organizations deploying their services;
- Whether the CVD procedure is deployed through legal regulation, organizational policies, guidelines, or performance indicators;
- Whether the CVD procedure is run in-house by an organization or whether they outsource that to a third party; and
- Whether people are credited, recognized, or remunerated for submissions deemed valid or worthy of remediating.[61]

As mentioned, there are invariably some risks associated with the implementation of CVD procedures, and the possibility for things to go wrong. Risks associated with the facilitation of CVD include the following:

- There is no contact information available for system providers;
- Disclosers can stop responding;
- Information can be leaked;
- People may discover vulnerabilities and not necessarily disclose it;
- A vulnerability discoverer may actively exploit the vulnerability;
- Relationships can go awry; and
- Vulnerability disclosure policies or procedures may exist for hype, marketing, or to limit the unwanted attention that comes from full or partial public disclosure of vulnerabilities.[62]

If a CVD procedure exists but is inadequate, it may be counterproductive. Organizations that set their program scope too wide, or that have less mature security practices, may struggle to handle external vulnerability reports, in turn fostering frustration among finders who expect clear communication and quick resolution from the organization.[63] Disclosers may also turn to full disclosure if organizational response or patching takes too long.[64]

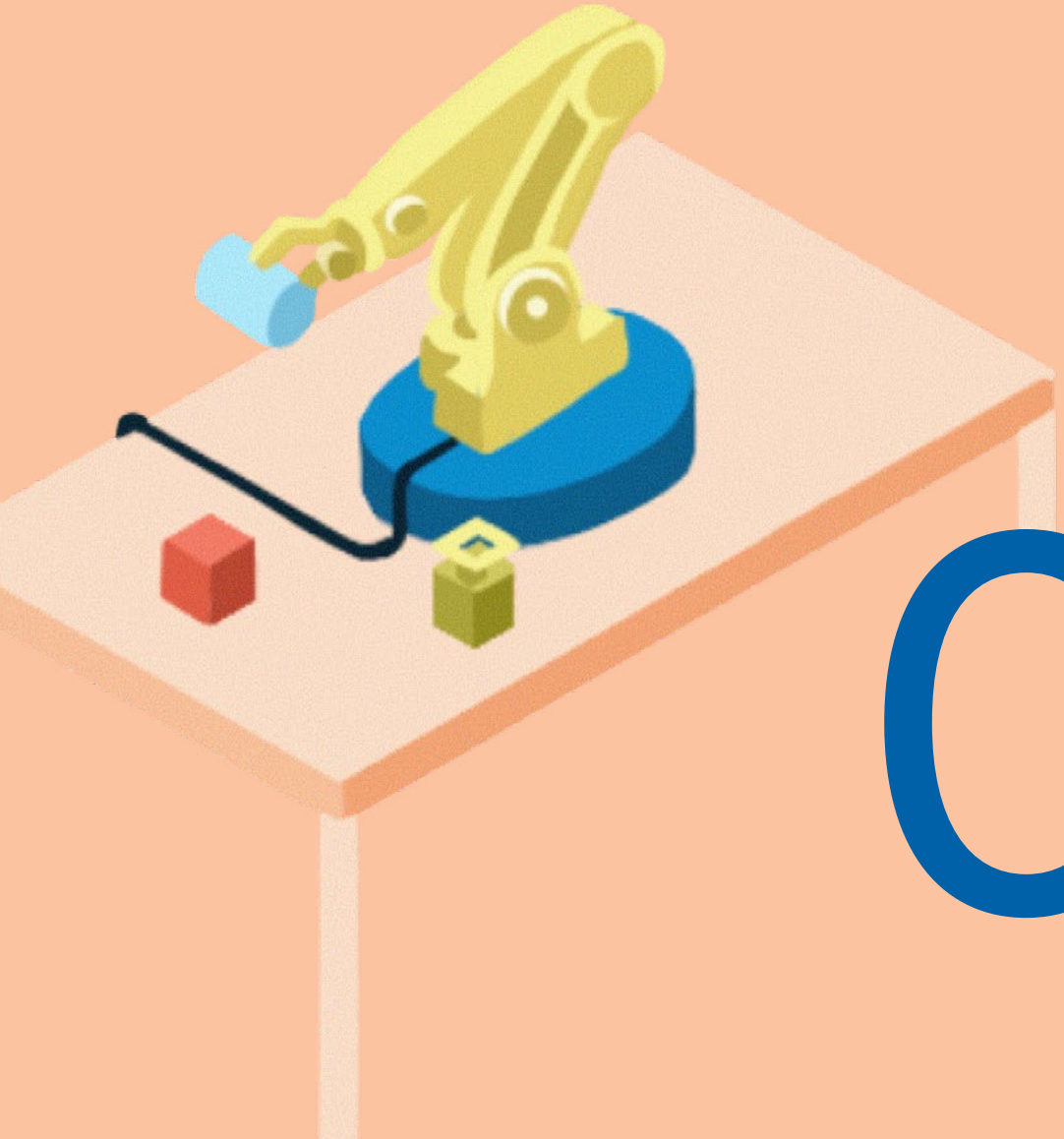
However, there are numerous benefits associated with the implementation of CVD procedures and policies. It is worth remembering that software and hardware will always contain flaws, whether obvious or latent in nature.[65] Facilitating CVD includes the following benefits, among others:

- Facilitating coordinated vulnerability disclosure can **enable good faith security research** and the **disclosure** of flaws found on an organization's systems.[66]
- CVD procedures facilitate the disclosure of vulnerabilities that could otherwise have been discovered and **exploited** by attackers.[67]
- In general, **external** security researchers can find things that **internal** security teams **do not discover in the software development process**[68] because they are often "exposed to a wider variety of programs and vulnerabilities through the different types of employments, exercises, and communities they are involved in and the more diverse bug reports they read," providing them with an important advantage over internal security testers.[69]
- CVD can help to provide **some legal clarification** for good faith security researchers, who can avoid legal liability by adhering to the CVD procedures, and otherwise may face significant legal repercussions for their activity.[70]
- Enabling vulnerability disclosure can also build **goodwill** and **trust** with security researchers.[71]
- Clearly written CVD procedures can provide **clear expectations** for disclosers, thereby preventing situations where disclosers demand remuneration or recognition for their disclosure.[72]
- CVD procedures can provide clarity regarding **who is responsible for receiving security flaws** in the case of governments using third-party software and hardware service providers.
- Vulnerability disclosure pipelines provide **clearer** and **more transparent vulnerability report triage** processes.

From the vantage point of the Canadian government, perhaps the most significant benefit of implementing CVD procedures is that doing so can result in patched vulnerabilities; and better ensure that the vulnerability will not be used for offensive or exploitative purposes in ways that harm the government's systems, infrastructure, and the people that they serve.

POLICY CASE STUDIES:

The Netherlands and the U.S.



03

The Netherlands and the U.S.

In the course of conducting analyses on CVD policies around the globe, certain aspects of the policy developments in two countries particularly stood out as worth emulating in Canada: the Netherlands and the US. These countries' approaches are distinct for the way they implemented vulnerability procedures involving the federal government relatively early on (in the 2010s) and have provided clarification regarding the legal treatment of vulnerability disclosure through various policy instruments.

The Netherlands: The NCSC, Guidelines, and Legal Protection for Public Interest Security Research

The Netherlands' approach to coordinated vulnerability disclosure encourages, but does not require, organizations to have CVD procedures. It can be seen as providing legal protection, to some extent and in light of certain considerations, for security research activity (including vulnerability discovery and disclosure) that occurs in the public interest.

In the Dutch context, the federal government's computer incident response team — the National Cybersecurity Centre (NCSC) — acts as a model to other organizations in the Netherlands for best practices regarding the handling of vulnerability disclosure as stipulated in its guidelines on CVD.[73] The NCSC provides publicly available and detailed guidelines for stakeholders in the coordinated vulnerability disclosure process.[74]

The NCSC was established in 2002.[75] It is the government organization charged with ensuring the security of computer systems and infrastructure in the Netherlands.[76] The NCSC sits within the Ministry of Justice and Security, which has the mandate to protect the freedom and safety of people in the Netherlands through its policies and regulations.[77]

The NCSC states that it is a best practice — but not legally required — for public and private organizations to implement their own CVD procedures.[78] This stands in contrast to the US approach described in the next section, where all federal agencies are now required to facilitate CVD through vulnerability disclosure policies.

The NCSC's CVD procedure outlined in its guideline is succinct yet informative, and not without its own gaps. People who discover a vulnerability in a government system or "a system with a vital function" are instructed to first approach the "owner" or "manager" of the system.[79] This is because organizations that manage, own or supply systems are expected to handle the vulnerability disclosure process that directly concerns them.[80] The NCSC encourages organizations to have their own CVD policies, and it provides resources to these organizations, including templates for such policies. However, one noteworthy downside to the Dutch approach to CVD is that its guidelines do not clarify what is required for disclosure affecting multiple parties, such as software vendors and the government.

In any case, the NCSC acts as an intermediary between the discloser and organizations that fail to respond or do not respond appropriately. The NCSC also provides a CVD report form and email contact information, as well as the

NCSC's PGP key, to better ensure the safety of the information sent to the NCSC.[81] Disclosers are instructed to submit the report as soon as possible after discovering the vulnerability. They are also encouraged to avoid sharing the vulnerability information until they have heard from the NCSC or until it has been resolved. Disclosers are not to take any action other than that which is needed to demonstrate that the problem exists.

The NCSC also performs the important role of delineating the responsibilities of security researchers. It requires that researchers avoid the following actions in the course of their testing activity:

- Installing malware;
- Copying, changing or deleting data in a system (an alternative is creating a directory listing of a system);
- Making changes to the system;
- Repeatedly gaining access to the system or sharing access with others;
- Using brute force to gain access to a system; and
- Using social engineering, or denial of service attacks or testing.[82]

The NCSC's policy also provides their own promises to the security researcher.[83] The NCSC will not share the personal details of the discloser to third parties without the discloser's consent, unless obligated to do so by law. The NCSC provides detailed information about response times post-report submission, including a promise to try to resolve the security issue within 60 days. They also commit to deciding along with the discloser whether and how details of the vulnerability will be published. It also provides rewards for those who disclose, dependent on the severity of the vulnerability and quality of the report, ranging from a T-shirt or gift voucher to a maximum of €300.

In its own CVD procedure, the NCSC states that it will have "no reason to take legal action" as a result of a vulnerability report, so long as it's been submitted in accordance with the requirements laid out.[84] Prosecutors and police in the Netherlands will take into consideration whether a CVD policy exists, and whether the security researcher adhered to it, when deciding to investigate or lay charges.[85]

The Dutch approach to CVD is also significant for the way it requires analysis, prior to prosecution, of whether the security research activity was done in the public interest, potentially providing some legal protection to disclosers in the context of coordinated vulnerability disclosure. A policy letter on CVD from the Dutch public prosecutor updated in December 2020 provides legal clarification that other jurisdictions may wish to learn from. At the outset, the letter seeks to "stimulate CVD" and encourage third parties to prevent careless or malicious behaviour on the internet.[86] The letter states that when an "ethical hacker" finds a vulnerability in an IT system and reports it to the relevant organization in a certain fashion, then "in principle, no criminal investigation is instituted," as such behaviour constitutes coordinated vulnerability disclosure.[87]

The organization and discloser may, in the context of CVD, agree that no criminal report will be filed and/or that no civil action will be taken.[88]

In the Netherlands, prosecutors (and not the police) lay criminal charges. When assessing if they are dealing with coordinated vulnerability disclosure, prosecutors must assess these three factors to determine whether the activity was done in the public interest:

- **Motives:** Was the action taken in the context of a substantial social interest?
- **Proportionality:** Was the act proportionate (did the person not go beyond what was necessary) to achieve the goal?
- **The principle of subsidiarity:** Was disclosure made to the appropriate entity (did they exhaust their remedies before disclosing further)?[89]

The public prosecutor's letter states that it has developed these three factors in accordance with jurisprudence, and in light of the rights to freedom of expression for individuals and journalists provided by article 10 of the *European Convention on Human Rights*. The letter states that a lack of a CVD policy is not immediate reason to classify an ethical hacker as a suspect. Instead, a prosecutor, ideally specialized in cybercrime, should be involved in a factual (not necessarily criminal) investigation as early as possible, in order to determine whether coordinated vulnerability disclosure has occurred or to proceed with a criminal investigation. The policy also describes the possibility of dismissing charges against an ethical hacker if CVD has occurred, even after commencement of a criminal investigation.

A noteworthy instance of the policy letter's application involved the Twitter account for former president Donald Trump. In late 2020, Dutch security researcher Victor Gevers discovered that then-President Trump was using the password "MAGA2020!" for his Twitter account.[90] Gevers had been conducting semi-regular testing regarding the security of Twitter accounts for high-profile US election candidates when he discovered that the president used this relatively easy-to-guess password. He did not change any of the account's settings, nor did he post any tweets from the account. He attempted to notify Trump's campaign team about this security error, informing them that other safeguards were lacking, including two-factor authentication, before going to the press. After investigating the situation, the Dutch public prosecutor concluded that Gevers' intention and behaviour under the circumstances fell under a criminal exemption for public interest ("ethical") security research and vulnerability disclosure.[91]

Since 2013, relevant case law in the Netherlands has demonstrated that the criteria set out in the Dutch AG's policy letter are also considered in court when an organization does not have a CVD policy[92] (as appeared to be the case involving Trump's Twitter account). The Dutch model has provided much needed legal certainty for the stakeholders involved in vulnerability disclosure processes.[93] The Dutch approach serves as one model for other jurisdictions to follow when it comes to CVD policies and guidelines.

The United States: CISA, Regulation, and Minimized Legal Risk Centred on Authorization

The approach in the US requires federal agencies to facilitate coordinated vulnerability disclosure and provides some minimization of the legal risks posed to security researchers who disclose in adherence to organization-run CVD procedures.

As of March 1, 2021, all US federal agencies are required to have developed, published, and implemented vulnerability disclosure policies, with exceptions for "national security systems" and "certain systems operated by the Department of Defense or the Intelligence Community."[94] These requirements are set out in the *Binding Operational Directive 20-01* by the US Department of Homeland Security through the Cybersecurity and Infrastructure Security Agency (CISA). CISA was created in 2018 and, in short, provides support, expertise, and resources to the federal government to defend against cyberattacks.[95]

The *Binding Operational Directive* provides detailed CVD requirements for federal agencies, specifying and providing:

- The need to develop and publish a vulnerability disclosure policy that begins smaller in scope and eventually expands over time, stipulating:
    - What is in scope;
    - How to submit vulnerability reports;
    - The agency's commitment not to recommend or pursue legal action regarding good faith efforts to follow the policy;
    - What the discloser can expect in terms of the communication and remediation process;
    - The possibility for disclosure from anonymous sources, regardless of citizenship; and
    - A prohibition against disclosing vulnerabilities to the Vulnerabilities Equities Process (which is described in greater detail below).
- Agencies' reporting requirements and disclosure of CVD metrics to CISA;
- The role of CISA in overseeing compliance with the Directive; and
- An implementation guide (including a checklist, vulnerability disclosure program template, FAQ and other information).

