Recommendations to Improve the Resilience of Canada's Digital Supply Chain

KEY PRACTICES, TECHNOLOGY OVERVIEW AND RECOMMENDATIONS FOR INDUSTRY AND GOVERNMENT

Version 01 – JUNE 3, 2022

AUTHORED BY:

Supply Chain Assurance Working Group (SCAWG)
of the Canadian Forum for Digital Infrastructure Resilience (CFDIR)

TLP:WHITE

The contents of this document are **TLP:WHITE**

Table of Contents

ACKNOWLEDGEMENTS

The information and recommendations contained herein were informed by the active participation and engagement of subject matter experts from the following organizations (listed alphabetically):

CFDIR MEMBERS

Accenture; BlackBerry; Canadian Centre for Cyber Security (CCCS); Innovation, Science, and Economic Development (ISED); Palo Alto Networks; Trend Micro Inc.

NON-CFDIR SUPPLY CHAIN ASSURANCE WORKING GROUP PARTICIPANTS

Shared Services Canada (SSC)

REVISION HISTORY

The following table describes the dates of the major changes to this document.

Authors	Date / Version	Notes
CFDIR SCAWG Participants, (January 2021 – June 2022)	JUNE 3, 2022 / v.01	Initial version of recommendations and key practices

1.0 INTRODUCTION

1.1 OVERVIEW

Fostering a secure, resilient digital supply chain is a key focus area for the Government of Canada and governments around the world. And rightly so. Utilizing the scale and resources of third-party suppliers and services, integrated across both hardware and software development lifecycles, Information and Communications Technology (ICT) organizations can maximize efficiency and productivity to deliver critical technology capabilities. Rarely are today's ICT tools and services built solely by a single team in a Canadian location by Government of Canada-screened developers, rather the tools and services are constructed by international teams with hardware and software elements sourced globally. End products, similarly, contain a variety of technology components sourced and licensed from a variety of third parties. Yet, the very interconnectedness of global supply chains that enables this productivity presents serious cybersecurity risks. Malicious actors can take advantage of the scale and complexity of these supply chains, exploiting vulnerabilities in third-party suppliers to disrupt, degrade, or exfiltrate sensitive data in end-user networks. In short, ICT providers are now responsible not only for the security of their own products and services, but must also have confidence in the security and resilience of their entire supplier network, including their suppliers' suppliers.

Supply chain resilience is of course not a new concept. Governments and organizations have collaborated for decades on best practices and other actions designed to promote hardware and software integrity. Despite these efforts, however, the supply chain compromise attack on network management provider SolarWinds that came to light in December 2020 was a watershed moment. In that incident, a malicious actor took advantage of trusted supply chain processes to obtain security credentials and access data of some of SolarWinds' most sensitive customers' networks, including critical infrastructure companies and important U.S. federal government agencies. In the aftermath of this incident, it is clear that government and industry should continue to move with urgency to address existing gaps.

With this backdrop, the Canadian Forum for Digital Infrastructure Resilience (CFDIR) convened a Working Group to identify actionable recommendations for Canada's federal government and critical infrastructure sectors to improve supply chain assurance. The Working Group reviewed global supply chain risk management (SCRM) activities and programs; reviewed lessons learned from significant events such as the SolarWinds supply chain compromise as well as important vulnerability remediation efforts like the Log4Shell remote code execution vulnerability; and received presentations from key agencies on current activities. Ultimately, the Working Group seeks to address this problem statement:

What steps can government and industry collectively take to promote confidence in a secure, resilient digital supply chain for Canada?

1.2 EXECUTIVE SUMMARY

This review is divided into three parts.

In Section 2, the Working Group reviewed actions taken in Canada and key global governments to promote strong governance principles for supply chain risk management. This section reviews current supply chain assurance actions within the Government of Canada, focused on the Supply Chain Integrity review process led by Shared Services Canada and the Canadian Centre for Cyber Security. It also highlights legal authorities, regulatory actions, and partnership activities currently underway in the United States, United Kingdom, and European Union, designed to promote confidence in a secure, resilient digital supply chain by enhancing collaboration and coordination across government agencies and with non-government partners. For instance, the United States government's *National Cyber Strategy* incorporates supply chain risk management as a key tenet, and building on a legal foundation that provides authorities to the U.S. to remove or exclude technology from government networks based on supply chain risk, promote best practice adoption, and share risk information with private industry partners.

The Working Group reviewed important success factors for strong governance, and identified opportunities for enhanced coordination and engagement with relevant stakeholders. In particular, the Working Group found that whole-of-government alignment is critical for ensuring the disparate agencies of the Government of Canada are aligned in their focus and actions to mitigate digital supply chain risks, and for providing a centralized point of contact for outreach and collaboration with Provincial, Territorial, Municipal governments, critical infrastructure owners and operators and their key suppliers, academia and international digital supply chain risk management efforts.

> **Section 2 recommends that the Government of Canada should develop a coordinated vision, strategy, and action plan for Canada's digital supply chain risk management activities, including opportunities for enhanced collaboration across federal agencies and engagement with non-governmental stakeholders and guidance to non-government stakeholders on the key activities and points of contact for relevant government agencies.**

Section 3 identifies digital supply chain defence strategies and technology capabilities that can promote confidence in a secure and resilient supply chain. While strong governance is an important foundation for securing the digital supply chain, state-of-the-art technology should also be brought to bear. This section draws on lessons from significant use cases: the SolarWinds supply chain compromise and the Log4Shell vulnerability. It then identifies vendor-agnostic defence strategies and key technologies that could help prevent or mitigate attacks or lessen the impact of those that are initially successful.

Key digital supply defence strategies seek to promote adoption of zero trust architectures, secure development lifecycles, software composition analysis tools, and other transparency initiatives. State-of-the-art technologies take advantage of advances in AI/ML to automate key

response activities, understand baseline risk by identifying vulnerable internet-accessible systems and assets, and test and verify secure software environments.

> **Section 3 recommends that the Government of Canada review existing government-wide security architectures and technical reference requirements, and update as appropriate to account for critical system defence strategies, practices and technology capabilities that could prevent, mitigate, or lessen the impact of supply chain attacks or vulnerabilities. Once completed, those architectures and reference requirements should be disseminated to industry as models for adoption, to the extent feasible and scalable.**

Section 4 identifies key digital supply chain risk management practices for organizations to implement. A number of best practices for digital supply chain assurance have been previously documented by governments and industry partners around the world. Thus, this section does not exhaustively catalogue all supply chain risk management practices. However, it is important to identify the key concepts and principles derived from existing bodies of work and identify opportunities to further implement these principles in industry and government organizations.

The practices identified in this section are key confidence indicators for instituting a secure, sustainable, and resilient ICT Supply Chain Risk Management program. This section highlights the importance of instituting a formal risk management program across the organization, and integrating a product's lifecycle with security and integrity practices at each stage. This section also highlights the importance of organizations understanding the totality of their supply chain, and closely collaborating with key upstream and downstream suppliers and consumers to assess, monitor and respond to risks proactively. Mechanisms for evaluating and assessing these practices will ensure resources are appropriately managed and deployed.

Section 4 includes recommendations for industry and for government.

> **For industry, the Working Group recommends that ICT organizations should begin preparing now to meet coming supply chain requirements. Industry ICT suppliers will need to be able to explain, defend, show auditable evidence of, and effectively operate a maturing supply chain risk management process and related practices that address well-known supply chain and asset management issues within their control.**
>
> **Additionally, industry should review their 2-5 year technology and risk management plans to ensure they are adopting appropriate key confidence indicators for supply chain risk management commensurate with the organization's maturity and risk profile, and taking advantage of the new technologies and innovations in the space to help meet future supply chain attestation requirements and/or mitigate supply chain incidents.**

While the responsibility is on individual industry organizations to adopt and implement key practices for confidence in their own supply chains, the Working Group also identified actions the Government of Canada could consider taking that would facilitate adoption.

For government, Section 4 recommends collaborations with industry on future projects to:

- **Develop and disseminate easily-implementable guidance for small and medium businesses;**
- **Develop a "maturity model" framework for organizations to make resource decisions about their supply chain assurance programs tailored to their risk profile and encourage knowledge sharing;**
- **Utilize policy levers to drive adoption of key practices by ICT suppliers to the government, such as through qualified procurement actions; and**
- **Develop a set of supply chain risk assessment requirements, questionnaire, and related scoring rubric.**

1.3 SCOPE AND FUTURE ACTIONS

The Working Group has focused its initial review on opportunities to better secure and promote confidence in the digital ICT supply chain across the Government of Canada and critical infrastructure sectors. As noted above, recommendations aligned to this scope, for both government and industry, include adopting strong governance principles, adopting defence strategies and key technologies, and adopting risk management best practices.

The Working Group also identified future lines of effort related to promoting confidence in the security of Canada's digital ICT supply chains. Future work, aligned to the recommendations in Section 4, could include:

- Development of a "maturity model" for organizations, especially small and medium-sized businesses, to make resource decisions about their supply chain assurance programs based on their own maturity and risk profile;
- Development of actionable, targeted guidance to small and medium-sized businesses; and
- Identifying policy levers that would further incentivize key practice adoption by the government's ICT suppliers.

