INTERNET
STANDARDS,
SECURITY AND
SAFETY COALITION
(IS3C)

MAKING THE INTERNET
MORE SECURE AND SAFER

Procurement and Supply Chain Management and the Business Case

An IS3C research report by

Liz Orembo
and
Mallory Knodel
(email authors)

Table of contents

1. Preface

This draft report aims to document existing policy requirements for public sector procurement contracts and supply chain management of digital technologies and asks whether security-related technical standards are mentioned. It highlights emerging best practice and gaps in an effort to provide high-level guidance at the global level on how procurement plays a role in improving the security and safety of the global Internet for all.

The main conclusions are that in the analysed documents, security-related Internet standards and ICT best practices are, with very little notable exceptions:

a) Not mentioned nor recognised in these documents:
b) Not used to procure secure by design ICT, and that;
c) Most documents are from the Global North.

In other words, there is a world to win for organisations, public and private, to become more secure by design. We close with discussion and suggestions for future work.

2. Background: Global governance

Internet and ICT security is an issue that is high on the agenda of governments, industry and individuals alike. Many networked products and services are increasingly vulnerable to security threats and the spread of online harms and criminal misuse. A massive cybersecurity industry sells products, services and insurance to governments and the private sector to mitigate cybersecurity incidents. However, prevention and the reduction of overall risk can be achieved if relevant security-related standards and best practices are more effectively adopted and deployed worldwide.

Global Internet governance provides an opportunity to shift normative practice in cybersecurity. Governments, the private sector, civil society, the technical community and academia tackle contemporary issues through open and inclusive processes. Since 2006 the Internet Governance Forum (IGF) provides a non-binding, multi-stakeholder space for policy dialogue on Internet governance issues under the auspices of the United Nations. One such process of the IGF is that of the Dynamic Coalition (DC). DCs are long-term intersessional groups dedicated to an Internet governance issue or set of issues.

The IGF Dynamic Coalition on Internet Standards, Security and Safety (IS3C) brings together key stakeholders with the shared goal of making online activity more secure and safer by advocating the wide spread deployment of security-related Internet standards and ICT best practices. The current work of the IS3C focuses on three areas in order to achieve this goal: Security by design; Education and skills; and Procurement and business models[1]. These areas of work set a foundation for the IS3C joint work that aims to consider both demand and supply factors in order to propose the best options, deployed as key standards. Standards, in this case, are essentially policy recommendations for decision makers to take forward.

[1] For more information on IS3C's work and working groups see: https://is3coalition.org/

The third working group of the IS3C (WG3) envisions the development of policy recommendations such as on the procurement of digital technologies. Ensuring procurement best practice takes into account Internet security and safety requirements, and that this is included in procurement training, in particular in developing countries.

To that end this worldwide survey of procurement guidance amplifies existing work and processes. The report begins with an introduction, providing background information, research objectives, and an overview of the methodology. The methods section follows, detailing the approach, tools, and techniques used in the study. The findings section presents the results and outcomes, including data analysis and relevant visual representations. The conclusions and future work section summarises the key findings, discusses their implications, and suggests potential areas for further research. The acknowledgements section acknowledges individuals or organisations that contributed to the study. Finally, the annex provides supplementary information, such as raw data.

3. Terminology: Procurement contracts and supply chain management

In the context of Internet technologies, we are concerned with the procurement, supply chain management and security standards therein.

Procurement, in the context of digital technologies, refers to the process of acquiring goods, services, or solutions from external sources to meet the needs and requirements of an organisation. It involves activities such as identifying suppliers, negotiating contracts, and managing the purchase and delivery of digital technologies. Effective procurement strategies ensure that organisations obtain high-quality products or services at competitive prices, within specified timelines, and with favourable terms and conditions. By adopting efficient procurement practices, organisations can optimise their resource allocation and enhance their operational capabilities in the digital domain.