Whereas the NCSC states that it can become an intermediary when an organization fails to respond to vulnerability disclosure or does not respond appropriately, **CISA may get involved in the disclosure process for various other additional reasons.** Federal agencies are required to immediately report to CISA when they receive newly discovered vulnerability information that involves commercial software or services that "affect or are likely to affect other parties in government or industry."[96] They are also expected to report to CISA if the agency "believes CISA can assist with or should know about, particularly as it relates to outside organization," as well as in "[a]ny other situation where it is deemed helpful or necessary to involve CISA."[97] On top of being a last resort for researchers who cannot reach a disclosure contact or where there has been no response,[98] it also appears that disclosures involving industrial control systems and medical devices are best disclosed to CISA.[99]

Other US federal agencies also have their own approaches to CVD that preceded the *Binding Operational Directive*. The Department of Defense (DoD) has facilitated CVD since 2016, enabling external security researchers to disclose vulnerabilities found in infrastructure owned, for example, by the Pentagon[100] and the Army.[101] Background checks and citizenship verification were initially needed for the DoD's invite-only, time-bound vulnerability disclosure procedures involving remuneration.[102] In May 2021, the DoD expanded the scope of its CVD procedures from public-facing websites and applications to now include all "publicly-accessible networks, frequency-based communication, Internet of Things, industrial control systems, and more."[103] The General Services Administration's Technology Transformation Services (TTS) has also facilitated CVD involving its civilian systems since 2016.[104]

In terms of limitations on security research activity, CISA's vulnerability disclosure template and the disclosure approaches of these other federal bodies (DoD and TTS) all generally prohibit security testing methods such as denial of service tests, physical testing, and social engineering, among others.

Without being exhaustive, there are **numerous other pieces of legislation regarding CVD that have been enacted** in the US. Since December 2018, the *SECURE Technology Act* has required the Secretary of Homeland Security to establish a vulnerability disclosure policy.[105] The *Hack Your State Department Act* has also required the Department of State to establish a vulnerability disclosure process since January 2019.[106] As of December 2020, the *IoT Cybersecurity Improvement Act* (ICIA) has required the National Institute of Standards and Technology (NIST) to publish guidelines for vulnerability disclosure processes related to government information systems, including IoT devices.[107] The ICIA also requires the Director of Management and Budget (in consultation with the Secretary of Homeland Security) to develop and oversee the implementation of coordinated disclosure policies for information systems as well as IoT devices. This Director is also required by the ICIA to disseminate information about security vulnerabilities once they have been resolved or remediated.

In the wake of the SolarWinds, Microsoft Exchange, and Colonial Pipeline incidents, President Joe Biden issued an executive order in May 2021 aiming to improve the cybersecurity and protection for the federal government's networks.[108] Among the many solutions identified to improve the security of the federal government's software supply chain, the executive order seeks to establish baseline security standards for the development of software sold to the government, creating an "energy star" type of label to allow the government and public to determine whether the software was developed securely.[109] It also requires standardization of the "federal government's playbook" for responding to security vulnerabilities and incidents involving a wide array of federal agencies.[110]

Though the impact of this executive order, if any, is not yet clear, many of these policy changes have brought with them incremental legal clarification as to how security research will be treated by the law — and in a way that still explicitly presumes the centrality of prohibitions against unauthorized computer access and use. To provide context, it is widely known to security researchers that the *US Computer Fraud and Abuse Act* is a broadly

scoped federal law that has significantly expanded since 1984 to prohibit an expansive range of activity in respect of computers, including their access and use.[111] The US *Digital Millennium Copyright Act* (DMCA) also prohibits the circumvention of technological measures (e.g., encryption) that control access to copyrighted works.[112]

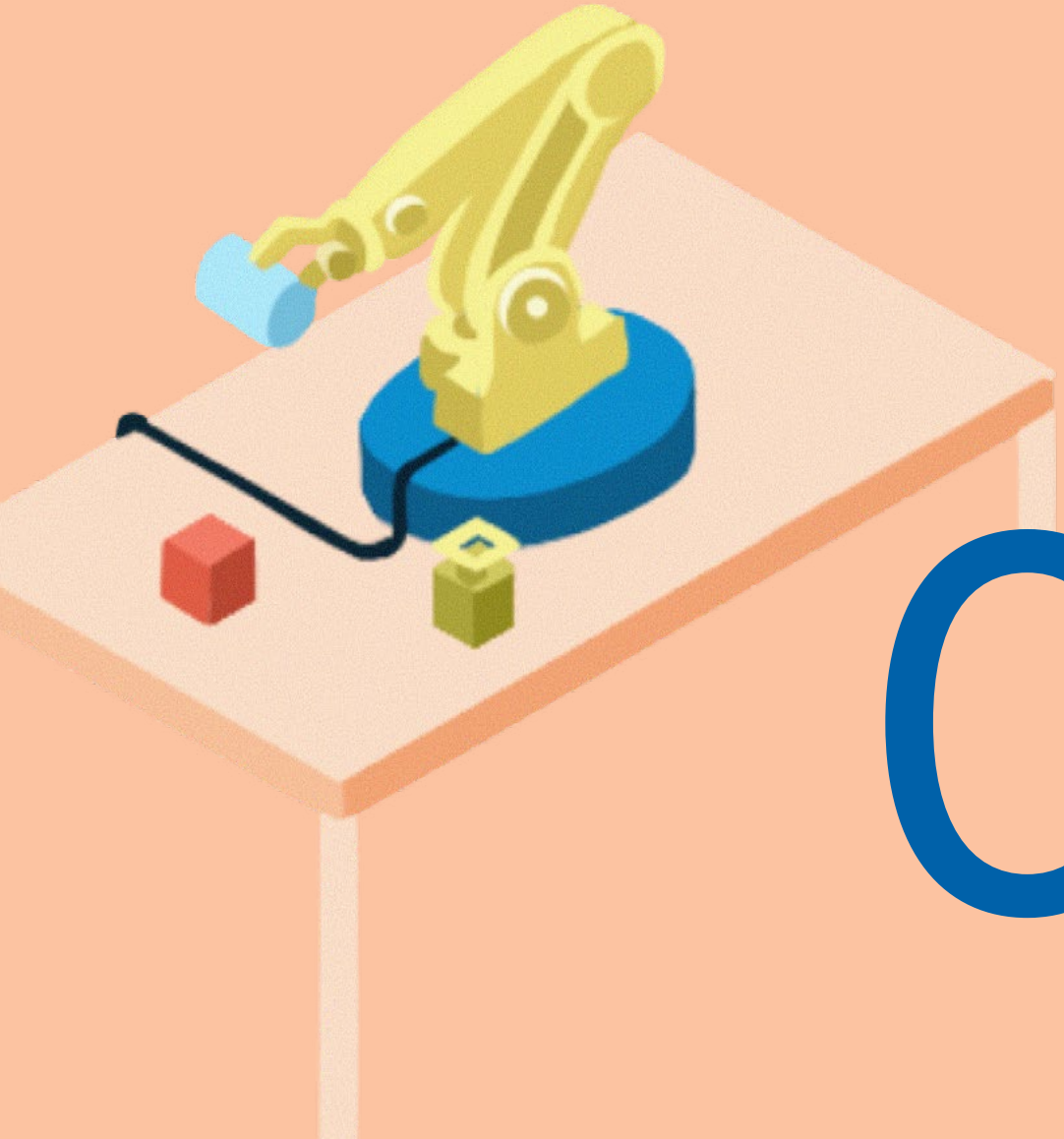
In 2017, the US Department of Justice stated that organizations that have implemented CVD policies that "clearly describe authorized vulnerability disclosure and discovery conduct" would substantially reduce "the likelihood that such described activities will result in a civil or criminal violation of law under the *Computer Fraud and Abuse Act*" (the CFAA).[113] A Supreme Court decision from June 2021 provides increased, yet limited, clarity regarding the legal treatment of computer security research in the US context.[114] And since at least 2018, it has been possible to engage in good faith security research involving the circumvention of technological measures that control access to copyrighted works in certain circumstances, so long as the activity does not contravene the CFAA.[115]

However, whether computer access and/or use has been "authorized" still remains central to the US policy approach to security research and vulnerability disclosure. For example, the *SECURE Technology Act* and *Hack Your State Department Act* both define vulnerability disclosure procedures involving remuneration ("bug bounty programs") as circumstances in which "individuals, organizations, and companies are *temporarily authorized* to identify and report vulnerabilities of appropriate information systems" of the relevant federal department.[116] CISA's *Binding Operational Directive* seeks to commit federal agencies to "authorize good faith security research" while still requiring organizations to delineate what constitutes authorized or unauthorized security testing.[117]

These policy developments suggest that any legal protections in the US afforded to security researchers in the context of CVD are still very much centred on the question of what constitutes authorized activity for the federal government. In some ways, this policy approach stands in contrast to that of the Netherlands, which requires consideration of specific factors that prioritize the circumstances and motivation surrounding security research activity. The Dutch model, unlike the US approach, requires examination of whether minimum actions were taken to demonstrate the existence of the vulnerability, as well as exhaustion of disclosure remedies prior to the prosecution of vulnerability disclosure — not only in the context of CVD, but also in the context of security research more generally.

CANADIAN CONTEXT:

Vulnerability Disclosure for Federal Systems



04

Vulnerability Disclosure for Federal Systems

The Government of Canada has not yet implemented a policy framework for facilitating coordinated vulnerability disclosure. There may also be legal risks for vulnerability discovery and disclosure under criminal law, as well as copyright law in certain circumstances — in many cases, without protection from legislation for whistleblowers.

The current approach may dissuade security researchers from disclosing vulnerabilities found in the federal government's systems. The Canadian Centre for Cyber Security facilitates the disclosure of "cyber incidents," defined in such a way that does not readily include vulnerabilities that have not yet been used for exploitation. Once vulnerabilities are disclosed, an opaque and discretionary remediation process is currently in use that provides inadequate transparency as to the fallout of disclosure.

Legal Risks for Vulnerability Discovery and Disclosure

There are numerous actions associated with security research that may invoke the application of federal laws. See, for example:[118]

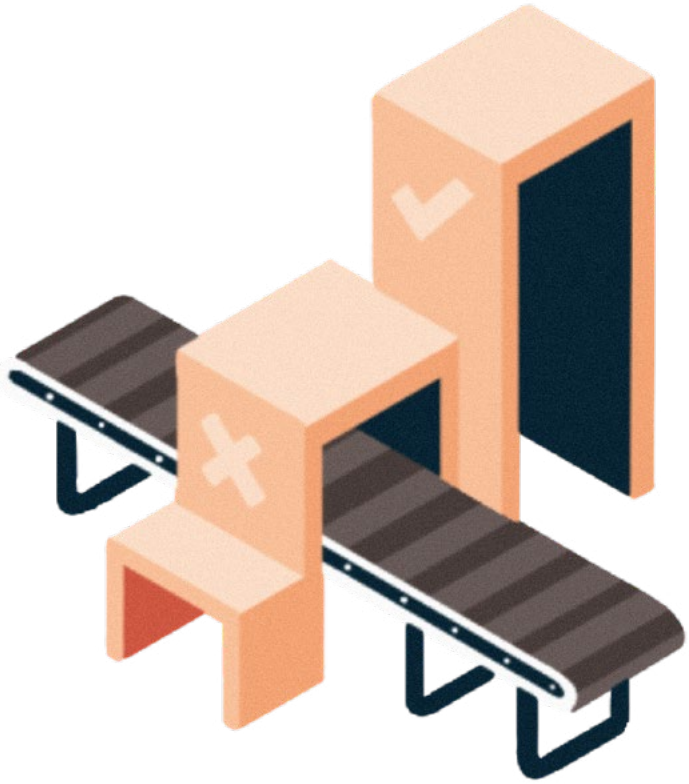
Security research activity	Potential applicable law and provision	Brief summary of provision
Hacking (i.e., unauthorized access), including unsolicited security or penetration testing	Section 342.1 of the *Criminal Code*	Unauthorized use of computer, computer service, or computer password
	Section 380(1) of the *Criminal Code*	Fraud
	Section 430 of the *Criminal Code*	Mischief, or wilfully destroying or damaging property, including overloading computer systems, "causing chaos"[119]
	Section 184 of the *Criminal Code*	Wilful interception of private communications
Obtaining, storing or retrieving computer data without permission	Section 342.1 of the *Criminal Code*	Unauthorized use of computer data, requiring intent to commit mischief under s. 430 of the *Criminal Code*
Impersonation (a technique that is commonly referred to as "social engineering" in the computer security industry[120])	Section 402.2 of the *Criminal Code*	Identity theft or identity fraud
Possessing, importing or using devices made for hacking	Sections 342.2 of the *Criminal Code*	Possession or use of hardware, software or other tools used to commit hacking (section 342.1 of the *Criminal Code*) or mischief (section 430 of the *Criminal Code*)
Circumventing security measures, including decryption	Section 41.1(1) of the *Copyright Act*	Circumvention of a "technological protection measure" for any technology, device or component that controls access to a copyrighted work or sound recording

When it comes to copyright law, good faith security researchers may benefit from the exemptions that exist regarding the prohibition on circumventing security measures that control access to copyrighted works. Security research may be exempted from such a prohibition when it is done under certain circumstances, such as for the purposes of encryption research,[121] or for "assessing the vulnerability of the computer, system or network or correcting any security flaws."[122]

On the other hand, a security researcher wishing to receive whistleblower protection in the disclosure process may not necessarily be protected by existing laws. Work by Florian Martin-Bariteau and Véronique Newman has uncovered that there are over 40 pieces of legislation across Canada that ostensibly protect whistleblowers from reprisals, albeit generally in the employment context.[123] For example, the federal *Public Servants Disclosure Protection Act* only applies to public servants who are employed in the federal public sector.[124] Similarly, Canada's federal private sector data protection law prohibits any kind of reprisal against an employee or independent contractor who discloses, in good faith and on the basis of reasonable belief, a violation of that law.[125]

While a detailed analysis of whistleblower protection law is out of scope for this report, such existing laws in Canada generally only protect security researchers if:

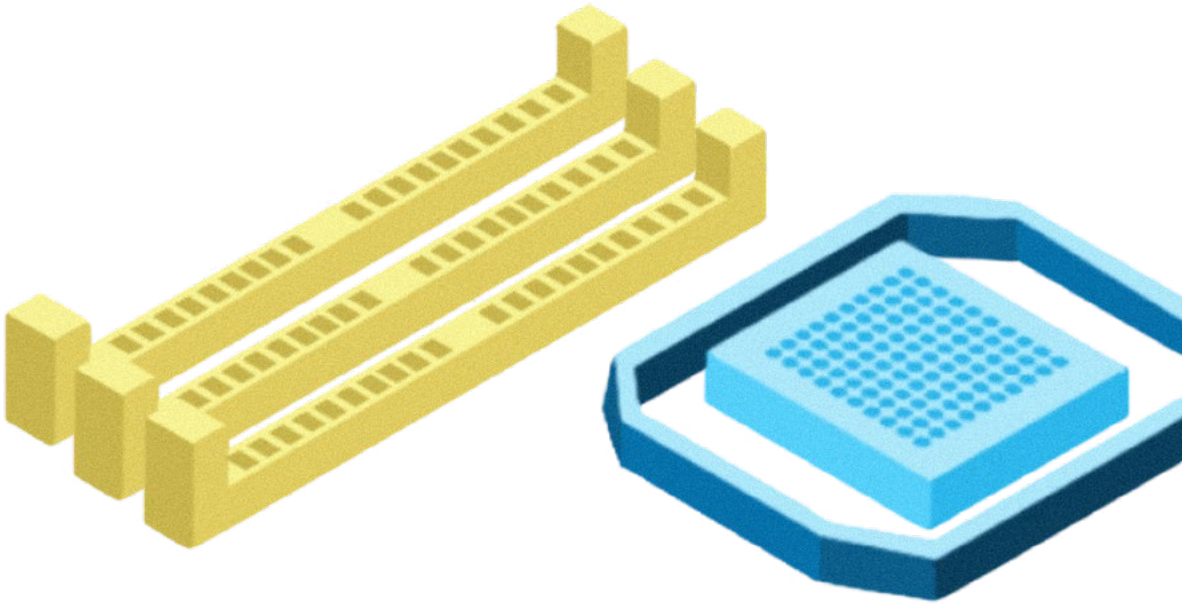
1. The person is an employee or contractor of the organization;
2. They disclose an issue that would violate a law; and
3. The disclosure is made to a higher-level officer or a specific governmental agency.[126]



Applying this to security vulnerabilities, disclosure may easily be made to a higher-level officer or specific governmental agency, dependent on the availability of instructions to do so, as well as contact information for these entities. However, many external security researchers are likely to operate outside of an organization, and would often not be considered employees or contractors. The disclosure of a security vulnerability may also not necessarily involve the violation of a law, since such information generally involves the disclosure of conditions in which exploitation could occur. Additionally, the exploitation of a security flaw would presumably often involve the violation of a law, but this is not necessarily the case in all circumstances.

In rare cases, a person protected under whistleblower protection law (such as an employee or contractor) may disclose to the general public vulnerability information that involves an immediate risk to public health, safety, or the environment.[127] Such disclosure is generally only protected when time constraints prevent the use of regular internal mechanisms. For example, someone who is eligible to receive whistleblower protection would potentially be able to publicly disclose information demonstrating that an exploitation involving critical infrastructure (such as an oil pipeline) could occur. However, the discloser would need to consider whether the benefits of disclosing such information would outweigh its harms. In terms of legal protection, situations that meet these circumstances are likely to be extremely rare.

In sum, this brief legal overview provides one indication that there currently exists no policy framework in Canada enabling good faith security research, including in the context of vulnerability discovery and disclosure. As such, the laws in Canada that currently apply to computer security research activity could serve as one reason to discourage and dissuade security researchers from discovering and disclosing vulnerabilities found, for example, in the federal government's computer systems.



The Government of Canada's Approach to Coordinated Vulnerability Disclosure

We uncovered little evidence of a straightforward or transparent disclosure and remediation path for someone who discovers security vulnerabilities in the Government of Canada's digital systems. For instance, there is only ad hoc use of a coordinated vulnerability disclosure policy for COVID Alert, Canada's COVID-19 exposure notification app.[128]

Our findings suggest that the Canadian Centre for Cyber Security (CCCS) is the only federal agency that readily addresses the disclosure of security-related information. The CCCS currently acts as Canada's computer security incident response team and was established within the Communications Security Establishment (CSE) in October 2018.[129] The CCCS aims to provide a "single, unified team of government cyber security technical experts that will be the definitive source of unique technical advice, guidance, services, messaging, and support on cyber security operational matters for government, critical infrastructure owners and operations, the private sector, and the Canadian public."[130]

Disclosure of a vulnerability may generally trigger the application of Canada's *Cyber Security Event Management Plan* (CSEMP), which has provided a detailed system since 2018 for responding to and reporting on what it calls "cyber security events",[131] including the issuance of advisories.[132] However, the CCCS facilitates the disclosure of "cyber incidents," which it defines as "[a]ny unauthorized attempt, whether successful or not, to gain access to, modify, destroy, delete, or render unavailable any computer network or system resource."[133]

Defining the term in this way assumes that it is clear what constitutes an "unauthorized" attempt to access a computer system — despite the fact that, as described previously, a good faith security researcher may engage in activity that unwittingly meets this definition of unauthorized computer access or use, potentially attracting liability and possibly severe punishment pursuant to various laws, due to lack of a policy framework on this topic in Canada.

The CCCS also tells those who visit its website: "If you believe a cyber incident is an imminent threat to life or of a criminal nature, please contact your local law enforcement agency (911) or the RCMP."[134] The text on the CCCS website may be imbued with the assumption that "cyber incidents" could easily constitute criminal activity. However, the existence of a security vulnerability does not necessarily equate to unauthorized attempts to modify, destroy, or render unavailable computer networks or systems. Instead, the discovery of a vulnerability is the discovery of a condition which *may* give rise to such activity.

The CCCS therefore does not readily facilitate the disclosure of system or code vulnerabilities; in fact, on its face, it primarily facilitates the disclosure of wrongdoing or potential wrongdoing. This stands in contrast to the Netherlands and the US, both of which explicitly seek to work with good faith security researchers in order to discover and repair vulnerabilities. It also specifically stands in contrast to the Dutch model, which has carved out a legal exemption from criminal liability for acts of vulnerability disclosure that are determined to occur in the public interest. By comparison, the cumulative effect of the CCCS's terminology may dissuade a person

from disclosing a security vulnerability found in the federal government's systems, for fear of having engaged in wrongdoing and potentially criminal activity.

On May 12, 2021, the CCCS updated its "cyber incidents" webpage in a largely cosmetic fashion by providing a "cyber incident" report form. The previous page was largely descriptive in nature, describing the relationship between cyber incidents and cybercrime, spam, phishing, scams, fraud, and child exploitation.[135] It enabled people to report "an urgent cyber incident" to the CCCS, directing them to a generic, catch-all contact page.[136] As of May 12, 2021, the "Report a cyber incident" webpage provides discrete reporting mechanisms on behalf of an IT security practitioner, a critical infrastructure organization, and a government department or agency.[137] The CCCS's page now provides dedicated contact information for information disclosure in the cybersecurity context and, interestingly, allows people who fill out its form to check off "Vulnerability identified", which they define as "when trusted parties identify flaws that could be exploited by attackers, which have not yet been leveraged" (see **Figure 2**). Nonetheless, nothing else uncovered in our examination of the form rectifies any of the longer-standing issues described earlier pertaining to under-inclusiveness when it comes to use of the term "cyber incident" leading up to that point in the reporting process.

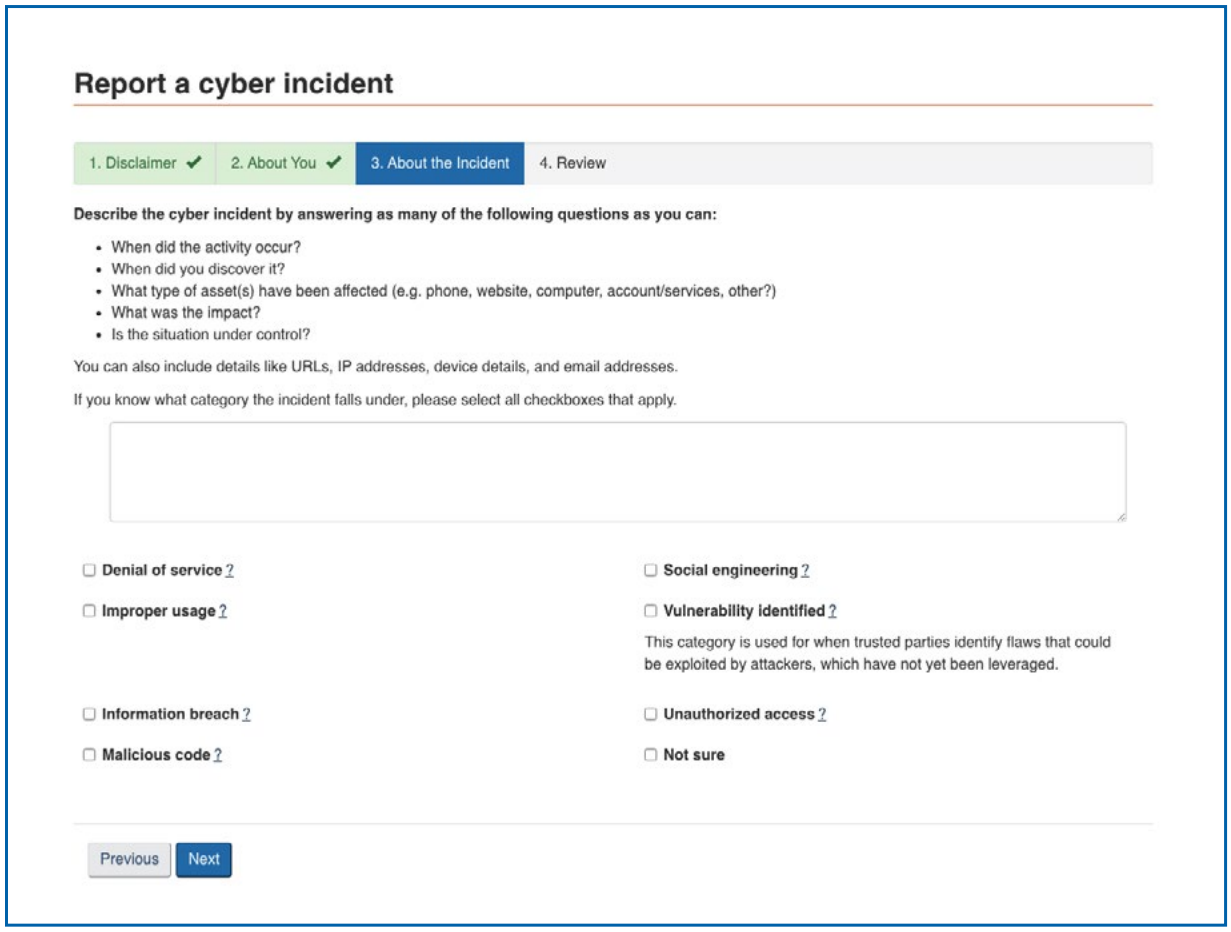


Figure 2: The CCCS's Report a cyber incident form as of June 2021

A Closer Look: Coordinated Vulnerability Disclosure and the Department of National Defence

The networks of Canada's Department of National Defence/Canadian Armed Forces (DND/CAF) are defended by an internal defence team that works in partnership with the CSE, the Department of Public Safety, Shared Services Canada (SSC), and the CCCS. The mandate of this collaboration is to develop policy for active cyber operations, to "establish and seek to preserve our freedom to maneuver within cyberspace and provide the Government of Canada with flexible cyber response options."[138] The development of these response solutions to evolving threats are conducted by the Cyber Security Engineering Program, with integrated IT solutions to joint operations provided by the Command, Control, Communications, Computer and Intelligence, Surveillance, and Reconnaissance program.[139]

Shared Services Canada provides and consolidates information technology services across federal government departments. The cyber and IT security mandate of the SSC involves the implementation of "firewall, anti-virus, and anti-malware, secure remote access, and vulnerability management to [GC] systems and services."[140] DND/CAF released a report in January 2021, warning that the Canadian Armed Forces' operations and security were at risk, with several concerns raised by defence and military officials relating to major delays, legacy technology, procurement challenges, and significant costs spent by DND/CAF on IT services and support annually.[141] In April 2021, SSC signed a multi-year agreement with BlackBerry to use its BlackBerry Spark and BlackBerry SecuSUITE cybersecurity products.[142]

Challenges for implementing a framework for CVD in Canada were raised in a 2019 Standing Committee on Public Safety and National Security meeting[143] — in particular, the need for security researchers to have a legitimate process to disclose vulnerabilities with proper legal authorities and security checks. Speaking as an individual, Steve Waterhouse, former Information Systems Security Officer for the Department of National Defence, pointed out that "the contracts that Public Services and Procurement Canada enter into have to be properly done. They have to contain a section on security. A security check has to be done. If an individual, or group of individuals, works on the government's information systems, they have to have received the appropriate legal authorization to be able to do the work."[144] As outlined below, clarity is important in the framing of such CVD eligibility requirements, as well as expectations around acceptable activity in the disclosure process.

Discretionary and Potentially Opaque Treatment of Vulnerabilities Once Disclosed

Perhaps one of the most troubling aspects — from the little that is publicly known — regarding the Government of Canada's vulnerability handling procedures concerns the withholding of vulnerability information for offensive and defensive purposes that may achieve certain military and/or intelligence goals. As it stands, the Communications Security Establishment has the discretion to withhold vulnerability information it receives from not only the public, but also potentially from other federal agencies and departments.

As mentioned, the *Cyber Security Event Management Plan* appears to provide a fairly robust system for the federal government's response to "cyber security events", which also includes the disclosure of vulnerabilities. While a detailed analysis of this framework is out of scope for this report, the CSEMP explicitly accounts for the fact that the Canadian government may receive "threat and intelligence," as well as "incident" reports, from "external sources" during the detection and assessment phase when it comes to Canada's awareness of security events.[145] The CCCS, among many of the solutions identified in the course of a "cyber security event", can coordinate messaging to "implicated stakeholders as required throughout the cyber security event management process" (see **Figure 3**), such as through the dissemination, for example, of advisories and alerts.