Beyond the resilience of the digital supply chain, additional future studies could also review important issues related to the *industrial* supply chain, such as a review and recommendations for alleviating Canadian impacts from the ongoing global semiconductor chip shortage.

1.4 STAKEHOLDERS AND TARGET AUDIENCE

The very interconnectedness of global supply chains means that every ICT consumer and supplier has a stake in a secure, resilient supply chain. Even narrowing the scope of this report to government and ICT critical infrastructure sectors still captures a large section of the Canadian economy. While we believe all of these organizations would gain from reviewing this report and adopting its recommendations, the key target audience is Federal government

agencies that play a role in supply chain risk management, as well as key ICT suppliers to the government and critical infrastructure sectors. (In general, in this paper "industry organizations" refers to these ICT suppliers to the government and critical infrastructure).

Among the key federal stakeholders are Innovation, Science and Economic Development Canada, the Canadian Centre for Cyber Security, Public Safety Canada, Shared Services Canada, Treasury Board Secretariat, Public Services and Procurement Canada, and the Privy Council Office; these government agencies have a range of unique mandates and resources that collectively support a secure and resilient supply chain, and can leverage operational, policy, and collaboration authorities in service of that goal. For key ICT suppliers, the overarching findings of the report are applicable to businesses of all sizes and resources, upstream and downstream, but, as noted above, future work could place particular emphasis on the needs of small- and medium-sized businesses.

2.0 CURRENT SUPPLY CHAIN GOVERNANCE ACTIONS

The Working Group reviewed actions currently underway in key countries designed to promote confidence in a secure, resilient digital supply chain, emphasizing that technology capabilities are important but not the only element of strong risk management. These activities encompass a mix of legal authorities, regulatory actions, and partnership programs. In particular, this review focused on the important role that strong governance plays in ensuring positive policy outcomes, especially in areas - like supply chain risk management - where multiple government entities each bring to bear their own unique mandates, authorities, resources, and activities in service of the common goal.

A key finding of this governance review is that many government entities around the world utilize a coordinated model of governance, whereby individual government agencies undertake supply chain risk management activities on their own, aligned to their own mandates and resources, with varying degrees of coordination with other relevant agencies. In such cases, the important success factors are: 1) whether and to what extent the individual agencies are operating under a unified strategy and vision, with a defined action plan; 2) the extent to which each relevant agency is aware of and able to complement other agencies' activities in a coordinated manner; and 3) the extent to which the coordinating structure enables collaboration with other government and non-government partners.

A brief review of global governance activities - in the United States, United Kingdom, European Union, and Canada - shows a number of illustrative supply chain risk management actions aligned to these three principles, but also shows opportunities for enhanced coordination, further alignment to overarching strategy, and opportunities to engage critical infrastructure sectors.

2.1 REPRESENTATIVE GLOBAL GOVERNANCE ACTIONS – UNITED STATES

A review of global government actions to mitigate digital supply chain risks shows the importance of governance success factors. For instance, in the United States, the 2018 *National Cyber Strategy* identified supply chain risk management as a key tenet of improving the federal government's cyber resilience.[i] The strategy built on a legal foundation that provides authorities to the U.S. government to remove or exclude technology from government networks based on supply chain risk, promote best practice adoption, and share risk information with private industry partners.[ii] Subsequently, the U.S. announced other legal and policy activities designed to limit actions the government considered risky, including a ban on the government or its contractors using certain risky telecommunications equipment (from Huawei, ZTE, or their affiliates) as a substantial component of any information system.

These strategy, legal, and policy actions are designed to foster close collaboration across U.S. federal agencies. For example, a 2019 Presidential action [iii], still in force at this time, requires the U.S. Department of Commerce to review national security risks related to companies' acquisition of ICT, and take mitigative action if the technology is controlled by or subject to the jurisdiction of foreign adversaries. That review requires coordination with the U.S. Department

of Homeland Security for an ICT risk assessment and with the U.S. intelligence community for a global threat assessment.

Finally, the U.S. has also developed a robust coordination mechanism with non-federal partners. In 2018, the U.S. government established a joint industry-government ICT Supply Chain Risk Management Task Force.[iv] The Task Force's mandate is to identify and develop public-private partnership strategies and deliverables to enhance ICT Supply Chain security. Since its inception, the group has reviewed legal obstacles to sharing supply chain risk information between government and industry; evaluated supply chain threats to suppliers, with mitigation measures for the corresponding threat scenarios; developed criteria and recommendations for utilizing Qualified Bidder/Manufacturer lists during the procurement process to drive down supply chain risks; and developed guidance specific to managed service providers and to small and medium businesses, among other actions.

2.2 REPRESENTATIVE GLOBAL GOVERNANCE ACTIONS – UNITED KINGDOM

As with the United States, the UK released a National Cyber Strategy in late 2021.[v] The strategy includes actions to mitigate systemic risks to digital supply chains by mapping dependencies across national critical infrastructure, identifying where digital supply chains are too concentrated, and working with international partners to manage collective risks, including via regulatory action.

This strategy builds on significant ongoing collaboration across government agencies, such as the Centre for the Protection of National Infrastructure (CPNI), and the National Cyber Security Centre's leadership in disseminating guidance and principles for effective control and oversight of supply chain risk management, as well as a supplier assurance framework released through the Cabinet Office.

The UK is also reviewing policy levers to drive industry behavior. In 2021, the Department for Digital, Culture, Media & Sport began a process to develop policy solutions for supplier cyber risk management, seeking input on how organisations manage supply chain cyber risk and whether additional government intervention would enable organisations to manage these risks more effectively, with a specific focus on managed service providers.

2.3 REPRESENTATIVE GLOBAL GOVERNANCE ACTIONS – EUROPEAN UNION

Similar to the United States and United Kingdom, the EU has taken action to incorporate supply chain security into its legislative toolkit. Insofar cybersecurity is concerned, the EU Commission has introduced supply chain security requirements within the ongoing review of the Network and Information Directive (NIS 2).[vi] Specifically, the new rules would require all critical operators and key ICT security providers to implement supply chain management practices, including "security-related aspects concerning the relationships between each entity and its suppliers or service providers such as providers of data storage and processing services or managed security services". Further guidance on the implementation criteria and enforcement is delegated to the national competent authorities in the EU Member States.

In addition, the EU Commission and the EU Member States have agreed to a joint toolbox of mitigating measures and addressing security risks related to the rollout of 5G.[vii] The Member States have identified risks and vulnerabilities at the national level and published a joint EU risk assessment. Through the toolbox, the Member States are committing to move forward in a joint manner based on an objective assessment of identified risks and proportionate mitigating measures. With its communication, the Commission is launching relevant actions within its competence and called for key measures to be put in place.

Additional work on supply chain in being carried out through other workstreams such as the EU Agency for Cybersecurity (ENISA). Its publication, "Threat Landscape for Supply Chain Attacks," analyzes prominent supply chain attack incidents and provides recommendations for managing the relationship to suppliers, ensuring the secure development of products and services and implementing good practices for vulnerability management.[viii]

2.4 REPRESENTATIVE GLOBAL GOVERNANCE ACTIONS – CANADA

Like its partners in the United States, United Kingdom, and the EU, the Government of Canada has taken significant steps to incorporate key governance success factors into its supply chain risk management practices, including actions to promote confidence in its ICT procurements, and guidance to promote strong risk management practices within both the critical infrastructure and small and medium business communities.

The Federal government is especially strong at collaborating across Federal agencies. For instance, Shared Services Canada (SSC), in coordination with the Communications Security Establishment (CSE), operates the Supply Chain Integrity (SCI) [ix] process, to "ensure that no untrusted equipment, software or services are procured by SSC and are used in the delivery and support of GC services." Bidders to technology procurements in four areas - email, data centres, networks, and workplace technology devices - provide product lists, network diagrams, and subcontractor lists for assessment of potential risks to national security. On a procurement-by-procurement basis, and based on guidance from CSE, Shared Services may require mitigation measures to address supply chain concerns. Once a contract bidder has been approved through this process, no technology modifications are permitted except under exceptional circumstances.

Federal agencies have also sought to use available policy levers to manage risk. Public Services and Procurement Canada (PSPC) contracts require contracting clauses for telecommunications equipment and services, especially managed telecommunications service, designed to protect the integrity, availability and confidentiality of Canada's data and communications by applying security acknowledgements and assurances in these contracts to prevent or to mitigate supply chain risks. In general, these security clauses acknowledge that Canada requires comprehensive security measures in telecommunications services and equipment, and commit contractors to implementing reasonable protection measures to achieve the highest possible levels of data protection.

Canadian government entities likewise have a good track record of identifying opportunities to collaborate with non-Federal partners, and provide timely and relevant risk-based information.