Supply chain management plays a crucial role in the procurement of digital technologies. It encompasses the coordination and integration of various activities involved in sourcing, procurement, production, and distribution of goods or services. In the context of digital technologies, supply chain management focuses on ensuring a seamless flow of products, information, and resources across the supply chain network. It involves managing relationships with suppliers, monitoring inventory levels, mitigating risks, and optimising logistics and transportation. Effective supply chain management in digital technology procurement can result in improved efficiency, reduced costs, enhanced customer satisfaction, and greater agility in responding to market demands. Best practice in supply chain management includes due diligence processes for ethical considerations and corporate social responsibility.

Security standards are critical in the procurement of digital technologies due to the increasing importance of protecting sensitive information, systems, and networks from cyber threats. Security standards provide guidelines, best practices, and frameworks that organisations should adhere to when procuring and implementing digital technologies. These standards ensure that the procured technologies meet specified security requirements, protect against vulnerabilities, and safeguard critical assets. Compliance with security standards helps organisations mitigate risks, prevent data breaches, and maintain the integrity, confidentiality, and availability of their digital infrastructure. Moreover this improves customer trust and loyalty, cost savings, and risk reduction in the procurement process itself. Identifying critical security standards helps organisations to create "conformance specifications" where suppliers would understand and be familiar with requirements.

4. Methods: Global survey of procurement guidance

With this framing and these definitions in mind, we seek to find a connection on the influence of procurement on the security of the Internet as a public infrastructure.

The aim of this research is to document what has been done by others and identify actionable areas for developing guidance and future research. First, we conducted basic desk research to answer “What has been done by others on procurement and supply chain management guidance”? Then, we developed a decision matrix to narrow in on global institutions within the UN IGF’s sphere of influence and impact to choose which cases to include in our research. We then collected and documented existing procurement and supply chain policies of those institutions. An outreach exercise to request for government and regional bodies procurement documents reached more than 2000 industry players, and governments. We received relevant documents from the IS3C working group members and the IGF community at large, and where required, we conducted interviews to get more insights into some of the documents.

For each document we reviewed, we asked the following research questions:

1. What has been published on procurement and cybersecurity standards already?
2. Are there any companies that publish their procurement and supply chain policies?
3. What procurement policy/documents focus on Internet and digital comms?

When searching for new primary sources, we ask, “What are the multilateral fora that publish best practice related to supply chain and procurement?” We sifted the data on existing and previous initiatives to identify a) common elements of best practice; b) shared problems barriers; and c) Global North and Global South applicability. We also identify gaps for future research needed to inform sound policy guidance in the second phase, or potentially in place of it.

5. Findings: Security standards in technology procurement policies

Technology standards are a set of functional specifications and processes that are developed to achieve purposes such as interoperability, better coordination and cybersecurity. Open standards have existed to serve public interests: such as to protect Internet infrastructure and organisations through no cost, or low cost implementation, provide better security safeguards for users and promote wider coordination in maintaining cyber resilience. The "open" in open security standards means that the process of developing these standards are open for participation by any stakeholder and that the standards are freely published for everyone to access.

Much of the evolution of the Internet has been based on layered, open technology standards, with the vision of the Internet being open for end innovation by any players across the globe. While the early developments of the Internet did not put much, if any, emphasis on security. As Vint Cerf explains[2]:

> *"Four decades ago, when Bob Kahn and I were creating the TCP/IP networking protocol for the Internet, we did not know that we were laying the tracks for what would become the digital superhighway that powers everything in society from modern business to interpersonal relationships"*].

This has changed. The threats posed by attacks on and abuse of the Internet and ICTs over the last two decades have underscored the need to develop cybersecurity standards to promote and maintain an Internet architecture that is secure for everyone to use by design. A wide array of standards development organisations (SDOs) cover technical cybersecurity include the Institute of Electrical and Electronics Engineers (IEEE), US National Institute of Standards and Technology, Open Worldwide Application Security Project (OWASP), the Internet Engineering Task Force (IETF) and the International Organization for Standardization (ISO). Policy standards are developed by regional bodies such as the European Union and African Union, and through international cooperation: countries coming together to develop and harmonise laws to facilitate coordination of cybersecurity measures across borders.