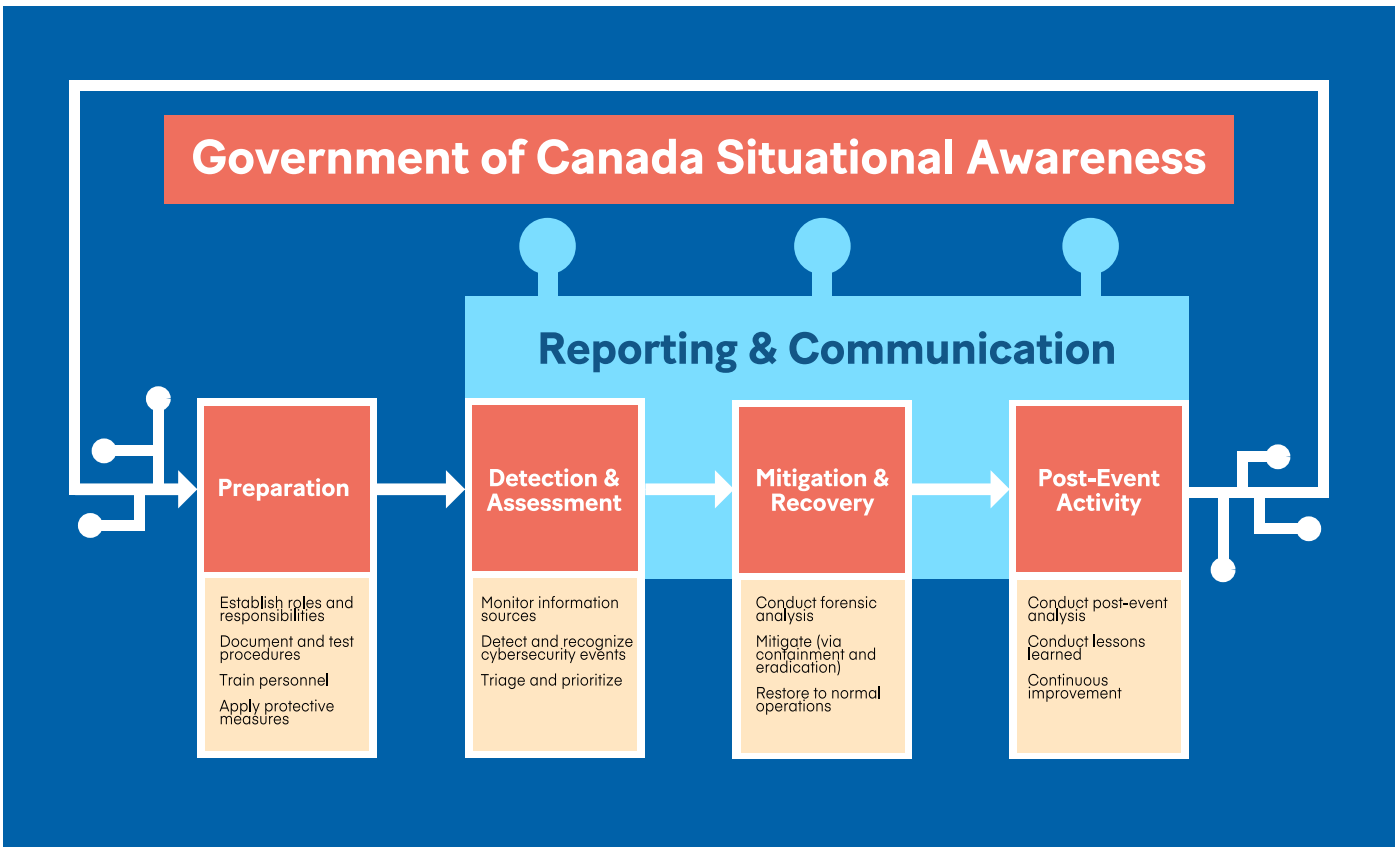


Figure 3: The CSEMP Cyber Security Event Management Process

For example, it seems plausible that the CCCS's alert first issued in March 2021 regarding the prominent security exploits associated with unpatched Microsoft Exchange servers[146] was disseminated pursuant to the CSEMP. We applaud the CCCS's decision to quickly release information on these known vulnerabilities and exploits, the publication of which generally serves the CSEMP's aim to adequately manage "cyber security events," such as vulnerability disclosure, in order to protect federal computer systems and the people they serve in Canada.

On the other hand, the CSE also has in place a vulnerability "equities management" framework.[147] This opaque term and procedure initially emerged in 2008 in the US context under President Bush, and was later developed during the Obama administration.[148] In layperson's terms, "equities management" refers to the process by which a government decides whether to disclose software vulnerabilities in order to mitigate the risks they pose or to "withhold [such] information ... for purposes including law enforcement, intelligence gathering, and 'offensive' exploitation."[149] The US Vulnerabilities Equities Process (VEP) charter was fully released in November 2017; the UK released details of its own equities process in 2018;[150] and Canada released details for its equities management process in March 2019.[151]

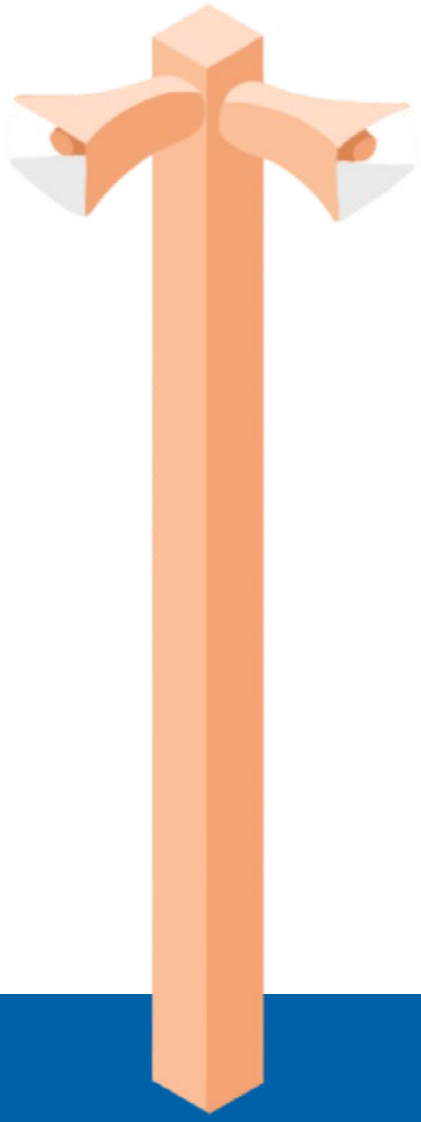
Government handling of security vulnerabilities has significant and potentially far-reaching consequences. For example, consider the US National Security Agency's (NSA) decision not to disclose a vulnerability in the Windows operating system and the aftermath that ensued.Rather than inform Microsoft of the existence of this vulnerability for risk mitigation, the NSA instead decided to develop code to exploit it for more than five years.[152] Then, starting in 2016, the anonymous Shadow Brokers group released an enormous trove of information about the NSA's intelligence gathering capabilities — including exploits and previously unknown vulnerabilities found in software and security products used for critical infrastructure and systems around the world.[153] In April 2017, one of the NSA exploits released by the Shadow Brokers, dubbed EternalBlue, involved the same vulnerability that the NSA had been exploiting for years.[154] The attackers behind the famed WannaCry ransomware in fact relied on the EternalBlue exploit, ultimately resulting in over 200,000 infected computers involving hospitals and banks, and an estimated $4 billion in losses worldwide.[155] This story reflects just the tip of the iceberg when it comes to the impact of vulnerabilities that are withheld by nation states — and that can potentially be exploited by others.[156]

While the US VEP is far from being perfect,[157] the Cybersecurity and Infrastructure Security Agency has nonetheless stated numerous times that vulnerability reports collected under its own CVD policy, as well as CVD policies for federal agencies, must be remediated and shall not be subject to consideration and adjudication in the VEP[158] (pursuant to section 5.4 of the US VEP charter).[159] Across the ocean, the UK Equities Process acknowledges, albeit less categorically, that vulnerabilities that "have already been subjected to similar considerations by a partner" and shared with the National Cyber Security Centre (a branch of the GCHQ) *may* not be subject to the Equities Process.[160] The UK Equities Process therefore provides no definition of "partner," and the term "may" renders this general rule discretionary.

In the Canadian context, many publicly available details of the Equities Management Framework (EMF) are lacking.[161] We do know that the CSE has a vulnerability disclosure assessment process involving experts from the CCCS for deciding whether to withhold or disclose vulnerability information based on a certain set of factors.[162] The EMF is also guided by the principle that vulnerabilities "that are public knowledge will not be subject to an equity assessment under this Framework." On its face, this principle could imply that vulnerabilities become "public knowledge" when they are disclosed to affected organizations and governments — and are therefore, in theory, not subject to assessment under the EMF.

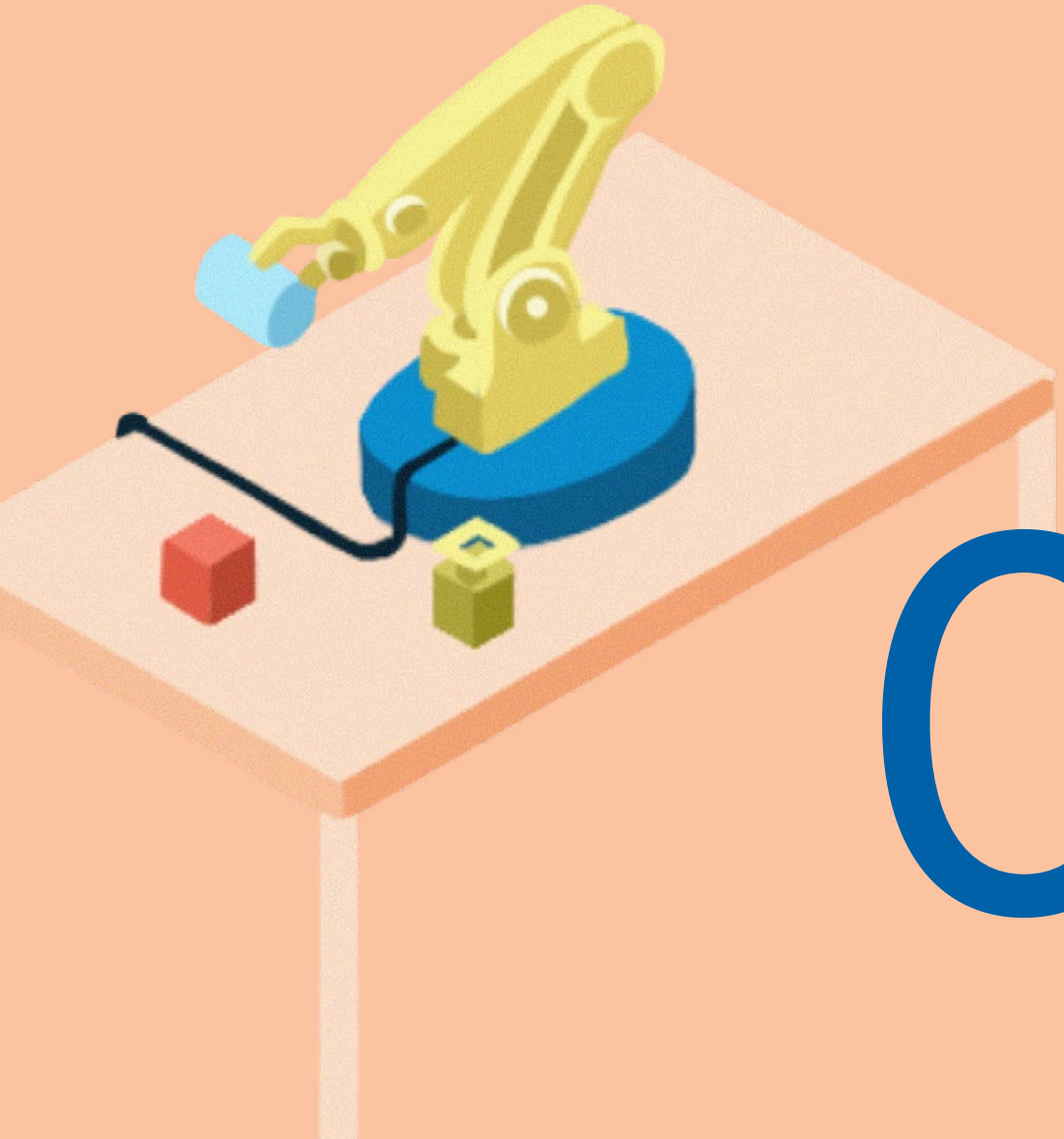
Yet, the use of the term "public knowledge" without further clarification could exclude vulnerabilities that are disclosed to government, the details of which are not disclosed to the public as a whole. Further, the EMF states that "[v]ulnerabilities discovered by CSE through operational research, or *otherwise obtained*, will be subject to the process outlined in this Framework."[163] This statement does not rule out the possibility that vulnerabilities disclosed to the CCCS will be handled under the CSE's framework, meaning that **vulnerability information already known by non-government individuals could be withheld by the CSE and exploited by malicious actors if this critical information ended up in the wrong hands.**

It remains unclear whether vulnerabilities that are disclosed to the CCCS could be assessed and withheld under Canada's EMF, which is currently marked by opacity. This lack of clarity, and the potential for the significant confusion it engenders from the perspective of the general public and security researchers, further confirms that a policy framework is lacking when it comes to the handling of vulnerability disclosure for federal government systems in Canada.



POLICY SOLUTIONS

Steps to Better Ensure Secure Systems in Canada



05

Steps to Better Ensure Secure Systems in Canada

Canada Needs a Policy Framework for Security Research and Good Faith Vulnerability Disclosure

Canada needs a policy framework that provides increased legal clarity for security research and vulnerability disclosure that occur in good faith. As described previously, certain aspects of Canada's criminal law may have a chilling effect on good faith computer security vulnerability discovery and disclosure.

Without being exhaustive, there are at least two possible ways forward in terms of a policy framework. **First**, the federal government could clarify the criteria that need to be met in order for a good faith security researcher to test, investigate and attempt to correct security vulnerabilities found within computer systems in a way that does not give rise to criminal liability, particularly under section 342.1 of the *Criminal Code*. Section 342.1 of the *Code* makes it a punishable offence to engage in unauthorized use of a computer (described in greater detail in the provision of the *Code* itself) when done so fraudulently and "without colour of right," which are both elements of the offence set out in section 342.1.

However, there is a growing body of legal decisions at the trial and appellate level, demonstrating that courts have spent considerable time deciding the thresholds required to meet the standards, particularly for these two terms.[164] The notion of "colour of right" is particularly significant in the context of coordinated vulnerability disclosure because some courts have come to interpret the term as referring to the ability to defend one's actions due to an honest but mistaken belief that justifies the action in question.[165] Enacting an amendment to the *Criminal Code* could provide useful legislative clarification up front as to when security research activity falls outside the scope of activity captured by section 342.1, rather than relying on the courts to fill these gaps when it comes to good faith security research.

Second, the Department of Justice could alternatively issue a Directive of the Attorney General pursuant to the *Director of Public Prosecutions Act* that directs the Director of Public Prosecutions to prosecute computer security research activity in light of certain considerations and only under certain circumstances. Such an initiative would not be unprecedented in Canada. For example, since December 2018, federal prosecutors and those acting on their behalf must now follow the Directive on *Prosecutions involving Non-Disclosure of HIV Status*, which stipulates when prosecution must not occur and should generally not occur, as well as what factors must be considered when prosecuting cases of non-disclosure of HIV status, given that such decisions must be determined on the basis of recent medical science on HIV transmission.[166] In a similar vein, a Directive of the Attorney General could be released in Canada that adopts aspects of the Dutch public prosecutor's policy letter, requiring federal prosecutors to consider the following when prosecuting computer security research activity involving vulnerability disclosure:

- **Motives:** Was the action taken in the context of a substantial social interest?
- **Proportionality:** Was the act proportionate (did the person not go beyond what was necessary) to achieve the goal?