CFDIR is an excellent example of this collaboration, bringing together industry and multiple government agencies. Additionally, the Canadian Centre for Cyber Security (CCCS) regularly issues guidance and threat alerts related to supply chain incidents, and regularly highlights risks to supply chain exploitation in its National Cyber Threat Assessments.[x]

Through the G7 Declaration of Digital and Technology Ministers on April 28, 2021, Canada committed to a framework for collaboration on digital technical standards, and discussions for promoting a more "secure, resilient, diverse, competitive, transparent and sustainable digital and ICT infrastructure supply chain." [xi] Such an approach must encourage innovation while enhancing security measures for ICT products and services.

While the Government of Canada's activities represent a solid foundation of managing risks to the digital supply chain, opportunities exist to expand and build on these actions to broaden their impact. For instance, ISED, which has a robust private sector collaboration mechanism, could work with key private sector partners to understand their risk information priorities, and collaborate with CSE and CCCS to incorporate those priorities into future guidance and alert products. Public Safety Canada, which did well to highlight supply chain risks in its *Action Plan for Critical Infrastructure* [xii], could identify specific policy levers that might mitigate those risks, such as incorporating supply chain elements into the grants it provides through the Cyber Security Cooperation Program.[xiii] Overall, these activities would benefit from the development of a unified, government-wide strategy and action plan dedicated specifically to mitigating digital supply chain risks. Such a strategy would align and focus current efforts, identify new collaboration opportunities, recommend new resources or policies if needed, and engage whole-of-nation stakeholders, including Provincial, Territorial, Municipal (PTM) governments, small/medium businesses, and critical infrastructure entities. It could also align and review lessons learned from approaches that blend supply chain assurance processes with broader IT security standards, such as is currently being undertaken by industry alliances and other communities of interest.[xiv]

2.5 KEY FINDINGS AND RECOMMENDATION

The Working Group found that whole-of-government alignment is critical for ensuring the disparate agencies of the Government of Canada are aligned in their focus and actions to mitigate digital supply chain risks, and for providing a centralized point of contact for outreach and collaboration with Provincial, Territorial, Municipal governments, critical infrastructure owners and operators and their key suppliers, academia and international digital supply chain risk management efforts.

Recommendation: **The Government of Canada should develop a coordinated vision, strategy, and action plan for Canada's digital supply chain risk management activities, including opportunities for enhanced collaboration across federal agencies and engagement with non-governmental stakeholders and guidance to non-government stakeholders on the key activities and points of contact for relevant government agencies.**

3.0 KEY DIGITAL SUPPLY CHAIN DEFENCE STRATEGIES AND TECHNOLOGICAL CAPABILITIES

A whole-of-government approach aligned to a unified governance strategy is just one element of secure supply chain foundation. In addition to adopting key best practices (*Section 4*), state-of-the-art technology can also be brought to bear. This section will identify the cyber defence strategies and key technologies that, taken together, could help prevent or mitigate attacks or lessen the impact of those that are initially successful. This section will not identify specific vendors or products; rather, it will focus on vendor-agnostic capabilities and toolsets to promote confidence in secure and resilient operations. While all of these technologies have use cases beyond preventing or mitigating supply chain attacks, in this section we focus specifically on their applicability to the supply chain context.

3.1 LESSONS FROM SIGNIFICANT INCIDENTS

The NIST SP 800-161 [xv] risk management framework for supply chain cybersecurity guides threat scenario identification, risk analysis, risk response strategy development, applicable controls determination and evaluation for continuous improvement. The risk exposure framework provides six supply chain scenarios and their risk assessment and mitigation: 1) Influence or Control by Foreign Governments Over Suppliers; 2) Telecommunications Counterfeits; 3) Industrial Espionage; 4) Malicious Code Insertion (such as the SolarWinds incident); 5) Unintentional Compromise; and 6) Vulnerable Reused Components Within Systems (such as Log4J open-source software).

Within these scenarios, two recent significant events - the SolarWinds supply chain compromise (Malicious Code Insertion) and the Log4Shell vulnerability (Vulnerable Reused Components Within Systems) - highlight specific use cases for key network defense strategies and technology capabilities.

3.1.1 SOLARWINDS SUPPLY CHAIN COMPROMISE

In late 2020, a significant cyber incident was discovered, impacting enterprise networks primarily in United States federal, state, and local governments, as well as critical infrastructure entities and other private sector organizations. The attack exploited the SolarWinds Orion platform and other information technology infrastructures, and the U.S. government attributed the intrusion to the Russian Foreign Intelligence Service.[xvi]

The SolarWinds attack, which the U.S. government called a "grave risk" to its national security, took advantage of trusted supply chain processes by gaining access to and exploiting the process by which SolarWinds provided software updates to its customer base. The adversary compromised SolarWinds' build system and successfully injected malicious code into regular software updates for its network management tools widely deployed in private and public sectors, evading detection. Software update patches are of course very common, a regular occurrence designed to ensure technologies are operating as efficiently or securely as possible. Exploiting this "trusted" update set off a series of steps that enabled the malware to obtain security credentials, and access victim data stored on premise and in the cloud. The adversary

selected high profile victims and used the malicious code to insert additional malware for data exfiltration. Both sets of malicious code were carefully crafted to avoid detection for an extended period of time, which ultimately enabled the malicious actor to gain access to many of SolarWinds' most sensitive customers' networks, including important U.S. government agencies.

The nature of this supply chain attack presents several important lessons, including the imperative for suppliers to secure their development and build practices. There are also specific takeaways for technology capabilities that can be brought to bear. In this instance, many foundational cybersecurity network architectures are predicated on stopping already-known threats. These "signature-based" defenses watch network traffic in real-time to prevent threats – so long as the threats have been pre-identified as a malicious action. Such defenses are important, but insufficient. In fact, the only cyber capability known to have mitigated aspects of the SolarWinds attack used behavioral analytics capabilities rather than signature-based detection. That is, instead of looking for specific, known, bad actions, the technology looked for anomalous behavior and, upon seeing it, prevented further action – and thus stopped the attack from progressing.[xvii] The overarching lesson is that today's risk environment, coupled with complex network environments, does not, broadly, lend itself to reliance solely or exclusively on traditional perimeter-based defenses. For sophisticated attacks like this one, defense in depth utilizing state-of-the-art technologies is an important strategy. This includes key defense strategies such as adopting zero trust architectures and secure software development lifecycles, as well as key technology capabilities that can detect anomalous network behavior and automate defensive capabilities for vulnerability management, threat hunting, and incident response (*Sections 3.2 and 3.3 provide more detail on these key strategies and technologies*).

3.1.2 LOG4SHELL REMOTE CODE EXECUTION VULNERABILITY

Log4J is a widely used Apache open-source software library for logging applications. Certain versions of the software library, which are used ubiquitously in enterprise products worldwide, have a critical vulnerability known as Log4Shell that could allow unauthenticated remote code execution, subsequent extensive unauthorized access to compromised servers, and an ability to insert malicious code at the target computer, install malware, or exfiltrate confidential information. Given the broad use of the affected software library in products worldwide - potentially hundreds of millions of devices and services, often without the end user even knowing that it is present in the code - and the relative ease of the exploit, this vulnerability is being widely and actively exploited by malicious actors. Sami Khoury, Head of the Canadian Centre for Cyber Security, echoed many of his cyber centre partners worldwide in calling the vulnerability an urgent challenge and "serious risk for organizations around the world." [xviii] CCCS issued alerts about active exploitation of the vulnerability, and joined with the national cyber centres of the U.S., U.K., Australia, and New Zealand to release a joint advisory with mitigation guidance.[xix]

The Log4Shell vulnerability demonstrates how important it is to identify and secure open-source code in commercial products or services. The more widely used the open source software, the higher the risk of exploitation of any identified vulnerability. In the case of Log4Shell, its

pervasiveness across the enterprise software ecosystem required quick and sustained coordination between government cyber centres and the vendor community to swiftly identify, mitigate, and patch the wide array of products using the software, and for vendors to proactively communicate to their customers whether their product contained this vulnerability.

Moreover, the nature of open source software development brings a unique security challenge, due to the decentralized responsibility for ongoing security maintenance. A new effort led by the Open Source Security Foundation seeks to mitigate this challenge by recruiting cybersecurity personnel at technology companies to address security gaps in open source software, and publish and maintain a list of vulnerabilities found across 10,000 of the most used open source projects. Microsoft and Google have collectively pledged $5 million to begin the initiative, plus personnel to resource the project. Although early, this is a promising start for collective action to mitigate this challenge.

In the immediate aftermath of the Log4Shell vulnerability, national cyber centers recommended that affected entities enumerate any external facing devices that have log4j installed and take action to automate response activities. As with the SolarWinds incident, these centres' recommendations highlight the importance of incorporating software assurance activities such as code scanning and vulnerability analysis, as well as utilizing technologies to ensure strong visibility across enterprises, like mapping internet-facing systems for vulnerability management (*Sections 3.2 and 3.3 provide more detail on these key strategies and technologies*).