Successful standards are measured by how wide they are used across geographies and industries. In this study, we ask how national governments and regional bodies use open cybersecurity standards through the analysis of public procurement policy documents.

We find policy documents regarding cybersecurity and procurement to be concentrated in the Global North. This does not mean that these regions do have cybersecurity policies that apply in

[2] See: Quartz (2019), *Internet Pioneer Vint Cerf on What we Need to Do to Fix the Web,* https://qz.com/1703322/Internet-pioneer-vint-cerf-on-what-we-need-to-do-to-fix-the-web/ Accessed on 13th July, 2023

procuring goods, but it could mean that these documents are either not online or not searchable by the search engines. But more noteworthy, it could also mean that not much work has been done to enhance cybersecurity during procurement of goods and services. Although direct use and reference to the international cybersecurity standards are missing in most of the documents we analysed, these documents, as national or regional guidelines, provide some sort of standardisation. For example requiring that service providers should follow standards in the EU's Global Data Protection Regulation and International Organization for Standardization standards.

Mapping cybersecurity standards to identify areas that have been less covered is a futile exercise because of its wide scope. Every industry will have its own standards and therefore it is hard to exhaust the list of all standards. In this literature review, we instead analyse the security standards elements in procurement documents to uncover how public bodies have relied on the existence of open standards to enhance cybersecurity in the procurement of ICT products. To map out the trends and areas of focus, we organise the literature according to the US's National Institute of Standards and Technology's (US NIST) five core cybersecurity functions: Identify, Protect, Detect, Respond and Recover. This framework builds an actionable and robust cybersecurity legal and technical model for organisations and businesses and US NIST standards are the most widely adopted cybersecurity standards. Fifty-eight percent of respondents in a 2018 study conducted by HIMSS (2018), adopted the US NIST framework for their own cybersecurity policy and standards. The US NIST standards provide a holistic framework of cybersecurity resilience, including technical, administrative and government related standardisation. This helps us map out the trends on cybersecurity standardisations across these functions of cybersecurity resilience.

A. Identify

Under the US NIST framework, the 'identify' function is the first action that lays the groundwork for the other core functions. It entails developing an understanding of the organisation and its cybersecurity resilience and maturity, as well as understanding how the cybersecurity risks relate and would affect core functions of the organisation. Activities in this stage include assessments of assets, governance frameworks, and people's understanding of cybersecurity within the organisation. In principle, all awareness raising documents fall in this category, but perhaps a leading example of awareness raising of cybersecurity standards is the US NIST (2018) document mapping IoT security standards among the US public and public agencies, highlighting their status of implementation. It not only promotes the use of already established standards, but also encourages government agencies to participate in international standards development bodies based on their missions and cite the appropriate standards in their procurement. At a national level, the guidance directs government agencies to work with industry to support the development of appropriate conformity schemes to the requirements in such standards.

Another example is the UK government publication, that is meant to guide organisations through the identify process, help them understand what needs to be protected and why, know their suppliers, understand security risks posed by their supply chain, communicate their view of security needs, raise awareness, provide support for security incidents, and build assurance activities into management approach, encourage continuous improvement, and build trust with suppliers (UK Government, 2018). This is reflected in the implementation guide, “Global Standard for Procurement and Supply” by the Chartered Institute of Procurement & Supply (CIPS), now in its 4th version as of 2021, in which understanding needs and security risks sets the stage for procurement and supply.

Regionally, while documenting good practices for cybersecurity in procurement, European Union Agency for Cybersecurity (ENISA) provides a good example on using open standards in mapping of ICT procurement in healthcare. In this document, ENISA has recommended the ISO 27000 family for security protocols that include; clinical information systems, remote care systems, and identification systems. Other standards included in the document as best practice are the OWASP, and global policy frameworks such as the GDPR, and European National Cybersecurity policy frameworks.