- **The principle of subsidiarity:** Was disclosure made to the appropriate entity (did they exhaust their remedies before disclosing further)?[167]

The Directive in Canada could also encourage organizations that implement CVD procedures to clearly state that disclosing in adherence with that policy's requirements would fall under authorized activity (which could otherwise be prohibited by various laws including criminal provisions). This legal clarification is provided in the Dutch context as described previously, and in a clarifying document published in 2017 by the Department of Justice.[168] The vulnerability disclosure policy template issued by CISA also requires federal agencies to consider good faith vulnerability disclosure that occurs in line with the applicable CVD policy as constituting authorized activity.[169] While such a Directive in the Canadian federal context would apply to Canada's territories, it would be important for provincial attorneys general to also adopt the Directive in their own provinces.

We encourage the Government of Canada, and particularly the Department of Justice, to examine these solutions as two possible ways forward, given the need for a policy framework for good faith computer security vulnerability discovery and disclosure in Canada.

Canada's Federal Agencies Need Vulnerability Disclosure Procedures in Line with Best Practices

On a more pragmatic level, the Government of Canada should consider strengthening its internal and external disclosure procedures for vulnerabilities involving federal computer systems. Governments and organizations stand to benefit when they work with security researchers to identify and remediate existing vulnerabilities, while making sure to alert those who might be affected.[170] Those who find flaws in the government's systems and critical infrastructure should therefore be provided with a well-thought-out pathway for disclosing vulnerabilities to the owners or managers of those systems and/or the federal government.

As discussed earlier, Canadian policymakers can particularly learn from two jurisdictions leading the way when it comes to the decision to require or encourage the use of CVD procedures. Canada has the option of implementing regulation as the US has done, issuing binding requirements that each federal agency deploys its own CVD policy. However, there are risks associated with this approach: the scope of what can be tested ought to be initially limited, and there must be adequate internal expertise to handle such disclosures. Canada may prefer to draw on the Dutch model for CVD, where organizations (such as software vendors or certain government bodies) that manage or own computer systems are encouraged (but not required) to facilitate coordinated vulnerability disclosure. In either case, a specific government cybersecurity agency in Canada could act as an intermediary on an as-needed basis. Clarification would also be useful as to when a security researcher should disclose vulnerability information to a software vendor and/or the affected federal agency.

As mentioned, CVD procedures for the Government of Canada's systems would ideally be implemented only when organizations and/or agencies have the ability to adequately respond to external vulnerability reports, as well as patch and remediate

those vulnerabilities. For example, the US Department of Defense vulnerability disclosure program slowly broadened the scope of what could be tested over the course of several years.[171] The UK has been working with vulnerability disclosure experts, such as Katie Moussouris of Luta Security, to carefully role out a multi-year pilot vulnerability disclosure program, improving its system slowly over time.[172] Implementing a pilot CVD program is necessary for avoiding initial overload, providing an opportunity for the government to collect data, to inform more mature handling of vulnerability disclosures. During the pilot, a security maturity assessment process should be developed and implemented to assess, prioritize, and add resources necessary for vulnerability management. It is also vital that any government entity wishing to facilitate CVD procedures for the first time avoid doing so primarily for the purposes of hype, marketing, or to mitigate the risk of unwanted attention associated with fully or partially public disclosure of vulnerabilities found in its systems.[173]

It is equally important that CVD procedures involving Canada's federal government systems contain certain standard elements and are written in a clear, accessible fashion. The benefits of clearly written procedures are two-fold. First, they allow organizations to glean the insight and expertise of highly motivated good faith security researchers. Second, they enable these researchers to disclose vulnerabilities and strengthen the security of systems with clarification around what constitutes legal activity.[174]

There are standard elements that CVD procedures should contain, including those run by governments. Drawing on established cybersecurity best practices[175] including NIST,[176] ISO standards,[177] and work by Woszczynski et al.,[178] we have identified that there are generally at least five aspects that are foundational for effective CVD processes:

1. **Define eligibility.** Who is able to submit vulnerability reports, and in what manner, should be clearly delineated. There should generally not be limitations on who can submit and whether people can submit anonymously. It is also not a common practice to limit who can disclose vulnerabilities based on security clearances, country of origin, or residence except in rare cases such as time-limited, invite-only new vulnerability disclosure procedures involving, for example, military systems.[179]

2. **Provide submission and verification procedural information.** The vulnerability reporting and triage processes should be clear. Encrypted communication should be an encouraged option to better secure the information passed on. The organization handling the vulnerability disclosure process should be transparent about how it responds to submissions and in what time frame. It is similarly important that the organization clearly state its commitment to take the steps needed to mitigate the risk and resolve the vulnerability once it is deemed valid. The process should also provide details as to how the organization verifies vulnerability information and assesses the level of criticality.

3. **Set out restrictions and expectations.** It is important to set out mutual expectations for both security researchers and those

to whom vulnerabilities are disclosed, in order to build goodwill and increase trust among all parties involved. Expectations of security researchers should be set out, including what activity is prohibited (such as the use of social engineering or denial of service testing). Similarly, organizations should set out the timeline that disclosers can expect in terms of communication and remediation of the flaw.[180] Drawing on the policy framework that we hope is provided by the Government of Canada, CVD policies should also clarify and limit the scope of legal liability for people who disclose vulnerabilities in good faith and in adherence with the procedures set out.

4. **Provide credit and recognition.** Disclosers should receive public credit for their submission once the vulnerability has been repaired, so long as they consent. Canada could run a page similar to that provided by Germany's armed forces, which provides details on all disclosed vulnerabilities (e.g., disclosure date, URL involved, type of vulnerability) and public recognition of the discloser (using their name or alias).[181] It is also possible to provide disclosers with recognition for their contributions in the form of awards, gift vouchers, and possibly monetary remuneration or honoraria. Various considerations accompany the decision of whether to remunerate for voluntary external disclosures. Remunerating disclosers for vulnerability information can encourage them to share this information with software and hardware vendors, as well as the Government of Canada, rather than to others in ways that could be used for offensive purposes against the Canadian government's systems. Remunerating disclosers can also be a way to acknowledge the labour and efforts of security researchers. However, when it comes to paying disclosers, governments may face administrative hurdles involving procurement procedures and requirements. Other remuneration considerations also include the long-term impacts of the government's potential reliance on an external, distributed workforce for vulnerability discovery and disclosure, particularly with respect to the labour rights implications for security researchers.[182]

5. **Advise the public of the vulnerability and its remediation.** It is important to provide the public with information about the vulnerability once remediation has occurred or is made available, as part of efforts to make vulnerability reports public in order to strengthen the security of government systems and critical infrastructure. In the US context, CISA alerts organizations to security threats to critical infrastructure networks and provides the public with information about exploits, security issues, and vulnerabilities for which a patch has become available.[183] Canada should build on its already existent alert and advisory system[184] by publishing advisory information about vulnerabilities discovered through CVD procedures enabled by the federal government.

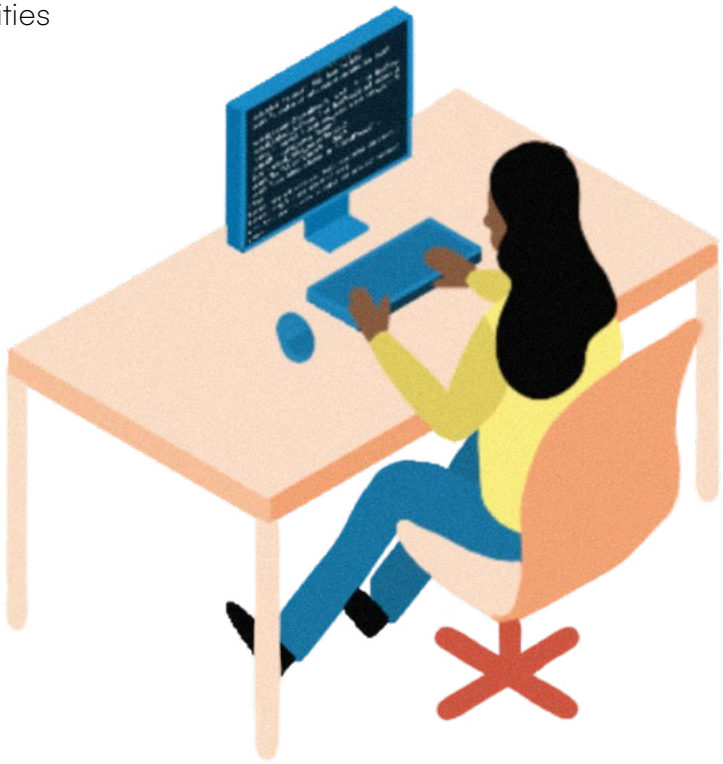
These emerging, standard elements of CVD are by no means exhaustive, and we encourage the Government of Canada to work with technical and policy experts in its determination of whether and how to implement CVD procedures for its systems.

Disclosed Vulnerabilities Must Be Kept Separate from the Equities Management Framework

It is vital that Canada shift away from an approach that attempts to achieve the security of its systems through reliance on obscurity and secrecy. Instead, it should move toward an approach that facilitates transparent and accountable procedures when it handles disclosed vulnerabilities. As described previously, it is currently not clear how Canadian government bodies, including the Canadian Centre for Cyber Security, handle the vulnerability reports they receive.

It is important that the Government of Canada ensures that appropriate steps are taken to mitigate the risks associated with externally reported vulnerabilities, including ensuring their remediation. When vulnerabilities disclosed through a CVD procedure end up being assessed in an equities management framework, this is an indication that the equities management process has failed. Failing to remediate flaws that have effectively become public knowledge can put the government's systems and critical infrastructure at risk due to the potential that the external actor and others who learn about these vulnerabilities could exploit them. One need only look to the story of WannaCry, described earlier, to understand the grave harm that can arise when governments fail to disclose vulnerabilities to vendors for risk mitigation and remediation, enabling attackers to exploit such vulnerabilities known to the government.

For these reasons, Canada should both state in its Equities Management Framework, and in any vulnerability disclosure procedures involving government systems, that vulnerabilities disclosed through CVD must be resolved and kept separate from the equities management and assessment process.



About the Authors

Yuan Stevens is the Policy Lead at the Cybersecure Policy Exchange and the Ryerson Leadership Lab. Yuan is an action-oriented researcher working at the intersections of law, policy and computer security. Her work equips society with the ability to understand and patch up harmful vulnerabilities in sociotechnical and legal systems. Passionate about building community, she is also a research affiliate at the Data & Society Research Institute and a research fellow at the Centre for Media, Technology & Democracy at McGill's School of Public Policy. She received her B.C.L./J.D. from McGill University in 2017, working as a research assistant for hacker expert Gabriella Coleman. She serves on the board of directors for Open Privacy Research Institute and previously worked at the Berkman Klein Center for Internet & Society at Harvard University.

Stephanie Tran is an experienced researcher with over five years of experience analyzing public policy and human rights issues related to digital technologies, with past experience working for the Citizen Lab, Amnesty International Canada, the United Nations Office for the Coordination of Humanitarian Affairs (UN OCHA) and more. She is a trained computer programmer, having earned a Diploma in Computer Programming from Seneca College. She also holds a dual degree Master of Public Policy (Digital, New Technology and Public Affairs Policy stream) from Sciences Po in Paris, and a Master of Global Affairs from the University of Toronto. She earned her BA degree from the University of Toronto specializing in Peace, Conflict and Justice.

Ryan Atkinson is an experienced researcher on cybersecurity challenges and solutions, pursuing his PhD in Political Science at the University of Western Ontario, where he is examining the cyber defence policy of NATO, Canada and other member states. He has led the Cybersecurity and Information Warfare Program at the NATO Association of Canada as Research Analyst and Project Manager, publishing numerous analytic articles and in-depth interviews on subjects of cybersecurity, hybrid warfare, and disinformation. He also guided organizational attainment of cyber industry resilience from information security infrastructure frameworks within various industries including telecommunications, healthcare, finance, technology and government as a cybersecurity consultant at KPMG Canada.

Sam Andrey is the Director of Policy & Research at the Ryerson Leadership Lab. Sam has led applied research and public policy development for the past decade, including the design, execution and knowledge mobilization of surveys, focus groups, interviews, randomized controlled trials and cross-sectional observational studies. He also teaches about public leadership and advocacy at Ryerson University and George Brown College. He previously served as Chief of Staff and Director of Policy to Ontario's Minister of Education, in the Ontario Public Service and in not-for-profit organizations advancing equity in education and student financial assistance reform. Sam has an Executive Certificate in Public Leadership from Harvard's John F. Kennedy School of Government and a BSc from the University of Waterloo.

Appendix A: Global State of Play for Coordinated Vulnerability Disclosure

Country	Membership	Organization name	If applicable, specific federal government organization	Has distinct and clear disclosure process for vulnerabilities involving government systems	Disclosure process open to the general public	Describes the submission and verification process	Provides terms and rules for disclosers (e.g., limiting what is in scope)	Disclosers can publicly receive credit	Remuneration (e.g. monetary) can be provided for those who submit	Publicly disseminates information about vulnerabilities disclosed through CVD process
Argentina	G20 Member	Dirección Nacional de Ciberseguridad	Innovación Pública	✗	✗	✗	✗	✗	✗	Unknown
Australia	G20 Member	CERT Australia	Australian Cyber Security Centre, based in Australian Signals Directorate	✓	✓	✗	✓	✗	✗	Unknown
Brazil	G20 Member	CTIR Gov	Department of Information and Communications Security	✗	✗	✗	✗	✗	✗	Unknown
Canada	G20 Member	Canadian Centre for Cyber Security	Communications Security Establishment	✗	✗	✗	✗	✗	✗	Unknown
China	G20 Member	CNCERT/CC	n/a	✓	✓	✓	✓	✗	✗	✓
EU	G20 Member	EU-CERT	n/a	✓	✓	✓	✓	✓	✗	✓
France	G20 Member	CERT-FR	National Agency for the Security of Information Systems (ANSSI)	✓	✓	✗	✗	✗	✗	Unknown
Germany	G20 Member	CERT-Bund	Federal Office for Information Security (BSI)	✓	✗	✓	✓	✗	✗	Unknown
India	G20 Member	CERT-In	Ministry of Electronics and Information Technology	✓	✓	✗	✗	✗	✗	✓
Indonesia	G20 Member	ID-CERT	n/a	✗	✗	✗	✗	✗	✗	Unknown
Italy	G20 Member	CSIRT Italy	Security Intelligence Department (DIS)	✓	✓	✗	✓	✗	✗	Unknown
Japan	G20 Member	JPCERT/CC	Independent, but working alongside Information-technology Promotion Agency (IPA)	✓	✓	✓	✓	✓	✗	✓

Latvia	Non-G20 Member	CERT.LV	Ministry of Defense of the Republic of Latvia	✓	✓	✓	✓	✗	✗	✓
Mexico	G20 Member	CERT-MX	Guardia Nacional	✗	✗	✗	✗	✗	✗	Unknown
Netherlands	Non-G20 Member	National Cyber Security Centre (NCSC)	Ministry of Justice and Security	✓	✓	✓	✓	✗	✓	Unknown
New Zealand	Non-G20 Member	CERT NZ	Ministry of Business, Innovation and Employment	✓	✓	✓	✓	✗	✗	Unknown
Russia	G20 Member	Data Security Threats Databank	Federal Service for Technical and Export Control, based in the Ministry of Defence	✓	✓	✓	✓	✓	✓*	✓
Saudi Arabia	G20 Member	CERT-SA	National Cybersecurity Authority	✓	✓	✗	✗	✗	✗	Unknown
Singapore	Non-G20 Member	Cyber Security Agency of Singapore and Government Technology Agency	Ministry of Communications and Information; Prime Minister's Office	✓	✓	✓	✓	✓	✗	✓
South Africa	G20 Member	South African Computer Security Incident Response Team	Dept. of Telecommunications and Postal Services	✗	✗	✗	✗	✗	✗	Unknown
South Korea	G20 Member	KN-CERT	National Cyber Security Center (NCSC), based in National Intelligence Service	✗	✗	✗	✗	✗	✗	Unknown
Spain	Non-G20 Member	CCN-CERT	Spanish National Intelligence Centre	✓	✓	✓	✓	✗	✗	✓
Turkey	G20 Member	TR-CERT	Information Technologies and Communication Authority	✗	✗	✗	✗	✗	✗	Unknown
United Kingdom	G20 Member	National Cyber Security Centre	Government Communications Headquarters (GCHQ)	✓	✓	✓	✓	✓	✓	✓
USA	G20 Member	CISA Binding Operational Directive for federal agencies	Cybersecurity & Infrastructure Security Agency	✓	✓	✓	✓	✓	✓	✓

Legend: * = Recognition given through points

Appendix B: List of Participants

It is important to note that the varied perspectives of our workshop participants greatly informed this report; however, the statements and recommendations are solely those of the authors.