3.2 KEY DEFENCE STRATEGIES TO ENHANCE DIGITAL SUPPLY CHAIN SECURITY

3.2.1 ADOPTING ZERO TRUST ARCHITECTURES

Traditional computer networks used a "castle and moat" security model, built on the notion that if you are inside the perimeter of the castle walls, you are likely trustworthy by default. By stealing the right credentials, malicious actors can often obtain unfettered access to organizations' most sensitive data simply by having breached the perimeter defense. In this case, implicit trust is a vulnerability. A "zero trust" model turns this paradigm on its head, creating more granular rules for how users can, or cannot, move around a network. Even if an adversary gains access to your network, utilizing zero trust can prevent further exploitation simply by denying broader access. Shared Services Canada (SSC), recognizing the global trend toward this new architecture model, is refreshing its network and security strategy and adopting zero trust architecture (ZTA) concepts.[xx] SSC's network security strategy utilizes zero trust concepts to move away from the old perimeter-based security toward a new design of protecting resources - data, software and hardware assets and applications - by verifying each request to access the resource without relying on implicit trust (e.g., inside the network perimeter). Similarly, the U.S. government has also published a Zero Trust Maturity Model for five pillars: identity, device, network, application workload, and data.[xxi]

Adopting ZTA principles also will enhance supply chain security. As the analysis of the SolarWinds supply chain compromise shows, securing and monitoring suppliers' build environments is very important as it is difficult for procurers to detect carefully crafted malware

that is injected in the update packages from suppliers, properly signed and designed to evade enterprise network security protocols. A supplier can increase protection of its key assets - including software, build and deployment systems, and production facilities - from sophisticated adversary attacks, by incorporating zero trust principles. Even if a malicious actor is able to gain access to a network through an attack on or vulnerability in a third-party supplier, adopting zero trust principles could help stymy further lateral movement across the network. In addition, a supplier and a purchaser can better monitor the user entity behavior and the operation of their network, and detect and prevent threats, resulting in supply chain security enhancement.

3.2.2 SECURE DEVELOPMENT LIFECYCLE PROCESSES

It is imperative for each supplier involved in a supply chain to adopt, manage and apply proven and widely accepted guidelines or standards for secure development lifecycle (SDLC) management. It is important for a security practice to identify supply chain risks across an entire product lifecycle – design, sourcing, manufacturing, fulfilment and service – and take action to ensure the integrity measures are put in place. Risk assessments should be performed early in the product development lifecycle to help determine the feasibility of product design and component sourcing decisions. The secure development lifecycle provides guidelines for enhancing organizational support, securing the development environment, developing secure systems for both hardware and software, and vulnerability management. The aim is to assure the integrity of components provided by each supplier in the supply chain so that the end products are secure, without known vulnerabilities and compromise.

Secure development lifecycle guidelines and standards provide risk-based, outcome-focused, flexible and adaptable frameworks, and define practices, tasks, activities and capabilities in terms of governance, design, implementation, verification and operations. Suppliers should establish their own SDLC processes based on the widely accepted guidelines to protect their build environment and produce secure products. Building on recent high-profile supply chain attacks and vulnerabilities, the latest efforts on SDLC standardization focuses on supply chain security:

- *NIST SP 800-218* -- Secure Software Development Framework (SSDF) Version 1.1 recommends practices and tasks in terms of organizational processes, the protection of software and development environments, the development of secure software and vulnerability management. The SSDF provides mapping of the practices and tasks to counterparts defined in the widely recognized industry best practices and standards, e.g., NIST SP 800-53, IEC 62443 and PCISSC's Secure Software Lifecycle (Secure SLC) Requirements and Assessment. The draft provides mapping to the actions called for by the "Enhancing Software Supply Chain Security" section of President Biden's executive order on improving cybersecurity, and existing SDLC guidelines to help an organization evaluate the amenability of its practices to the framework. Each phase of this framework includes security activities to reduce vulnerabilities in the software product.[xxii]
- *OWASP* -- Software Component Verification Standard defines controls to measure and improve software supply chain assurance in six categories including inventory, Software

Bill of Materials, Build Environment, Component Analysis and Pedigree and Provenance.[xxiii]

- *Cloud Native Computing Foundation* -- Software Supply Chain Best Practices provides a series of recommended practices, tooling options and design consideration to secure cloud software supply chain, including the protection of source code, materials, build pipelines, artifacts and deployment.[xxiv]
- *Supply chain Levels for Software Artifacts (SLSA)* -- The Open Source Security Foundation is developing the SLSA standard, a security framework to prevent tampering, improve integrity, and secure packages and infrastructure of enterprises. SLSA defines four level of assurance and requirements for source, build, provenance and common management. SLSA provenance provides verifiable information how the software is constructed in its supply chain.[xxv]

3.2.3 SOFTWARE ASSURANCE AND SUPPLY CHAIN TRANSPARENCY

Understanding and effectively managing the security posture of a complex supply chain remains a key challenge. Suppliers providing visibility on the software composition and interdependencies and purchasers and end users verifying the information from the suppliers is the first step to meeting that challenge. A key strategy in mitigating this risk is strong and transparent supplier management, focused on supplier security requirements, maintaining a robust supplier inventory, as well as establishing collaborative relationships backed by contractual obligations to ensure a complete view of suppliers' security posture, and a collaborative ecosystem of information sharing, risk reduction and remediation, and incident management.

Given the number of upstream and downstream suppliers involved in the supply chain of a complex product, organizations should focus on increased transparency by developing and applying means to identify and verify suppliers involved, the provenance of their components, and their development processes so that customers can verify whether steps taken within the supply chain for developing a product are legitimate, effective, and secure. The more transparent the supply chain becomes, the more difficult for adversaries to take malicious action.

Software transparency in particular is a key lesson learned from the Log4Shell vulnerability, which has fostered renewed calls for Software Bill of Materials (SBOM) efforts. SBOMs aim to increase software assurance by defining and utilizing a standardized "ingredients list" identifying the provenance of code in each software build. The U.S. National Telecommunications and Information Administration (NTIA) recognizes three standards as interoperable SBOM formats, and work is ongoing to define the elements of an SBOM. While an SBOM will not be a panacea by itself, the effort has promise for instances like the Log4Shell incident response, when network defenders were scrambling to find out if the affected software library was incorporated into any of their software technologies across complex network enterprises, and will be a key component of overall software assurance strategies.[xxvi] [xxvii] [xxviii]

Finally, organizations developing software capabilities should employ a secure continuous integration/continuous delivery (CI/CD) approach that focuses on integrating security tools early

into the engineering lifecycle. Controls like static and dynamic analysis help detect any inadvertent vulnerabilities in code, and access should be controlled so that only authorized personnel can make build changes.

3.2.4 PROTECTION OF PLATFORMS AND PRODUCTS

At the end of a supply chain, a purchaser or customer is required to verify, install, correctly configure, and monitor the product's effectiveness and security posture. Considering that products are increasingly connected to each other or with other networks, it is important to protect not only the product but the platform to which it is connected. Applying a risk-based approach, an organization should identify its critical products, ensure that they are securely designed and built, and test them before installation, and monitor their security posture within the platform in which they are connected. Some examples of critical products may include network management tools, mission critical applications and password managers.[xxix]

For protection against sophisticated supply chain attacks against critical products and networks, it is essential to ensure security controls are correctly implemented and functioning within the product and the network. Deploying AI/ML-based monitoring is a foundational strategy that can monitor the critical assets including endpoints, network and applications and automate security and compliance posture reporting, improve their visibility, and detect anomalies to prevent or mitigate attacks from adversaries, including previously unknown zero-day threats. This is especially important for zero trust migration, including ensuring security capabilities are effective no matter where the data resides on a network.

3.2.5 PRINCIPLES-BASED ASSURANCE POLICIES

Current technology assurance often relies on checklists of defences and requisite tooling & standards that organizations should have in place to protect against threats. Unfortunately, such checklist-based compliance schemes tend to be static or slow to update, meaning they do not and cannot keep up with the increasingly changing, industry/sector-nuanced and global digital threat landscape. As such, compliance to the slower moving list of specific defenses, tooling, and standards creates an undue burden on security vendors and organizations alike as they are required to show compliance to requirements that may be invalidated, secure-by-design, or risk transferred in newly available technologies, design patterns, available services, or frameworks.

The burden of explaining non-compliance due to a compensating control or non-applicability can prevent timely adoption of new defenses, and encourages a minimum-effort-to-comply organizational culture which actually increases overall risk to organizations, people, and nations, as adversaries have no such deterrents to adopting new technology, and are increasingly able to share, purchase, and develop information and tactics that bypass known defenses and lower their barrier to entry as a threat agent. Additionally, compliance with an increasingly outdated checklist & related standard can give organizations a false sense of security in the changing digital threat landscape. The movement towards principles-based assurance, on the other hand, shifts the focus to what threats the technology will encounter, and the guiding principles that organizations will need to demonstrate due care over.

The principles-based method is meant to provide a flexible guide within a defined security framework that can be more easily adapted to varying and innovative technology products and applications, and remain consistent over longer periods of time because it focuses on objectives and outcomes and the adequate demonstration of achieving the principles. The principles-based approach also encourages organizations to examine what a principle means to them, how threats can be realistically realized in their situation, and what defenses they can offer. This enforced understanding and self-reflection means organizations to take a more active role against threat protection.