Many procurement and cybersecurity awareness guidance documents have also encouraged periodical and wholesome assessments of systems. For example, the guidelines for the Kingdom of the Netherlands (2022) advise that in procurement, the supplier should allow the client to be able to make their own independent security audit and penetration testing.

On the supply chain management, the identify functions entails identifying risks from suppliers and their products, including third party suppliers, through periodical evaluation. A good example here is a guide by the New Zealand government which aims to help business leaders and cybersecurity professionals to identify supply chain entities and supplier management processes, assess the cyber threat landscape and determine which suppliers are most critical to establish effective processes for managing supply chain risk. (New Zealand Government, n.d.)

B. Protect

The ‘protect’ function involves setting measures to limit or contain potential cybersecurity risks. Functions under this category may include organisation and country policy development, training and awareness raising, putting measures for protecting data, and maintenance.

Various government documents on chain management have called for an enabling policy environment so that organisations are able to protect themselves and respond to attacks. For example, requiring suppliers from foreign countries to adhere to regulations such as the Budapest Convention, facilitates coordination at a regional level. The Taiwanese Government Procurement Act (2019) requires that the procurement of ICT products and services from foreign entities and their implementation should follow international treaties that Taiwan is party to, and creates avenues for coordination between government agencies when it comes to procurement concerning national security. For example, it provides for consultation with relevant government agencies when procurement touches on matters of national security. This presents an opportunity for open standards bodies to integrate these international standards into their work, and encourage countries and regions to harmonise policies to facilitate such coordination in protecting systems. Of course the downside of such large scale regional standardisation would mean that cybersecurity threats would also be large scale.

The government of Netherlands guidance on trustworthiness of consumers requires that suppliers should follow the principle of security by design. It also proposes that the supplier is obliged to provide maintenance updates. For the Czech Republic, the concept of security by design will be embedded in the whole public procurement process. In line with its national public procurement act, the National Cybersecurity act which comes into force in 2024 will allow clients to terminate contracts of suppliers whose services are not in line with the cybersecurity act. And to minimise loss from the suppliers, the procuring, in their request for services, are required to set out service specification requirements in line with the cybersecurity act (email response from a member of IS3C Working Group, 2023).

Both worth noting and recommendable, is countries directly adopting standards from other well established nations. For example, Poland adopted the US NIST standards to develop its own (Republic of Poland, n.d). This provides policy coherence, especially where there are trade functions between countries. The downside however, the countries may miss out on prioritising policy harmonisation with their neighbouring countries and trade blocks, which are also crucial for coordinated protection and response. Similarly Bahamas, in its own policy document notes, “the technical specifications shall, to the extent compatible with national requirements, be based on international standards or standards widely used in international trade." (Bahamas Public Procurement Act, 2021).

C. Detect

The ‘detect’ function defines activities that would enable organisations to detect cybersecurity attacks as soon as they occur. It may involve setting up continuous monitoring mechanisms that detect anomalies in the systems.

The supply chain documents we came across called for continuous monitoring of systems to detect cybersecurity threats in time, but also went further to call for continuous relationship between clients and their service providers to ensure vulnerabilities detected by the suppliers are communicated as soon as they occur. The guidance by the Australian government (2023) puts emphasis on risk management activities to be conducted during the earliest possible stage of procurement to manage jurisdictional, governance, privacy and security risks. The Kingdom of Netherlands advises that apart from providing the clients with maintenance updates, suppliers should also be willing to report on the vulnerability of their solutions at the time of provision and those that emerge in the future.

D. Respond

The ‘respond’ function contains activities put in place to contain cybersecurity incidents. This includes both long term and short term measures to control the spread of cybersecurity attacks.

It may also involve setting up crisis communication mechanisms, frameworks/channels for coordination and analysis to draw lessons learnt for better response in future.