A list of workshop participants (who consented to having their names made publicly available) is as follows:

1. **Amit Elazari,** Director, Global Cybersecurity Policy, Intel Corporation
2. **Baiba Kaškina,** CERT.LV
3. **Brenda McPhail,** Director, Privacy, Technology & Surveillance Project, Canadian Civil Liberties Association
4. **Christopher Parsons,** Senior Research Associate at Citizen Lab, Munk School of Global Affairs & Public Policy, University of Toronto
5. **Florian Martin-Bariteau,** Associate Professor of Law, University Research Chair in Technology and Society, and Director, Centre for Law, Technology and Society, University of Ottawa
6. **Gianluca Varisco,** CEPS Research Affiliate
7. **Jeroen van der Ham,** National Cyber Security Centre (Netherlands); Associate Professor of Incident Response, University of Twente
8. **Josh Kenway,** Cybersecurity & Technology Policy Analyst, PayPal
9. **Katherine Rusk,** Lawyer, Osler, Hoskin & Harcourt LLP
10. **Katie Moussouris,** CEO, Luta Security
11. **Lisa Wiswell Coe,** Independent (Former architect of the Hack the Pentagon CVD program and DoD VDP)
12. **Melanie Rieback,** CEO and Co-founder of Radically Open Security
13. **Milos Stojadinovic,** Senior Director, Adversary Emulation (Red Team), Royal Bank of Canada
14. **Rafal Rohozinski,** CEO, SecDev / ZeroPoint
15. **Sumit Bhatia,** Director, Innovation and Policy at Rogers Cybersecure Catalyst; Canada's National Cybersecurity Centre
16. **Tara Swaminatha,** Principal, ZeroDay Law
17. **Tarah Wheeler,** Cyber Project Fellow, Belfer Center for Science and International Affairs & International Security Fellow, New America

Appendix C: Definitions

Bug bounty program: Programs that provide financial rewards for individuals who disclose security vulnerabilities to the relevant organization. Bug bounty programs can be one mechanism as part of a larger coordinated vulnerability disclosure program. They can be time-bound or ongoing, as well as invite-only or open to the public.

Community Emergency Response Team (CERT): A malleable term that often takes the form of a security operations centre, incident response team, group of forensic investigators or engineering teams that respond to security incidents.[185] However, Carnegie Mellon University owns the trademark for "CERT" and must approve any uses of the term.[186]

The first CERT was created by DARPA (Defense Advanced Research Projects Agency) after the 1988 Morris worm, where grad student Robert Morris spread a non-destructive worm across Cornell university computers that caused many computers to crash.[187] This incident led to the creation of the first computer security incident response team (CSIRT) in November 1988, the CERT Coordination Center.[188] Over time, the CERT model has adapted and evolved to other jurisdictions.[189]

Computer security incident response team (CSIRT): A term that has essentially the same meaning as CERT, but is not trademarked and can therefore by used by any organization without permission from the Software Engineering Institute at Carnegie Mellon University.[190]

Communications Security Establishment: Canada's intelligence agency responsible for monitoring foreign intelligence activity, maintaining the security and assurance of information in Canada, and conducting defensive and offensive foreign cyber operations.[191]

Discloser: An individual who discloses a vulnerability found in an information system.

Vulnerability: A weakness that can be exploited by an attacker, allowing them to perform unauthorized and/or undesirable actions. The weakness can be found in hardware or software, "in an information system, system security procedures, internal controls, or implementation."[192]

Vulnerability disclosure: Providing information on a vulnerability to a party that is likely unaware of it.[193] Different options for disclosure may include:

- **No disclosure:** Everything known about the vulnerability is kept private. Vendors may prefer this method in order to prevent implicating their public image, or to protect trade secrets.[194] This may also occur due to researchers feeling discouraged from disclosing out of fear of retribution, or as a result of governments wanting to take advantage of the vulnerability for national security or intelligence purposes.[195]

- **Coordinated vulnerability disclosure (CVD):** An approach, framework or process where disclosers and organizations work in cooperation to examine and resolve discovered vulnerabilities. It typically involves "reporting, coordinating, and publishing information about a vulnerability and its resolution," aiming to ensure that vulnerabilities are resolved and that risk is limited.[196] Some principles that underly CVD are to reduce harm, presume benevolence of individuals who report vulnerabilities, and incentivize cooperative behaviour.[197]

- **Full disclosure:** All information about the vulnerability is released to the public. This usually includes a published report on the vulnerability, as well as proof of concept code.[198]

- **Limited (partial) disclosure:** Some, but not all, of the information known about the vulnerability is disclosed publicly. In these cases, some information on the vulnerability is provided, while technical details and proof of concept code may be withheld.[199]

Vulnerabilities equities process (VEP): A term used by some government agencies to determine the processes to follow when deciding whether to disclose vulnerabilities or to retain knowledge of the vulnerability in order to exploit it for law enforcement, national security, or intelligence purposes. They are the "internal policymaking structures" that help governments decide how to handle vulnerabilities.[200]

Examples include the US' Vulnerabilities Equities Process,[201] the UK's Equities Process,[202] and Canada's Equities Management Framework.[203]

References

[1] Digital Security Group. (2008, March 7). *Security Flaw in Mifare Classic*. Nijmegen Institute for Computer Science and Information Science. https://www.sos.cs.ru.nl/applications/rfid/main.html; Digital Security Group Radboud University Nijmegen. (2008, March 12). *Security Flaw in MIFARE Classic* [Press release]. https://www.cs.ru.nl/~flaviog/publications/Security_Flaw_in_MIFARE_Classic.pdf.

[2] Kirk, J. (2008, June 20). Dutch Launch Open-source Smart Card Software Project. *ABC News*. https://abcnews.go.com/Technology/PCWorld/story?id=5210881.

[3] EDRi. (2008, July 16). *Dutch University sued to stop publishing research on chip technology. EDRi.* https://edri.org/our-work/edrigramnumber6-14dutch-university-chip.

[4] NXP BV v. Radboud University, 18 July 2008, Court of Justice Arnhem, https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBARN:2008:BD7578.

[5] EDRi (2008, July 16).

[6] NXP BV v. Radboud University (2008).

[7] van t'Hof, C. (2016). Helpful Hackers: How the Dutch do Responsible Disclosure. *Vior Webmedia*. 52.

[8] Hof, *Helpful Hackers,* 51-52.

[9] *NXP BV v. Radboud University* (2008).

[10] Ibid

[11] Ibid, para. 3.3, translation by report authors.

[12] Radboud University Nijmegen. (n.d.). *Roel Verdult*. Institute for Computing and Information Sciences. http://www.cs.ru.nl/~rverdult/.

[13] Pupillo, L., Ferreira, A., & Varisco, G. (2018). *Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges* (Report of a CEPS Task Force). Centre for European Policy Studies (CEPS) Brussels. https://www.ceps.eu/wp-content/uploads/2018/06/CEPS%20TFRonSVD%20with%20cover_0.pdf; Health Canada. (2019, December 10). Scientific Advisory Committee Digital Health Technologies (SAC-DHT) November 23, 2018 Record of Proceedings [Decisions]. Government of Canada. https://www.canada.ca/en/health-canada/services/drugs-health-products/medical-devices/activities/scientific-expert-advisory-committees/digital-health-technologies/record-proceedings-2018-11-23.html.

[14] OECD. (2021). *Encouraging vulnerability treatment: Overview for policy makers.* OECD Digital Economy Papers, 307, 1-45. https://www.oecd-ilibrary.org/docserver/0e2615ba-en.pdf.

[15] Brady, R. M., Anderson, R. J., & Ball, R. C. (1999). Murphy's law, the fitness of evolving species, and the limits of software reliability. *University of Cambridge Computer Laboratory,* 471, 1-14. https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-471.pdf.

[16] Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the Future of Cyber War. *Survival*, *53*(1), 23–40. https://doi.org/10.1080/00396338.2011.555586; Perlroth, N. (2021). *This Is How They Tell Me the World Ends: The Cyberweapons Arms Race*. Bloomsbury Publishing. https://thisishowtheytellmetheworldends.com/.

[17] Public Safety Canada. (2019). *National Cyber Security Action Plan (2019-2024): Budget 2018 Investments.* Government of Canada. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2019/index-en.aspx.

[18] Samos, C. (2021, April 29). Ransomware demands estimated to have cost hundreds of millions of dollars in Canada in 2020: report. *CTV News.* https://www.ctvnews.ca/sci-tech/ransomware-demands-estimated-to-have-cost-hundreds-of-millions-of-dollars-in-canada-in-2020-report-1.5407727.

[19] Statistics Canada. (2020, October 20). About one-fifth of Canadian businesses were impacted by cyber security incidents in 2019. *Government of Canada.* https://www150.statcan.gc.ca/n1/daily-quotidien/201020/dq201020a-eng.htm.

[20] Wheeler, T. (2018, September 12). In Cyberwar, There Are No Rules. *Foreign Policy* (Fall 2018). https://foreignpolicy.com/2018/09/12/in-cyberwar-there-are-no-rules-cybersecurity-war-defense/.

[21] Yes We Hack. (n.d.). Coordinated Vulnerability Disclosure: Joining Forces to Reduce Risk [White paper]. Yes We Hack. https://f.hubspotusercontent00.net/hubfs/7520354/livre-blanc-yes-we-hack-CVD-EN.pdf.

[22] Tech Checkup: Dealing with Technology Change in Pandemic Recovery. (2020, October 15). *The Conference Board of Canada.* https://www.conferenceboard.ca/focus-areas/innovation-technology/tech-checkup.

[23] Shekar, S. (2020, August 5). Cost of Data Breaches in Canada up 6.7% in 2020. *Yahoo Finance.* https://ca.finance.yahoo.com/news/cost-of-data-breaches-in-canada-up-67-in-2020-191002562.html.

[24] National Cyber Threat Assessment. (2020, November 16). Canadian Centre for Cyber Security. *Communications Security Establishment.* https://cyber.gc.ca/sites/default/files/publications/ncta-2020-e-web.pdf

[25] Henriquez, M. (2020, December 9). IoT Cybersecurity Improvement Act signed into law. *Security Magazine.;* Information Technology Laboratory: Computer Security Resource Center. (2021, February 4). *Vulnerability Disclosure Guidance.* National Institute of Standards and Technology. https://csrc.nist.gov/Projects/vdg.

[26] Canadian Centre for Cyber Security. (2020). *National Cyber Threat Assessment 2020.* Communications Security Establishment. https://cyber.gc.ca/sites/default/files/publications/ncta-2020-e-web.pdf

[27] Householder, A. D., Wassermann, G., Manion, A., & King, C. (2017). *The CERT Guide to Coordinated Vulnerability Disclosure.* Software Engineering Institute. https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_503340.pdf.

[28] Public Prosecution Service. (2020, December 14). *OM Policy Letter Coordinated Vulnerability Disclosure.* https://www.om.nl/documenten/richtlijnen/2020/december/14/om-beleidsbrief-ethisch-hacken.

[29] Elazari, A. "The Law and Economics of Bug Bounties" (2018), USENIX 27th Security Symposium, https://www.usenix.org/conference/usenixsecurity18/presentation/elazari-bar; OECD, *Encouraging vulnerability treatment*

[30] Secretary of the Air Force Public Affairs. (2018, November 5). USAF announces Hack the Air Force 3.0. U.S. Air Force. https://www.af.mil/News/Article-Display/Article/1682502/usaf-announces-hack-the-air-force-30/

[31] *Vulnerability Reporting.* (2018, November 15). National Cyber Security Centre. https://www.ncsc.gov.uk/information/vulnerability-reporting

[32] *EU-FOSSA 2—Free and Open Source Software Auditing.* (n.d.). European Commission. Retrieved February 24, 2021, from https://ec.europa.eu/info/departments/informatics/eu-fossa-2_en

[33] Braga, M. (2016, November 28). *The Canadian government doesn't want hackers' help. CBC.* https://www.cbc.ca/news/technology/canadian-government-hackers-1.3866336; *The Canadian Press.* (2015, July 28). Hackers target Canadian government websites. *The Globe and Mail.* https://www.theglobeandmail.com/news/national/hackers-target-canadian-government-website/article25729750/; Jones, R. P. (2020, August 17). Cyberattacks that targeted Government of Canada online services brought under control, officials say. *CBC.* https://www.cbc.ca/news/politics/cra-gckey-cyberattack-1.5689106.

[34] Carin, B. (2017, June 20). G20 safeguards vulnerabilities of digital economy, with financial sector focus. *G20 Insights.* https://www.g20-insights.org/policy_briefs/g20-safeguards-vulnerabilities-digital-economy-financial-sector-focus/.

[35] Khan, M. K., Goldberg, S., Grainger, P., & Sethi, B. (2020, November 26). Heightening cybersecurity to promise safety and fairness for citizens in the Post-Covid-19 Digital World. *G20 Insights.* https://www.g20-insights.org/policy_briefs/heightening-cybersecurity-to-promise-safety-and-fairness-for-citizens-in-the-post-covid-19-digital-world/.