An active example of the principle-based assurance model is the European Union General Data Protection Regulation (EU GDPR) [xxx], which sets out seven (7) key principles for the lawful processing of personal data and then provides guidance on roles and responsibilities, scope, jurisdiction, implementation, and specific processing situations.

A principles-based cyber security assurance model is currently in development by the UK's National Cyber Security Centre.[xxxi] NCSC is developing their principles collaboratively with industry to develop usable principles for technology assurance. These will involve the description of the principle, potential threats, and protective/defensive measures that can be applied. In the UK model, the NCSC will publish security requirements and then ask vendors to self-attest to those requirements while working with the vendors to ensure the validity of their claims.[xxxii]

Applying principles-based assurance is currently in its early stages, but is a promising methodology that will act as a guide for government and private organizations on how to make informed risk decisions applicable to the digital supply chain.

3.2.6 CYBERSECURITY SUPPLY CHAIN INFORMATION SHARING

Finally, exchanging supply chain risk information, vulnerability and threat information, and defensive measures among a sharing community of interest is imperative to prepare and protect organizations from novel and sophisticated cyber attacks, including supply chain risks. Organizations should consider what risk information it needs to ensure confidence in both its products and its downstream suppliers, and work - in accordance with well-established standards or practices, such as through Information Sharing and Analysis Centers - to incorporate that information sharing into its network defence strategies.[xxxiii]

On a more tactical level, organizations should maintain a robust asset and supplier inventory with explicit points of contact so that, should an incident or high-level risk materialize, they can take immediate, coordinated action to secure their environment, inform upstream consumers and downstream providers, and request, collaborate on, or enforce remediation/mitigation in their own supply chain.

3.3 KEY TECHNOLOGY CAPABILITIES FOR SUPPLY CHAIN ASSURANCE

3.3.1 AI/ML: INTEGRATING ENDPOINT DETECTION AND RESPONSE AND SECURITY ORCHESTRATION AND AUTOMATION TECHNOLOGIES

In incidents like the SolarWinds supply chain compromise, which was designed to evade traditional signature-based defence architectures, automated cyber defence capabilities play an important role in the incident response. While not exclusively used to protect against supply chain attacks or vulnerabilities, these automated technologies hold key advantages that do help to prevent or mitigate those attacks or vulnerabilities in a supply chain use case. In this case, two key technology capabilities can be brought to bear. First, endpoint detection and response (EDR) technology is useful for continuous monitoring and real-time security policy enforcement, especially since the recent phenomenon of a rapid move to remote worksites have significantly reduced reliance on traditional perimeter-based defence. EDR enabled by local machine learning models can isolate compromised endpoints; prevent malware before execution; detect and respond to malicious codes; and stop accessing malicious URLs without connectivity to the enterprise network or cloud. Advancements in EDR technologies enable anomalous activity detection, such as user behavior analytics to identify malicious activity. EDR is most impactful when it can aggregate network, cloud, and endpoint data from across the whole network architecture to provide enterprise-wide monitoring and enable automated defensive capabilities, often referred to as Extended Detection and Response. Organizations that automatically collect and integrate relevant data across network, endpoint, and cloud sensors can realize significant operational benefits. Machine learning can be applied to the entire dataset, to correlate different events or alerts from any source, providing visibility into the full chain of events for an attack. Then, ML-driven user behavioral analysis capabilities can help differentiate between suspicious and benign activity, even among unknown or highly evasive tactics.

Second, security orchestration and automation capabilities can take advantage of integrated datasets to automate incident response. Orchestration and automation capabilities support data collection for analytics and taking automatic actions necessary to remediate identified cybersecurity risks. The collected data could include vulnerability scores, access logs, traffic metadata and user entity behavior analytics to evaluate the security posture of users, devices, applications, and network. Based on the analytics output, access policy can be dynamically adjusted - such as in a zero trust architecture - and applied automatically. Alerts from analytics, combined with other datasets, enables curated threat intelligence for analysts to undertake threat hunting activities. By reducing manual tasks in incident response actions, analysts are freed to respond to more significant alerts and collaborate with other analysts on higher-tier responses.

In the event of a supply chain compromise, organizations that effectively make use of technologies to integrate security data across the entire network enterprise, and use that data to automate defensive capabilities wherever possible, will be best positioned to effectively prevent or mitigate an incident.

3.3.2 INTERNET-ACCESSIBLE ASSET SCANNING TECHNOLOGIES

As discussed in Section 3.1.2, the key initial response action during the Log4Shell incident response was to "enumerate any external facing devices that have log4j installed." [xxxiv] This response action recognized the increasing importance of accurately understanding a given network's baseline risk and security posture, by inventorying and managing internet-facing systems and assets (including not only the network and infrastructure layer but also application vulnerabilities) based on attackers' views of the internet. The "attacker view," often referred to as enterprise Attack Surface Management, helps to account for shadow IT discovery, malicious exploit call-outs, or other unauthorized internet-facing connections. To overcome the inherent challenges for organisations of all sizes to reliably track every internet-exposed asset, asset scanning technologies enable real-time discovery of and visibility over a network's attack surface which are at increased risk of exposures exploitable by malicious adversaries, particularly its forward-facing internet assets and assets held in cloud environments. In use cases such as the SolarWinds compromise, internet-asset scanning technologies could have been utilized to identify infected servers connected to the internet via the malicious payload exploit, a typically unusual posture for network management tools.

In its newly updated and released *Guidance on Federal Information Security and Privacy Management Requirements*, the U.S. Office of Management and Budget includes a new section on "Scanning Internet-Accessible Addresses and Systems." This guidance requires U.S. government agencies to maintain an accurate, up-to-date picture of their internet-facing assets, to facilitate swifter vulnerability remediation and incident response for incidents such as the SolarWinds compromise and Log4Shell vulnerability.[xxxv]

3.3.3 CODE SCANNING, TESTING, AND SECURITY VERIFICATION TECHNOLOGIE

As discussed in Section 3.2.3, organizations should employ a secure CI/CD approach to software development or integration, incorporating controls like static and dynamic testing to help detect any inadvertent vulnerabilities in code. Software composition analysis tools are available to scan source or binary code, identify components, and create an SBOM. These capabilities include detecting components of unknown origin, identifying the provenance of the detected components and evaluating vulnerabilities and weaknesses within each component, including open source software. It is also recommended that producers and acquirers in the supply chain utilize binary scanning tools to verify the components included in the final packages where no source code is available.

Additionally, testing and verification technologies can also be used to secure new advances in development environments, like containers and infrastructure-as-code build deployments. Container vulnerability analysis can evaluate containers against common misconfiguration and software package vulnerabilities, while secure infrastructure-as-code can likewise prevent or remediate security misconfigurations in those environments.

3.3.4 HARDWARE ROOT OF TRUST

All of the defence use cases above rely on a trusted execution environment and an established hardware root of trust. Hardware root of trust can be leveraged to provide better visibility into potential supply chain compromises, given that it is the foundation upon which the computing system's trust model is built. Without the trusted hardware baseline, confidence in the ICT supply chain cannot be established. The Trusted Computing Group's Trusted Platform Module (TPM) 2.0 specification defines a cryptographic microprocessor designed to secure hardware by integrating cryptographic keys and services. A TPM functions as a root of trust for storage, measurement, and reporting. TPMs are currently included in many computing devices. The NIST SP 1800-34 series shows best practices to construct a trusted execution environment utilizing existing commercial products.

3.4 KEY FINDINGS AND RECOMMENDATION

Whether seeking to prevent or mitigate a malicious compromise or inadvertent supplier vulnerability, key endpoint and network defence strategies and technology capabilities play an important role in supply chain assurance. These strategies seek to promote adoption of zero trust architectures, secure development lifecycles, software composition analysis tools, and other transparency initiatives. Key technologies take advantage of advances in AI/ML to automate key response activities, understand baseline risk, and test and verify secure software environments.

Recommendation: **The Government of Canada should review existing government-wide security architectures and technical reference requirements, and update as appropriate to account for critical system defence strategies, practices and technology capabilities that could prevent, mitigate, or lessen the impact of supply chain attacks or vulnerabilities, as reviewed in this section. Once completed, those architectures and reference requirements should be disseminated to industry as models for adoption, to the extent feasible and scalable. (An additional recommendation for industry adoption of key practices is covered in Section 4.)**

4.0 KEY PRACTICES FOR SUPPLY CHAIN SECURITY AND INTEGRITY: PRINCIPLES FOR INDUSTRY ADOPTION, AND RECOMMENDATIONS FOR INDUSTRY AND GOVERNMENT

Section 4 identifies key digital supply chain risk management practices for organizations to implement. These assurance practices have been previously documented by governments and industry partners around the world; among the most influential are NIST SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*,[xxxvi] ISO 28001, *Security Management Systems for the Supply Chain*,[xxxvii] and NISTIR 8276, *Key Practices in Cyber Supply Chain Risk Management: Observations from Industry*.[xxxviii] Thus, this section does not exhaustively catalogue all existing supply chain risk management practices. However, it is important to identify the key concepts and principles derived from existing bodies of work and identify opportunities to further implement these principles in industry and government organizations.