The respond function actually employs the standards already in place to contain cyberthreats. For example, building collaborative networks for coordination, and information sharing could help mitigate cyberthreats. The Trusted Automated Exchange of Indicator Information (TAXII) defines protocols for services and message exchange that "*enable sharing of actionable cyber threat information across organisation and product/service boundaries."* (OASIS Open, 2016)

E. Recover

The 'recover' function not only contains a set of activities that restores the organisation to how it was, but also sets up activities to implement actions from the lessons learnt. It therefore might include setting up measures that were not there before to prevent a repeat cyber threat, and these might be the same measures set in the aforementioned cybersecurity functions. For example, if there were security gaps before the incident, or if the security protocols in place were interfered with, the recover function gives guidelines to restore them back in place. Because it mainly relies on the ability of organisations to learn from incidents, standards on information exchange would be helpful here.

"Security governance" is defined as a broad concept within the document "System security and certification considerations" by the European Cybersecurity Organisation (2021), in which security lifecycle, threat landscape evolution all recognise the pervasive reality of design challenges within security architectures, bringing a cyclical and reflexive approach to all stages from identify to recover into processes that can inform or implicate both supply chain management and procurement of technology tools.

6. Conclusions: Best practice and gaps

GDPR

At the very best level of standards harmonisation is the use of regionally developed policies to procurement policies and guidelines. The GDPR in the European Union, for example, has provided opportunities for common understanding and harmonisation with regards to the security of information systems. The GDPR recognises that there are risks in data processing, and therefore obliges data processors to put in place state of the art kind of protection. As such, putting in place standards such as the ISO 27000 series standards does not necessarily mean full compliance to the GDPR though in practice, these standards are considered as 'state of the art' measures of protection in data processing and management.

Comply or explain

The approach of the Dutch Ministry of the Interior and Kingdom Relations towards all levels of government is close to mandatory on the topic of standards deployment. The 'Pas-Toe-Leg-Uit

Lijst'[3] (comply-or-explain list) of the Standardisation Forum (Forum Standaardisatie) is a document containing 43 open standards that all governments in the Netherlands have to demand when procuring ICTs, unless there is a very good reason not to do so. The comply-or-explain list was created with a few criteria in mind. The basis for this selection is the criterion of interoperability. With interoperability comes an interdependency where security is concerned, in the sense that the use of an insecure standard affects all concerned and the deployment of the latest standards secures all simultaneously. Often there is no first mover advantage for industry. The government can stimulate deployment by demand. Further criteria are: they have to be security related, available through an open process and proven to work, e.g. by way of successful deployment by others[4].

Internet.nl

Under this Forum, the Platform Internet Standards operates a checking tool to track standards adoption called Internet.nl[5]. It raises awareness of the deployment of certain Internet standards for all organisations and allows the general public to test the deployed level of security of an organisation based on three indicators: website, email and connection. When a website is analysed with the tool, it automatically tests whether the website has deployed the following standards: DNSSEC, TLS, SPF, DMARC, DKIM, HTTPS, StartTLS, and IPv6. The Internet.nl software is open source and available for all countries to adopt. Currently, as far as known, the software has been adopted in Australia, Brazil, Denmark, Portugal and Singapore.

While this report focussed on the presence of security standards in procurement and supply chain management policies, this does not mean that the global Internet governance community should not consider wider topics around procurement and supply chain. We note that supplier ethics is a critical piece worth further investigation.

7. Future work: High level guidance

From this exercise, we note the following trends in procurement and cybersecurity, though it is important to note that these cannot be the generalisations of all public procurement trends because not enough documents have been analysed, which is in itself an area for future work.

1. There are many awareness documents targeting businesses, organisations and government agencies, however, none of these guidelines make use of open cybersecurity standards as points of reference, besides they provide at best guidance and advise of a voluntary nature.
2. A number of government procurement regulations in relation to cybersecurity procurement e.g. Finland and Taiwan point to the compliance of international treaties.