[36] Woszczynski, A., Green, A., Dodson, K., & Easton, P. (2020). Zombies, Sirens, and Lady Gaga – Oh My! Developing a Framework for Coordinated Vulnerability Disclosure for U.S. Emergency Alert Systems. *Government Information Quarterly, 37*(1), 101418. https://doi.org/10.1016/j.giq.2019.101418.

[37] International Organization for Standardization. (2020). *Information technology — Security techniques — Vulnerability handling processes* (CSA ISO-IEC 30111-20). https://www.scc.ca/en/standardsdb/standards/30641.

[38] H. Cavusoglu, H. Cavusoglu and S. Raghunathan, "Efficiency of Vulnerability Disclosure Mechanisms to Disseminate Vulnerability Knowledge," in *IEEE Transactions on Software Engineering*, vol. 33, no. 3, pp. 171-185, March 2007, doi: 10.1109/TSE.2007.26.

[39] Householder, Wassermann, Manion, & King, *The CERT Guide to Coordinated Vulnerability Disclosure.*

[40] Hathaway, M. (2019). *Patching Our Digital Future Is Unsustainable and Dangerous.* Centre for International Governance Innovation. https://www.cigionline.org/articles/patching-our-digital-future-unsustainable-and-dangerous/.

[41]Householder, Wassermann, Manion, & King, *The CERT Guide to Coordinated Vulnerability Disclosure.*

[42] Joint Task Force Transformation Initiative. (2013). *Security and Privacy Controls for Federal Information Systems and Organizations* (NIST SP 800-53r4; p. NIST SP 800-53r4). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r4

[43] OECD, *Encouraging vulnerability treatment.*

[44] Ibid

[45] Ibid.

[46] CBC News. (2019, July 22). Equifax to pay up to $700M in U.S. to settle data breach, but Canada is not included. *CBC News.* https://www.cbc.ca/news/business/equifax-fine-1.5219957.

[47] Whittaker, Z. (2018, December 10). Equifax breach was 'entirely preventable' had it used basic security measures, says House report. *TechCrunch.* https://techcrunch.com/2018/12/10/equifax-breach-preventable-house-oversight-report/.

[48] OECD, *Encouraging vulnerability treatment.*

[49] Ibid.

[50] Neutze, J. (2017), Coordinated Vulnerability Disclosure (CVD), https://www.ceps.eu/wp-content/uploads/2017/05/Jan%20Neutze%20Microfsoft%20-%20CVD.pdf; Kranenbarg, M., Holt, T. J., & van der Ham, J. (2018). Don't shoot the messenger! A criminological and computer science perspective on coordinated vulnerability disclosure. *Crime Science, 7*(1), 16. https://doi.org/10.1186/s40163-018-0090-8.

[51] Wheeler, T. (2021, May 3) "Cybersecurity Ignorance Is Dangerous", *Foreign Policy.* https://foreignpolicy.com/2021/05/03/cybersecurity-ignorance-is-dangerous/.

[52] Neutze, J. (2017), Coordinated Vulnerability Disclosure (CVD); Kranenbarg, Holt, & van der Ham, Don't shoot the messenger!

[53] Householder, Wassermann, Manion, & King, *The CERT Guide to Coordinated Vulnerability Disclosure.*

[54] OECD, *Encouraging vulnerability treatment.*

[55] See, for example, work by E. Gabriella Coleman and Alex Golub, which identifies that security researchers and hackers are not homogenous in their intention and motivation and that there exists a wide array of ethical viewpoints held by hackers animating the work they do. Coleman, E. G., & Golub, A. (2008). Hacker practice: Moral genres and the cultural articulation of liberalism. *Anthropological Theory, 8*(3), 255–277. https://doi.org/10.1177/1463499608093814.

[56] Householder, Wassermann, Manion, & King, *The CERT Guide to Coordinated Vulnerability Disclosure.*

[57] Erik Silfversten, William Phillips, Giacomo Persi Paoli, & Cosmin Ciobanu. (2018). *Economics of Vulnerability Disclosure.* European Union Agency For Network and Information Security. https://www.enisa.europa.eu/publications/economics-of-vulnerability-disclosure/at_download/fullReport. See also Neutze, J., Coordinated Vulnerability Disclosure (CVD).

[58] Householder, Wassermann, Manion, & King, *The CERT Guide to Coordinated Vulnerability Disclosure.*

[59] Ibid.

[60] Ibid.

[61] Ibid.

[62] Ibid.

[63] Swaminatha, T. (n.d.). *Bug Bounty and Vulnerability Disclosure Programs.* ZeroDay Law LLC. Retrieved March 8, 2021, from http://uk.practicallaw.thomsonreuters.com/w-014-4541.

[64] Ruohonen, J., Hyrynsalmi, S., & Leppänen, V. (2020). A mixed methods probe into the direct disclosure of software vulnerabilities. *Computers in Human Behavior, 103,* 161–173. https://doi.org/10.1016/j.chb.2019.09.028.

[65]Brady, R. M., Anderson, R. J., & Ball, R. C., Murphy's law, the fitness of evolving species, and the limits of software reliability.

[66] Kranenbarg, Holt & van der Ham, Don't shoot the messenger!

[67] Ozment, A. (2005). The Likelihood of Vulnerability Rediscovery and the Social Utility of Vulnerability Hunting. *Fourth Workshop on the Economics of Information Security (June 2–3 2005).* https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.61.154.

[68] Finifter, M., Akhawe, D., & Wagner, D. (2013). An Empirical Study of Vulnerability Rewards Programs. *22nd USENIX Security Symposium.* https://www.usenix.org/system/files/conference/usenixsecurity13/sec13-paper_finifter.pdf.

[69] Votipka, D., Stevens, R., Redmiles, E., Hu, J., & Mazurek, M. (2018). Hackers vs. Testers: A Comparison of Software Vulnerability Discovery Processes. *2018 IEEE Symposium on Security and Privacy (SP)*, 374–391. https://doi.org/10.1109/SP.2018.00003.

[70] Swaminatha, *Bug Bounty and Vulnerability Disclosure Programs*.

[71] Kranenbarg, Holt & van der Ham, Don't shoot the messenger!

[72] Rhysider, J. (2018, November 1). *EP 25: Alberto (No. 25)*. https://darknetdiaries.com/episode/25/

[73] National Cyber Security Centre. (2018). *Coordinated Vulnerability Disclosure: The Guideline*. National Cyber Security Centre. https://english.ncsc.nl/publications/publications/2019/juni/01/coordinated-vulnerability-disclosure-the-guideline.

[74] National Cyber Security Centre, *Coordinated Vulnerability Disclosure*.

[75] FIRST Improving Security Together. (n.d.). National Cyber Security Centre of The Netherlands Team Information. FIRST Improving Security Together. https://www.first.org/members/teams/ncsc-nl.

[76] National Cyber Security Centre. (n.d.). About the NCSC. Ministry of Justice and Security. https://english.ncsc.nl/about-the-ncsc.

[77] Government of the Netherlands. (n.d.). Ministry of Justice and Security. Government of the Netherlands. https://www.government.nl/ministries/ministry-of-justice-and-security.

[78] National Cyber Security Centre, *Coordinated Vulnerability Disclosure*.

[79] National Cyber Security Centre. (n.d.). *Reporting a Vulnerability (CVD)*. Ministry of Justice and Security. https://english.ncsc.nl/contact/reporting-a-vulnerability-cvd

[80] National Cyber Security Centre, *Coordinated Vulnerability Disclosure*.

[81] National Cyber Security Centre, *Reporting a Vulnerability (CVD)*.

[82] Ibid

[83] Ibid

[84] Ibid

[85] National Cyber Security Centre, *Coordinated Vulnerability Disclosure*.

[86] Public Prosecution Service. (2020). *OM-beleidsbrief Coordinated Vulnerability Disclosure*. Public Prosecution Service. https://www.om.nl/documenten/richtlijnen/2020/december/14/om-beleidsbrief-ethisch-hacken

[87] Public Prosecution Service, *OM-beleidsbrief Coordinated Vulnerability Disclosure*.

[88] National Cyber Security Centre, *Coordinated Vulnerability Disclosure,* 9.

[89] Public Prosecution Service, *OM-beleidsbrief Coordinated Vulnerability Disclosure*.

[90] Tidy, J. (2020, November 20). Trump Twitter 'hack': Dutch police question researcher. *BBC News*. https://www.bbc.com/news/technology-55019858.

[91] Public Prosecution Service. (2020, December 16). Trump Twitter account login not punishable. *Public Prosecution Service*. https://www.om.nl/actueel/nieuws/2020/12/16/inlog-twitter-account-trump-niet-strafbaar

[92] National Cyber Security Centre, *Coordinated Vulnerability Disclosure,* 10.

[93] Pupillo, Ferreira & Varisco, *Software Vulnerability Disclosure in Europe*, 46.

[94] Cybersecurity and Infrastructure Security Agency. (2020, September 2). *Binding Operational Directive 20-01*. Department of Homeland Security. https://cyber.dhs.gov/bod/20-01/.

[95] Cybersecurity and Infrastructure Security Agency. (2018, November 19). *Cybersecurity and Infrastructure Security Agency Act of 2018*. Department of Homeland Security. https://us-cert.cisa.gov/ncas/current-activity/2018/11/19/NCCIC-Now-Part-Cybersecurity-and-Infrastructure-Security-Agency.

[96] Cybersecurity and Infrastructure Security Agency, *Binding Operational Directive 20-01*, 8(a).

[97] Ibid, 8(b) & 8(c).

[98] Cybersecurity and Infrastructure Security Agency, *Binding Operational Directive 20-01*

[99] Cybersecurity and Infrastructure Security Agency. (n.d.). *CISA Coordinated Vulnerability Disclosure (CVD) Process*. Department of Homeland Security.https://www.cisa.gov/coordinated-vulnerability-disclosure-process.

[100] *Hack The Pentagon*. (n.d.). HackerOne. Retrieved March 8, 2021, from https://www.hackerone.com/hack-the-pentagon.

[101] Army Cyber Command. (2020, November 9). Hack The Army 3.0 furthers innovative bug bounty program to defend networks, data. United States Army. https://www.army.mil/article/240719/hack_the_army_3_0_furthers_innovative_bug_bounty_program_to_defend_networks_data.

[102] Athy, D. (2016, March). Department of Defense Announces Initiative for Vetted Hackers to Hack the Pentagon. *Synack*. https://www.synack.com/blog/hack-the-pentagon/; Kushto, G. (2016, September 22). Bug bounties: How federal agencies can learn from Apple. *GCN*. https://gcn.com/Articles/2016/09/22/Bug-bounty-program.aspx?m=1.

[103] DOD News. (2021, May 4). DOD Expands Hacker Program to All Publicly Accessible Defense Information Systems. *U.S. Department of Defense*. https://www.defense.gov/Explore/News/Article/Article/2595294/dod-expands-hacker-program-to-all-publicly-accessible-defense-information-syste/.

[104] Feldman, A., & Feola, A. (2020, December 14). TTS Bug Bounty Program: 3 Year Review. *Digital.Gov*. https://digital.gov/2020/12/14/tts-bug-bounty-program-3-year-review/.

[105] *H.R.7327—Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act*, Congress, 115th Congress (2017-2018) (2018) (testimony of Will Hurd). https://www.congress.gov/bill/115th-congress/house-bill/7327/text

[106] *H.R.5433—Hack Your State Department Act*, Congress, 115th Congress (2017-2018). https://www.congress.gov/bill/115th-congress/house-bill/5433

[107] *H.R.1668—IoT Cybersecurity Improvement Act of 2020*, Congress, 116th Congress (2019-2020) (2020). https://www.congress.gov/bill/116th-congress/house-bill/1668/text.

[108] The White House. (2021, May 12). *FACT SHEET: President Signs Executive Order Charting New Course to Improve the Nation's Cybersecurity and Protect Federal Government Networks*. The White House. https://wwwwhitehouse.gov/briefing-room/statements-releases/2021/05/12/fact-sheet-president-signs-executive-order-charting-new-course-to-improve-the-nations-cybersecurity-and-protect-federal-government-networks/.

[109] Ibid.

[110] Ibid.

[111] Marshall Jarrett, Michael W Bailie, Ed Hagen, & Scott Eltringham. (2010). *Prosecuting Computer Crimes*. Office of Legal Education Executive Office for United States Attorneys. https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf.

[112] Library of Congress. (1998). *The Digital Millennium Copyright Act of 1998: U.S. Copyright Office summary*. Washington, D.C.: Copyright Office, Library of Congress. https://www.copyright.gov/legislation/dmca.pdf.

[113] Cybersecurity Unit. (2017). *A Framework for a Vulnerability Disclosure Program for Online Systems*. U.S. Department of Justice. https://www.justice.gov/criminal-ccips/page/file/983996/download.

[114] *Van Buren v. USA*. US Supreme Court. (2021) https://www.supremecourt.gov/opinions/20pdf/19-783_k53l.pdf.

[115] Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies 2018, 83 FR 54010 (October 28, 2018) (to be codified at 37 CFR 201).https://www.federalregister.gov/documents/2018/10/26/2018-23241/exemption-to-prohibition-on-circumvention-of-copyright-protection-systems-for-access-control.

[116] H.R.7327 - 115th Congress (2017-2018): Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act. (2018, December 21). https://www.congress.gov/bill/115th-congress/house-bill/7327/text.

[117] Cybersecurity and Infrastructure Security Agency, *Binding Operational Directive 20-01*.

[118] Wasser, L. A., & Pennington, K. (2021). Cybersecurity 2021: Canada. *In International Comparative Legal Guide: Cybersecurity 2021* (4th ed.). Global Legal Group. http://mcmillan.ca/wp-content/uploads/2020/07/Lyndsay_Wasser-Kristen_Pennington_CYB21_Chapter-9_Canada.pdf.

[119] *R. v. Geller,* 2003 CanLII 31190 (ON SC), https://canlii.ca/t/1bx92

[120] Hadnagy, C. (2010). *Social Engineering: The Art of Human Hacking*. Wiley

[121] *Copyright Act*, RSC 1985, c C-42, section 41.13.

[122] *Copyright Act*, RSC 1985, c C-42, section 41.15.

[123] Martin-Bariteau, F. and Newman, V., *Whistleblowing in Canada. A Knowledge Synthesis Report* (February 15, 2018). Ottawa Faculty of Law Working Paper No. 2018-07.

[124] *Public Servants Disclosure Protection Act*, SC 2005, c 46, https://canlii.ca/t/54317 at paras 20(4) and 19.

[125] Martin-Bariteau, F. and Newman, V. (2018); *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5, para. 27.1

[126] Martin-Bariteau, F., Stevens, Y., & Tran, S. (2021, May). *See Something, Say Something? The State of Coordinated Vulnerability Disclosure in Canada's Federal Government*. NorthSec.

[127] Martin-Bariteau, F. and Newman, V., *Personal Information Protection and Electronic Documents Act*, 4.

[128] Canadian Digital Service & Office of the Chief Information Officer. (2020, July 31). *Vulnerability Disclosure Process for the COVID Alert service. GitHub*. https://github.com/cds-snc/covid-alert-documentation.