This section highlights the importance of instituting a formal risk management program across the organization, and integrating a product's lifecycle (design, sourcing, manufacturing, fulfilment and service, decommissioning) with security and integrity practices at each stage. This section also highlights the importance of organizations understanding the totality of their supply chain, closely collaborating with key upstream and downstream suppliers and consumers to assess, monitor and respond to risks proactively. Finally, mechanisms for evaluating and assessing these practices will ensure resources are appropriately managed and deployed.

Future work in this area could include the development of a "maturity model" for organizations, especially small and medium-sized businesses, to make resource decisions about their supply chain assurance programs based on their own maturity and risk profile. *Ultimately, an organization's goal is a secure, sustainable, and resilient ICT Supply Chain Risk Management program.*

4.1 ESTABLISH AND IMPLEMENT AN ICT SCRM PROGRAM INTEGRATED WITH OTHER PROGRAMS ACROSS YOUR ORGANIZATION

A key confidence indicator is the ability to demonstrate supply chain risk management across the enterprise and across a product's entire lifecycle in a formalized SCRM program. Using key standards and guidance documents [xxxix] as a guide, organizations should establish, document, manage and evaluate the policies and procedures that will ensure integrity practices are proactively integrated at every stage of a product's design, sourcing, manufacturing, fulfillment, and service. Risk assessments can help determine the feasibility of product design decisions. A culture of executive management buy-in, with strong coordination and review mechanisms, is critical to successful programs.

(a) Based on the organization's business, operations, and strategic goals, select relevant program areas to integrate with. Program areas include but are not limited to enterprise risk management, procurement and contract management, information security, change management, business continuity, and quality control.

(b) Ensure that supply chain integrity requirements are included in your organization's procurement contract management processes.[xl]
(c) Determine your organization's supply chain risk criteria, appetite, tolerance, and mitigation strategies. Ensure that these are in alignment with that of the existing enterprise risk management program.
(d) Ensure that the ICT SCRM program addresses the lifecycle management of both one-time supply chains and repeatable/continuous supply chain.
(e) Monitor and review the ICT SCRM program to ensure that it remains aligned with your organization's goals and security requirements.

4.2 UNDERSTAND YOUR ORGANIZATION'S SUPPLY CHAIN

Another key confidence indicator is the ability to establish visibility into the production processes of organizations' suppliers. Organizations should implement supplier onboarding & review processes encompassing data on risk management plans, incident and security disclosure and response coordination and visibility downstream into the supply chain. Organizations should also consider monitoring for environmental, geopolitical, and other events; financial risk disruptions; and component supply source assessment. Hardware component traceability, including suppliers' internal production and test history, and keeping up-to-date software component inventories and provenance as discussed in Section 3.2, are also key practices. Having these critical details in place allows organizations to act quickly in the event of a supply chain disruption.

(a) Identify critical elements/components of the supply chain and verify their integrity, for example, obtaining comprehensive SBOM and provenance data for the software supply chain or utilizing software composition analysis tools.
(b) Categorize criticality of supply chain elements and determine dependencies of the elements.
(c) Determine the risks to your supply chain via a risk assessment supported by automation tools, e.g., known vulnerabilities associated with identified software components
(d) Using the supply chain risk appetite and tolerance level as a guideline, ensure that identified risks are mitigated to an acceptable level.
(e) Continuously monitor the risk factors (at a frequency pre-determined by criticality) to ensure that risks introduced into your supply chain remain managed within your organization's risk tolerance level.
(f) Maintain a robust supplier inventory which facilitates/stores the above elements and also tracks main points of contact, contractual obligations, and procedures for security-related incident response and disclosure.

4.3 ESTABLISH AND MANAGE RELATIONSHIPS WITH SUPPLIERS/VENDORS AND CLIENTS/CUSTOMERS

Strong supplier relationships go hand-in-hand with understanding your organization's supply chain. Most supplier relationships are managed contractually, which could include requirements to disclose security incidents or component vulnerabilities so that organizations can take appropriate risk mitigation actions. Even with contract-based management, organizations should

seek as collaborative as possible a relationship with their suppliers, including investing in their security postures and fostering two-way exchanges of risk information and other insights.

(a) Regularly evaluate activities and practices of suppliers to ensure that suppliers' approach to information security practices is consistent with and/or complements your organization's practices.
(b) Build collaborative (trust) relationships with identified key suppliers to ensure that practices are consistent with those of your organization. Practices include but are not limited to incident management, access control, disaster recovery, personnel vetting/hiring, risk management, security, manufacturing, and quality control
(c) Negotiate and establish mutual polices, procedures, and service-level agreements around incident disclosure and handling, definition & handling of data & privacy violations, vulnerability communication & remediation expectations and timelines, backed by legal contractual obligations.
(d) Maintain a list of points of contact and their roles & responsibilities for vulnerability and incident handling and disclosure.
(e) Regularly review supplier contracts to include updated provisions and enforce increasing levels of maturity in the above.

4.4 CONTINUOUSLY MONITOR SECURITY POSTURE OF CRITICAL SUPPLY CHAIN PRODUCTS/COMPONENTS

Organizations should implement a program to continuously monitor supplier adherence to key practices and standards, including vulnerability disclosure and remediation. Utilizing the key strategies and technologies identified in Section 3, organizations should identify critical components of hardware and software tools and take steps for enhanced risk management across the development lifecycle. Anti-tampering and anti-counterfeiting measures, such as boot time software integrity checks on hardware platforms, also help ensure component and final product authenticity.

(a) Monitor known and emerging vulnerabilities as well as their compromise and resolution status, including through integration with your organization's enterprise asset and patch management program.
(b) Monitor for risks that could be inherited directly/indirectly from your suppliers. These include vulnerability disclosures and attempts/successful compromises of suppliers' environment.
(c) Integrate security measures into all aspects of the product and support lifecycle, including anti-tampering and anti-counterfeiting practices.
(d) Identify and monitor critical ICT components for behaviour and activity that is anomalous or indicative of tampering in the supply chain, as discussed in Section 3. Unlike exploits or other post-delivery tampering, supply chain attacks usually involve "believed good code" and will pass hash-code and vendor validation. "Behaving oddly" can be a leading indicator of a compromise.

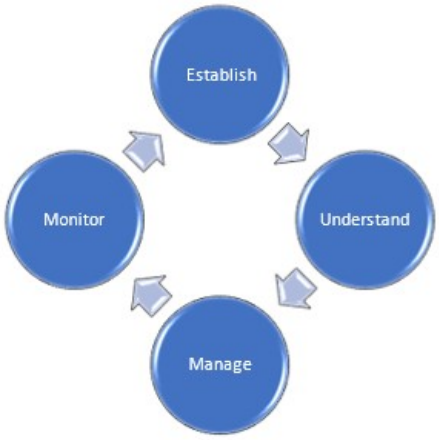

Figure 1: Establish, Understand, Manage, Monitor Loop

4.5 KEY FINDINGS AND RECOMMENDATIONS

The practices identified in Section 4 are key confidence indicators for instituting a secure, sustainable, and resilient ICT Supply Chain Risk Management program, focused on building security and integrity practices into all stages of a hardware or software product's development lifecycle. While these key practices are generally well known and grounded in guidance documents and international standards, there are opportunities to facilitate further adoption across Canadian industry.

In particular, future work of the government could be collaboration on easily-understandable and actionable guidance for small and medium businesses, building on existing programs such as CyberSecure Canada [xli] and Get Cyber Safe [xlii] that provide overarching cybersecurity guidance. These small and medium businesses are vital to Canada's economic prosperity, but do not often have the resources to implement a full-scale risk management program. Such a collaboration could build on work CCCS has already undertaken and distill the key steps small and medium businesses should take to maintain confidence in their supply chain.[xliii]

Similarly, a future government and industry collaboration could also consider how the Government of Canada can drive adoption of key practices across industry. For instance, the U.S. government has developed key considerations for government procurements that include creating "qualified bidder lists" based on organizations' adoption of supply chain key practices.[xliv] Ultimately, a similar collaboration on the development of a "maturity model" for organizations to make resource decisions about their supply chain assurance programs based on their own maturity and risk profile.

Recommendation for industry: **ICT organizations should begin preparing now to meet coming supply chain requirements.**

Governments worldwide, in consultation with industries, are increasingly focused on mandating improved supply chain risk management practices as a condition of procurement, and

enforcement of these improvements is materializing as new certification schemes, compliance framework updates, or principles-based assurance frameworks.