[129] Government of Canada. (2021). *Canadian Centre for Cyber Security*. https://cyber.gc.ca/en/.

[130] Public Safety Canada. (2019). *National Cyber Security Action Plan, 2019-2024*. 17. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2019/index-en.aspx; Public Safety Canada. (28 May 2019). National Cyber Security Strategy. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx.

[131] Treasury Board of Canada Secretariat. (2018). *Government of Canada Cyber Security Event Management Plan (GC CSEMP) 2019*. Government of Canada. https://www.canada.ca/en/government/system/digital-government/online-security-privacy/security-identity-management/government-canada-cyber-security-event-management-plan.html.

[132] Canadian Centre for Cyber Security. (n.d.). *Alerts & Advisories*. Communications Security Establishment. https://cyber.gc.ca/en/alerts-advisories.

[133] Canadian Centre for Cyber Security. (n.d.). *Glossary*. Communications Security Establishment. https://cyber.gc.ca/en/glossary.

[134] Canadian Centre for Cyber Security. (n.d.). *Report a Cyber Incident*. Communications Security Establishment. https://cyber.gc.ca/en/incident-management.

[135] Canadian Centre for Cyber Security. (2018, August 15). *Canadian Centre for Cyber Security*. Canadian Centre for Cyber Security. https://web.archive.org/web/20210427205257/https://cyber.gc.ca/en/

[136] Canadian Centre for Cyber Security. (2021, February 16). *Canadian Centre for Cyber Security*. Canadian Centre for Cyber Security. https://cyber.gc.ca/en/

[137] Canadian Centre for Cyber Security. (2021, May 12). *Canadian Centre for Cyber Security*. Canadian Centre for Cyber Security. https://cyber.gc.ca/en/.

[138] Government of Canada. (10 March 2020). *Department of National Defence and the Canadian Armed Forces 2020-21 Departmental Plan*. 8-9. https://www.canada.ca/en/department-national-defence/corporate/reports-publications/departmental-plans/departmental-plan-2020-21-index.html.

[139] Government of Canada, *Department of National Defence and the Canadian Armed Forces 2020-21 Departmental Plan*, 57.

[140] Government of Canada. (2015). "Cyber and Information Technology Security." *Shared Services Canada*. https://www.canada.ca/en/shared-services/corporate/cyber-information-technology-security.html.

[141] Berthiaume, L. (2021, January 5). "Poor IT Support Hurts Canadian Military Operations, Internal Review Finds." *National Observer*. https://www.nationalobserver.com/2021/01/05/news/technology-support-canadian-military-operations-internal-review-Canadian-armed-forces-defence-canada-computers.

[142] Bharti, B. (12 April 2021). "Federal Government Signs Deal with BlackBerry to Use Its Cybersecurity Tools." *Financial Post*. https://financialpost.com/news/federal-government-signs-deal-with-blackberry-to-use-its-cybersecurity-tools.

[143] Parliament of Canada. (4 February 2019). "Standing Committee on Public Safety and National Security." *Number 147, 1st Session, 42nd Parliament*. https://www.ourcommons.ca/DocumentViewer/en/42-1/SECU/meeting-147/evidence.

[144] Ibid.

[145] Treasury Board of Canada Secretariat. (n.d.). *Government of Canada Cyber Security Event Management Plan (GC CSEMP) 2019*. Government of Canada. https://www.canada.ca/en/government/system/digital-government/online-security-privacy/security-identity-management/government-canada-cyber-security-event-management-plan.html.

[146] Canadian Centre for Cyber Security. (2021, March 2). *Active Exploitation of Microsoft Exchange Vulnerabilities - Update 4*. Communications Security Establishment. https://cyber.gc.ca/en/alerts/active-exploitation-microsoft-exchange-vulnerabilities.

[147] Communications Security Establishment. (n.d.). *CSE's Equities Management Framework*. Government of Canada. https://archive.is/jDKbU.

[148] Electronic Privacy Information Center. (n.d.). *Vulnerabilities Equities Process*. Electronic Privacy Information Center. https://epic.org/privacy/cybersecurity/vep/

[149] Electronic Privacy Information Center, *Vulnerabilities Equities Process*.

[150] Kenway, J., Sugihara, M., Zilberfarb, A., & Tortolero, P. (2021). *More Sunlight, Fewer Shadows: Guidelines For Establishing & Strengthening Government Vulnerability Disclosure Policies*. Center for Cybersecurity Policy and Law, 1-20. https://www.cyberthreatalliance.org/wp-content/uploads/2021/02/More_Sunlight_Fewer_Shadows.pdf

[151] CSE [@cse_cst]. (2019, March 8) Today, CSE has published our Equities Management Framework for the first time [Tweet]. Twitter. https://twitter.com/cse_cst/status/1104088450935021570.

[152] Timberg, C., & Nakashima, E. (2017, May 16). NSA officials worried about the day its potent hacking tool would get loose. Then it did. *The Washington Post*. https://www.washingtonpost.com/business/technology/nsa-officials-worried-about-the-day-its-potent-hacking-tool-would-get-loose-then-it-did/2017/05/16/50670b16-3978-11e7-a058-ddbb23c75d82_story.html.

[153] Healey, J. (2016). The U.S. Government and Zero-Day Vulnerabilities: From Pre-Heartbleed to Shadow Brokers. *Columbia Journal of International Affairs*, 1-20. https://jia.sipa.columbia.edu/online-articles/healey_vulnerability_equities_process.

[154] Fruhlinger, J. (2018, August 30). What is WannaCry ransomware, how does it infect, and who was responsible? *CSO*. https://www.csoonline.com/article/3227906/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html

[155] Kaspersky. (n.d.). *What is WannaCry ransomware?* Kaspersky. https://www.kaspersky.com/resource-center/threats/ransomware-wannacry.

[156] Perlroth, *This Is How They Tell Me the World Ends*.

[157] Kenway, J., & Garcia, M. (2021, June 1). *To Patch or Not to Patch: Improving the US Vulnerabilities Equities Process*. Third Way. https://www.thirdway.org/memo/to-patch-or-not-to-patch-improving-the-us-vulnerabilities-equities-process

[158] Cybersecurity and Infrastructure Security Agency, *Binding Operational Directive 20-01*; Cybersecurity and Infrastructure Security Agency, *CISA Coordinated Vulnerability Disclosure (CVD)*.

[159] The White House. (2017, November 15). *Unclassified Vulnerabilities Equities Policy and Process for the United States Government*. Trump White House Archives. https://trumpwhitehouse.archives.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF.

[160] Government Communications Headquarters. (2018, November 29). *The Equities Process*. GCHQ. https://www.gchq.gov.uk/information/equities-process.

[161] Parsons, C. (2021, March 29). Christopher Parsons Delivers Testimony to Special Committee on Canada-China Relations. *The Citizen Lab*. https://citizenlab.ca/2021/03/christopher-parsons-delivers-testimony-to-special-committee-on-canada-china-relations/.

[162] Communications Security Establishment, *CSE's Equities Management Framework*.

[163] Ibid.

[164] For cases where the court attempted to interpret both of these terms, see for example: *R v McNish*, 2020 ABCA 24, *R v Horse*, 2019 SKCA 56, R. c. Parent, 2012 QCCA 1653, *R v Braile*, 2018 ABQB 361, *R. v. Senior*, 2021 ONSC 272. For cases where the court attempted to interpret the term "fraudulently," see, for example: *U.S.A. v. Su Bin*, 2015 BCSC 1586, *R. v. Alexander*, 2006 CanLII 26480, *R. v. R.J.S.*, 2010 NSSC 253. For cases where the court attempted to interpret the term "colour of right," see, for example: O'Brien I.M.G. (Master Corporal), *R. v.*, 2015 CM 1013, *R. v. Livingston*, 2018 ONCJ 25, R. c. St-Martin, 2012 QCCQ 575, R. c. Lauzon, 2013 QCCQ 5060.

[165] *R v McNish*, 2020 ABCA 249 (CanLII) at para 63; Thibodeau c. R., 2018 QCCA 1476 (CanLII) at paras 12-13.

[166] Public Prosecution Service of Canada. (2018, December 8). *5.12 Prosecutions involving Non-Disclosure of HIV Status*. Public Prosecution Service of Canada. https://www.ppsc-sppc.gc.ca/eng/pub/fpsd-sfpg/fps-sfp/tpd/p5/ch12.html

[167] Public Prosecution Service, *OM-beleidsbrief Coordinated Vulnerability Disclosure*.

[168] Cybersecurity Unit Computer Crime & Intellectual Property Section. (2017, July). *A Framework for a Vulnerability Disclosure Program for Online Systems*. U.S. Department of Justice. https://www.justice.gov/criminal-ccips/page/file/983996/download.

[169] Cybersecurity and Infrastructure Security Agency. (n.d.). *Vulnerability Disclosure Policy Template*. Department of Homeland Security. https://cyber.dhs.gov/bod/20-01/vdp-template/.

[170] Woszczynski, A., Green, A., Dodson, K., & Easton, P. (2020). Zombies, Sirens, and Lady Gaga – Oh My!

[171] Bannister, A. (2021, May 5). US Department of Defense expands vulnerability disclosure program. *The Daily Swig*. https://portswigger.net/daily-swig/us-department-of-defense-expands-vulnerability-disclosure-program

[172] *Vulnerability Co-ordination Pilot*. (2017, March 13). The National Cyber Security Centre. https://www.ncsc.gov.uk/blog-post/vulnerability-co-ordination-pilot; *NCSC Vulnerability Disclosure Co-ordination*. (2018, October 19). The National Cyber Security Centre. https://www.ncsc.gov.uk/blog-post/ncsc-vulnerability-disclosure-co-ordination; Hack the Gov't and Tell the NCSC? You'll Now Get a Pat on the Back. Tech Monitor. (2018, December 21). https://techmonitor.ai/techonology/cybersecurity/ncsc-vulnerability-reporting.

[173] Householder, Wassermann, Manion, & King, *The CERT Guide to Coordinated Vulnerability Disclosure*.

[174] Woszczynski, Green, Dodson & Easton, Zombies, Sirens, and Lady Gaga – Oh My!

[175] Zhao, M., Laszka, A., & Grossklags, J. (2017). Devising Effective Policies for Bug-Bounty Platforms and Security Vulnerability Discovery. *Journal of Information Policy, 7*. https://doi.org/10.5325/JINFOPOLI.7.2017.0372.

[176] National Institute of Standards and Technology. (2018). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1* (NIST CSWP 04162018; p. NIST CSWP 04162018). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.04162018

[177] International Organization for Standardization. (2018, October 23). *Information technology — Security techniques — Vulnerability disclosure* (ISO/IEC 29147:2018). https://www.iso.org/standard/72311.html; International Organization for

Standardization (2013). *Information technology — Security techniques — Vulnerability handling processes International Standard* (ISO/IEC 30111). https://www.iso.org/standard/69725.html

[178] Woszczynski, Green, Dodson & Easton, Zombies, Sirens, and Lady Gaga – Oh My!

[179] Athy, Department of Defense Announces Initiative for Vetted Hackers to Hack the Pentagon; Kushto, Bug bounties: How federal agencies can learn from Apple.

[180] Ellis, R., Moussouris, K., & Stevens, Y. (2020, January 10). *Emailed comments from Ryan Ellis, Katie Moussouris, Yuan Stevens · Issue #133 · cisagov/cyber.dhs.gov.* https://github.com/cisagov/cyber.dhs.gov/issues/133

[181] *IT-Sicherheitsforschende (Finder)*. (n.d.). Bundeswehr. https://www.bundeswehr.de/de/security-policy/danksagung.

[182] Ellis, R., Huang, K., Siegel, M., Moussouris, K., & Houghton, J. (2018). CHAPTER 4 Fixing a Hole: The Labor Market for Bugs. In H. Shrobe, D. L. Shrier, & A. Pentland (Eds.), *New Solutions for Cybersecurity* (pp. 129–159). MIT Press. http://ieeexplore.ieee.org/document/8333100.

[183] *Industrial Control Systems.* (n.d.). Cybersecurity & Infrastructure Security Agency. Retrieved June 14, 2021, from https://us-cert.cisa.gov/ics.

[184] Canadian Centre for Cyber Security, *Alerts & Advisories.*

[185] Horne, B. (2014). On Computer Security Incident Response Teams. *IEEE Security Privacy*, 12(5), 13–15. https://doi.org/10.1109/MSP.2014.96.

[186] *Authorization to Use the CERT Mark. (n.d.)*. Software Engineering Institute. Retrieved March 9, 2021, from https://www.sei.cmu.edu/education-outreach/license-sei-materials/authorization-to-use-cert-mark/index.cfm

[187] Kelty, C. (2011). The Morris Worm. *Limn*, 1(1). https://escholarship.org/uc/item/8t12q5bj.

[188] Horne, On Computer Security Incident Response Teams.

[189] Carpenter, J. J. (2008). *CERT Overview.* https://www.sis.pitt.edu/jjoshi/courses/IS2150/Fall08/CertOverview.pdf.

[190] Ruefle, R. (2007). *Defining Computer Security Incident Response Teams*. Software Engineering Institute, Carnegie Mellon University. https://resources.sei.cmu.edu/asset_files/WhitePaper/2007_019_001_294579.pdf.

[191] Communications Security Establishment. (2020, October 27). *Authorities and Capabilities for CSE*. https://cse-cst.gc.ca/en/corporate-information/mandate; Maurer, T., Hohmann, M., Skierka, I., & Morgus, R. (2015). National CSIRTs and Their Role in Computer Security Incident Response [White paper]. New America. https://www.newamerica.org/cybersecurity-initiative/policy-papers/national-csirts-and-their-role-in-computer-security-incident-response/.

[192] Joint Task Force Transformation Initiative. (2013). *Security and Privacy Controls for Federal Information Systems and Organizations* (NIST SP 800-53r4; p. NIST SP 800-53r4). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r4

[193] Joint Technical Committee ISO/IECJTC1. (2018). *ISO/IEC 29147:2018 Information technology—Security techniques—Vulnerability disclosure*. ISO/IEC. https://www.iso.org/obp/ui/es/#iso:std:iso-iec:29147:ed-2:v1:en

[194] Ibid.

[195] Pupillo, Ferreira & Varisco, *Software Vulnerability Disclosure in Europe*, 5.

[196] Ibid.

[197] Householder, Wassermann, Manion, & King, *The CERT Guide to Coordinated Vulnerability Disclosure.*

[198] Ibid, 43.

[199] Ibid.

[200] Kenway, Sugihara, Zilberfarb & Tortolero, *More Sunlight, Fewer Shadows.*

[201] The White House, *Unclassified Vulnerabilities Equities Policy and Process for the United States Government.*

[202] *The Equities Process*. (2018, November 29). GCHQ. https://www.gchq.gov.uk/information/equities-process.

[203] Communications Security Establishment. (n.d.). *CSE's Equities Management Framework*