For instance, in March 2022, the U.S. Office of Management and Budget announced that, consistent with President Biden's cybersecurity executive order, U.S. government agencies that purchase software will require the software vendors to attest to compliance with secure development practices; the practices follow the Secure Software Development Framework (NIST SP800-218) and related guidance. For vendors to the U.S. government, the secure development attestation will come into force after an OMB-led private sector engagement process to determine how best to implement this requirement.[xlv]

While attestation schemes, especially those requiring static assessments or certifications, have limitations in their effectiveness (principles-based assurance policies as described in Section 3.2.5 have considerable merit as a collaborative assurance methodology) many governments appear intent to use attestation in some form, e.g., self-conformity assessment and supplier's declaration. To the extent that governments continue to do so, ICT vendors should be aware of and prepared to meet those requirements. As such, **industry ICT suppliers will need to be able to explain, defend, show auditable evidence of, and effectively operate a maturing supply chain risk management process and related practices that address well-known supply chain and asset management issues within their control** [xlvi], specifically in the areas of:

- Custom software development and the software development/operation lifecycle;
- Open-source software and commercial off-the-shelf software used by the organization;
- SaaS/PaaS suppliers and systems used by the organization; and
- Shadow IT and evolving organizational attack surface management.

Industry should review their 2-5 year technology and risk management plans to ensure they are adopting appropriate key confidence indicators for supply chain risk management commensurate with the organization's maturity and risk profile, and taking advantage of the new technologies and innovations in the space to help meet future supply chain attestation requirements and/or mitigate supply chain incidents. In particular, confidence indicators include:

- A dedicated supply chain risk management program management with executive oversight, corresponding budget, and board-level reporting;
- An increased focus on integrated asset and supplier management to inform and mature security and integrity practices built into a systemic product lifecycle management strategy;
- Systemic collection and aggregation of third-party component information and organizational attack surface used - especially in custom software development - as part of asset management (e.g. in the form of SBOMs or equivalent industry-accepted materials, and perhaps with the assistance of Internet-Accessible Asset Scanning Technologies listed in 3.3.2);
- Contract-based and trusted-supplier relationship-based visibility and transparency into component suppliers' production processes, and associated risk assessments, especially for commercial off-the shelf software providers; and

- Contract-based notification and audit provisions to ensure remediation and communication of critical vulnerabilities, incidents, and risks can be enforced with suppliers.

While the responsibility is on individual industry organizations to adopt and implement key digital supply chain defense strategies and technologies for securing their own supply chains, there are additional actions the Government of Canada could consider taking that would facilitate adoption. Among these are developing actionable, targeted guidance to small and medium businesses; identifying policy levers to incentivize key practice adoption by the government's ICT suppliers; and developing a "maturity model" framework to assist organizations developing SCRM programs.[xlvii]

Recommendation for government:

- **Develop and disseminate easily-implementable guidance for small and medium businesses;**
- **Develop a "maturity model" framework for organizations to make resource decisions about their supply chain assurance programs tailored to their risk profile and encourage knowledge sharing;**
- **Use policy levers to drive adoption of key practices by ICT suppliers to the government, such as through qualified procurement actions; and**
- **Develop a set of supply chain risk assessment requirements, objectives, and/or principles, and related guidance on questionnaires, contracting, and scoring rubrics.**

5.0 CONCLUSION

The very interconnectedness of global supply chains means that every ICT consumer and supplier has a stake in a secure, resilient supply chain. As key events like the SolarWinds supply chain compromise and Log4Shell vulnerability show, supply chain incidents have the potential to significantly affect Canada's economy and security.

Given this interconnectedness, promoting confidence in a secure, resilient digital supply chain requires close collaboration across stakeholders in government as well as ICT organizations of all sizes and maturity levels that support critical infrastructure sectors. While significant activities have been undertaken, it is clear that government and industry should continue to move with urgency to address existing gaps. Thus, recommendations aligned to this imperative include adopting strong governance principles aligned to a unified Canadian vision and strategy, adopting digital supply chain defence strategies and state-of-the-art technologies, and adopting key confidence indicators for risk management best practices.

Beyond these initial recommendations, future work could facilitate broader adoption: collaboration on easily-understandable and actionable guidance for small and medium businesses; the development of a "maturity model" for organizations to make resource decisions about their supply chain assurance programs; and identifying policy levers to drive adoption of key confidence indicators.

Ultimately, what these findings show is that the policy actions and investments to promote confidence in a secure, resilient digital supply chain should not be one-off or *ad hoc*. Only sustained, continued investment and focused coordination can create the foundations of a strong ICT supply chain.

6.0 APPENDIX

Additional supply chain incident case studies

Incident	Entry Point	SCLC Phase
Codecov Attackers exploited a mistake in how Codecov built docker images and compromised the Codecov bash uploader via a docker image. Environment variables, credentials, and secrets were exfiltrated. Impacted clients include GitHub, Twilio, IBM, Google, HP and other enterprise Source: https://blog.gitguardian.com/codecov-supply-chain-breach/	Unauthorized alterations to Codecov Bash uploader script	Operation
Quanta Apple supplier, Quanta had their network and breached in a ransomware attack. After gaining access to Apple's product designs, the attackers also demanded that Apple pay the ransom to avoid leaking future product designs. Source: https://www.theverge.com/2021/4/21/22396283/apple-schematics-leak-ransomware-quanta-supplier-leak	Highjacked product designs from supplier	Delivery and Deployment
Mimecast A compromise of Mimecast's production grid environment resulted in the exposure and theft of source code repositories. Mimecast-issued security certificates were compromised including a certificate that authenticates Mimecast's services on Microsoft 365 Exchange Web Services. While a low number of customers were targeted, about 10% of Mimecast's customers used impacted certificates. Source: https://arstechnica.com/gadgets/2021/03/mimecast-says-solarwinds-hackers-breached-its-network-and-spied-on-customers/	Security certificate compromise	Operation

Dependency Confusion A security researcher was able to breach Microsoft, Uber, Apple, Shopify, Tesla, Netflix and others by taking advantage of dependencies that applications use to provide services to end-users. Through these dependencies, the researcher was able to transmit data packets to its victims. Source: https://arstechnica.com/information-technology/2021/02/supply-chain-attack-that-fooled-apple-and-microsoft-is-attracting-copycats/	Libraries	Operation
Passwordstate An attacker gained access to Passwordstate's update server and inserted a malicious DLL into an update that was downloaded by customers. The malicious DLL enabled the attacker to harvest sensitive information and decrypt the entire database using encryption keys hosted on the web server's filesystem. Source: https://duo.com/decipher/supply-chain-attack-hits-passwordstate-password-manager	Update functionality of the Passwordstate enterprise password manager	Maintenance
SITA An aviation IT company that serving about 90% of the world's airlines by providing passenger ticketing and reservation systems to airlines via its Passenger Service System (PSS). The SITA PSS was breached, resulting in the theft of the personal information of multiple airlines' customers. The breach is believed to have originated from Star Alliance, and then spread across the entire supply chain to impact all carrier members. Many airlines have reported data breaches related to the SITA PSS breach. Source:	Passenger Service System	Operation

https://www.zdnet.com/article/airlines-warn-passengers-of-data-breach-after-aviation-tech-supplier-is-hit-by-cyberattack/		

7.0 LIST OF ACRONYMS

Term	Description
5G	Fifth generation wireless networks
AI/ML	Artificial Intelligence/Machine Learning
CCCS	Canadian Centre for Cyber Security
CFDIR	Canadian Forum for Digital Infrastructure Resilience
CI/CD	Continuous integration/Continuous delivery
CPNI	Centre for the Protection of National Infrastructure
CSE	Communications Security Establishment
EDR	Endpoint Detection and Response
ENISA	EU Agency for Cybersecurity
EU	European Union
G7	The Group of Seven
ICT	Information and Communications Technology
ISED	Innovation, Science and Economic Development Canada
NCSC	U.K. National Cyber Security Centre
NIS	Network and Information Directive
NIST	(United States) National Institute for Standards and Technology
NISTIR	U.S. National Institute of Standards and Technology Interagency Report
NTIA	U.S. National Telecommunications and Information Administration
OMB	U.S. Office of Management and Budget
OWASP	Open Web Application Security Project
PSPC	Public Services and Procurement Canada
PTM	Provincial, Territorial, Municipal governments
SBOM	Software Bill of Materials
SCI	Supply Chain Integrity
SCRM	Supply chain risk management
SDLC	Secure Development Lifecycle
SLSA	Supply chain Levels for Software Artifacts
SSC	Shared Services Canada
SSDF	Secure Software Development Framework
TPM	Trusted Platform Module
UK	United Kingdom
US	United States
ZTA	Zero Trust Architecture

8.0 ENDNOTES

[i] National Cyber Strategy Of The United States Of America. Washington: The White House; September 2018. https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

[ii] H.R.7327 - Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act. Library of Congress. https://www.congress.gov/bill/115th-congress/house-bill/7327/text. Published December 2018.

[iii] National Cyber Strategy Of The United States Of America. Washington: The White House; September 2018. https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

[iv] ICT SCRM Task Force. CISA. https://www.cisa.gov/ict-scrm-task-force.

[v] National Cyber Strategy 2022 (HTML). GOV.UK. https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022. Published December 15, 2021.

[vi] Publications Office of the European Union. Document 52020PC0823: Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148. EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:823:FIN. Published 2020.

[vii] Secure 5G networks: Commission endorses EU toolbox and sets out next steps. Press corner of the European Commission. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_123. Published January 29, 2020.

[viii] ENISA Threat Landscape For Supply Chain Attacks. European Union Agency for Cybersecurity (ENISA); July 29, 2021. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

[ix] Thuppal R. Cyber and IT Security. Government of Canada. https://www.canada.ca/en/shared-services/corporate/doing-business-with-us/information-technology-infrastructure-roundtable/main-roundtable-meetings/december-7-2015-cyber-it-security-presentation.html. Published December 5, 2015.

[x] Alerts and advisories. Canadian Centre for Cyber Security. https://cyber.gc.ca/en/alerts-advisories

[xi] The G7 Digital and Technology Ministers. G7 Digital and Technology Ministerial Declaration. G7 Information Centre of the University of Toronto. http://www.g7.utoronto.ca/ict/2021-digital-tech-declaration.html. Published April 28, 2021.

[xii] National Cross Sector Forum 2021-2023 Action Plan for Critical Infrastructure. Public Safety Canada - Publications. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2021-ctn-pln-crtcl-nfrstrctr/index-en.aspx.

[xiii] Cyber Security Cooperation Program. Public Safety Canada. https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/cprtn-prgrm/index-en.aspx. Modified December 15, 2020.

[xiv] For instance, the American Institute of Certified Public Accountants (AICPA) has a System of Organization and Control (SOC) for Supply Chain for risk management that is mostly known only within the CPA community.

[xv] Boyens J, Paulsen C, Moorthy R, Bartol N. Supply Chain Risk Management Practices for Federal Information Systems and Organizations. NIST Computer Security Resource Center. https://csrc.nist.gov/publications/detail/sp/800-161/archive/2015-04-08. Published April 2015.

[xvi] TTP Table for Detecting APT Activity Related to SolarWinds and Active Directory/M365 Compromise. CISA. https://us-cert.cisa.gov/sites/default/files/publications/Supply_Chain_Compromise_Detecting_APT_Activity_from_known_TTPs.pdf Published March 17, 2021.

[xvii] Palo Alto Networks Rapid Response: Navigating the SolarStorm Attack. Arora, Nikesh. https://www.paloaltonetworks.com/blog/2020/12/solarwinds-statement-solarstorm/ Published December 17, 2020.

[xviii] CISA, FBI, NSA, and International Partners Issue Advisory to Mitigate Apache Log4J Vulnerabilities. National Security Agency Press Room. https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/2881834/cisa-fbi-nsa-and-international-partners-issue-advisory-to-mitigate-apache-log4j/. Published December 22, 2021.

[xix] Alert (AA21-356A) Mitigating Log4Shell and Other Log4j-Related Vulnerabilities. CISA Alerts. https://www.cisa.gov/uscert/ncas/alerts/aa21-356a. Published December 22, 2021. Updated December 23, 2021.

[xx] Network and Security Strategy. Shared Services Canada, Government of Canada. https://www.canada.ca/en/shared-services/corporate/publications/network-security-strategy.html

[xxi] CISA. Zero Trust Maturity Model (pre-decisional draft). https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf Published June 2021.

[xxii] NIST SP800-218 - Secure Software Development Framework (SSDF) Version 1.1. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf Published February 2022.

[xxiii] OWASP. Software Component Verification Standard. https://owasp.org/www-project-software-component-verification-standard/

[xxiv] Cloud Native Computing Foundation. Software Supply Chain Best Practices. https://project.linuxfoundation.org/hubfs/CNCF_SSCP_v1.pdf

[xxv] Supply chain Levels for Software Artifacts (SLSA). https://slsa.dev/

[xxvi] ISO/IEC 5926:2021. Information technology — SPDX® Specification V2.2.1. https://spdx.github.io/spdx-spec/

[xxvii] OWASP. CycloneDX. https://cyclonedx.org/docs/1.3/

[xxviii] ISO. Software Identification Tag – ISO/IEC 19770-2:2015 https://www.iso.org/standard/65666.html

[xxix] NIST. Definition of Critical Software Under Executive Order (EO) 14028. https://www.nist.gov/system/files/documents/2021/10/13/EO%20Critical%20FINAL.pdf Published October 13, 2021.

[xxx] General Data Protection Regulation (GDPR) – Official Legal Text. https://gdpr-info.eu/

[xxxi] National Cyber Security Centre (NCSC). Principles and how they can help us with assurance. https://www.ncsc.gov.uk/blog-post/principles-and-how-they-can-help-us-with-assurance Published September 24, 2021.

[xxxii] National Cyber Security Centre. Cloud security guidance. NCSC.GOV.UK. https://www.ncsc.gov.uk/collection/cloud-security. Published November 17, 2018. Reviewed May 10, 2022.

[xxxiii] NTIA. The Minimum Elements for a Software Bill of Materials (SBOM). https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf Published July 12, 2021.

[xxxiv] STATEMENT FROM CISA DIRECTOR EASTERLY ON "LOG4J" VULNERABILITY. CISA. https://www.cisa.gov/news/2021/12/11/statement-cisa-director-easterly-log4j-vulnerability. Published December 11, 2021.

[xxxv] Miller J. MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES (M-22-05): Fiscal Year 2021-2022 Guidance On Federal Information Security And Privacy Management Requirements. Washington: EXECUTIVE OFFICE OF THE PRESIDENT OFFICE OF MANAGEMENT AND BUDGET; December 6, 2021. https://www.whitehouse.gov/wp-content/uploads/2021/12/M-22-05-FY22-FISMA-Guidance.pdf

[xxxvi] Boyens J, Paulsen C, Moorthy R, Bartol N. Supply Chain Risk Management Practices for Federal Information Systems and Organizations. NIST Computer Security Resource Center. https://csrc.nist.gov/publications/detail/sp/800-161/archive/2015-04-08. Published April 2015.

[xxxvii] ISO 28001:2007. ISO. https://www.iso.org/standard/45654.html. Published 2007. Reviewed 2021.

[xxxviii] Boyens J, Paulsen C, Bartol N, Winkler K, Gimbi J. Key Practices In Cyber Supply Chain Risk Management: Observations From Industry. NIST Technical Series Publications; February 2021. https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8276.pdf.

[xxxix] ANSI/ASIS SCRM.1-2014 Supply Chain Risk Management Standard: A Compilation of Best Practices American National Standards Institute Inc. https://www.asisonline.org/publications--resources/standards--guidelines/scrm/ Published March 2014

[xl] TSCG-01 Technology Supply Chain Guidelines, Communications Security Establishment, https://cyber.gc.ca/sites/default/files/publications/tscg-ccat01g-eng_4.pdf. Published October 2010.

[xli] CyberSecure Canada. Innovation, Science, and Economic Development Canada. https://ised-isde.canada.ca/site/cybersecure-canada/en.

[xlii] Get Cyber Safe. Government of Canada. https://www.getcybersafe.gc.ca/en.

[xliii] Supply chain security for small and medium-sized organizations (ITSAP.00.070). Canadian Centre for Cyber Security. https://cyber.gc.ca/en/guidance/supply-chain-security-small-and-medium-sized-organizations-itsap00070. Published March 2019.

[xliv] ICT Supply Chain Library | CISA. CISA. https://www.cisa.gov/publication/ict-scrm-task-force-qualified-lists-report.

[xlv] OMB Statement on "Enhancing The Security Of Federally Procured Software." The White House. https://www.whitehouse.gov/omb/briefing-room/2022/03/07/omb-statement-on-enhancing-the-security-of-federally-procured-software/. Published March 7, 2022.

[xlvi] Framework for Improving Critical Infrastructure Cybersecurity v1.1, Section 3.3

National Institute of Standards and Technology.
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf Published April 2018.

[xlvii] An SCRM template that could feed into a maturity model: VENDOR SUPPLY CHAIN RISK MANAGEMENT (SCRM) TEMPLATE. CISA; 2021.
https://www.cisa.gov/sites/default/files/publications/ICTSCRMTF_Vendor-SCRM-Template_508.pdf.

In addition, further references for Section 4:

1. Information Security Risk Management Standards (ITSG-33, NIST SP 800-53, NIST SP 800-39) *Influenced Principles*: #1 – 4
2. Guide for Conducting Risk Assessments (NIST SP 800-30)
   Influenced Principle: #2
3. Managed Service Providers: How to manage risk to customer networks (ACSC Protect, December 2018)
   Influenced Principle: #3
4. Mitigations and Hardening Guidance for MSPs and Small- and Mid-sized Businesses (CISA Insights, July 2021)
   Influenced Principle: #2
5. Best Practices for Cyber Security Supply Chain Risk Management (NIST)
   Influenced Principle: #1
6. The Minimum Elements for a Software Bill of Materials (SBOM) Pursuant to Executive Order 14028 on Improving the Nation's Cybersecurity (NTIA, July 2021)
   Influenced Principles: #2

The contents of this document were developed during the course of CFDIR SCAWG meetings between January 2021 and June 2022.

Version 01 - June 3, 2022

Prepared by the Supply Chain Assurance Working Group of the
Canadian Forum for Digital Infrastructure Resilience

TLP:WHITE