[3] https://www.forumstandaardisatie.nl/open-standaarden/verplicht

[4] After finalising the report, in IS3C WG 5 it was pointed out that both Denmark and Norway have documents on security, but not in combination with government procurement. Denmark: "Minimum technical requirements for government agencies", Norway: "Standards for the public sector"

[5] https://Internet.nl/

This demonstrates an opportunity for the role of international institutions like the IGF to provide guidance on technical and policy standards.

3. Many government ministries do not have a standalone document addressing cybersecurity standards in the procurement of ICT and electronic services. At best, they have procurement of cybersecurity products.
4. General public procurement regulations do not give provisions of guidelines to ensure cybersecurity safeguards, which is fine, but they also don't give directions for the development of frameworks to enhance cybersecurity in the procurement of ICT goods and services.
5. In general, procurement documents touching on cybersecurity standards focus on reducing disruptions. For example, they address interoperability and the ability of internal handlers to continue to be familiar with the systems for maintenance and to be able to tackle unforeseen challenges. These are mostly addressed in the requirements for proper documentation before and after service provision.
6. There seems to be little coordination among industry and public agencies in how these standards are applied, mostly because of lack of awareness by these agencies and lack of coordination among the standards setting bodies themselves.

Recommendations

Specific use of open standards is conspicuously missing in the procurement documents we analysed. Based on this work we see the need for a fit for purpose suite of materials aimed at decision makers. These might include guidelines, checklists, or other educational toolkits. For future policy recommendations it is critical to identify to whom recommendations will be made: government procurement agencies; trade and industry bodies; tech sector; standards body liaisons; and others.

As much as there are already existing standards to promote security in cyberspace, there could be a lack of understanding and cooperation between regional and national bodies with regards to the wider aims of promoting cybersecurity on the Internet. Next steps should therefore look at developing a best practice toolkit that guides organisations on how to use open international cybersecurity standards, not only for their own cybersecurity resilience, but also for better coordination in efforts to promote a secure cyberspace for all. The toolkit will look at how procurement bodies can integrate international cybersecurity standards with national cybersecurity strategies, regional policies, as well as developing national standards for cybersecurity considering the different cybersecurity priorities for different countries and regions.

Upcoming IS3C toolkit and guideline

In the coming months IS3C will present two tools from two working groups. Working Group 5, ‘Prioritizing and listing existing, security-related Internet standards and ICT best practices’, is in the process of creating a list containing the most urgent and important Internet standards and ICT best practices for organisations to consider when procuring ICT or renegotiating existing contracts. This concept list is on public consultation between 10 October and 5 November. You are invited to join this process. Working Group 8, ‘DNSSEC and RPKI deployment’, will provide a guideline on how to convince decision-takers to include cybersecurity and more specifically the aforementioned standards and best practices in procurement processes. For more information, see https://is3coalition.org/.

8. Acknowledgements

The authors would like to offer many thanks to the DC IS3C members who provided feedback on the very early concept of this working group. Thank you to Abraham Selby for communications support and the design and layout of this report. Special thanks to the DC IS3C coordinator Wout de Natris and senior policy advisor Mark Carvell. We also thank the community members for providing support in locating resources relevant to this research and their expertise. For this, we specifically thank Consettina Cassa, Karolína Menšíková, and Timothy Asiedu. This research was supported by RIPE NCC Community Projects Fund 2022. We welcome participation from a wide range of geographies and stakeholder groups on future work.

A. Annex: Bibliography of policy documents

African Union. (2016). *National Procurement Manual*. African Union. Retrieved May 12, 2023, from https://au.int/sites/default/files/documents/36320-doc-african_union_procurement_manual_v._2.0_-_2016-1.pdf

Australian Government. (2023, March 2). *Guidelines for Procurement and Outsourcing | Cyber.gov.au*. Australian Cyber Security Centre. Retrieved May 19, 2023, from https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-procurement-and-outsourcing

Bahamas. (2021). *Public Procurement Act*. The Parliament of the Bahamas. Retrieved Sept 28, 2023, from https://laws.bahamas.gov.bs/cms/images/LEGISLATION/PRINCIPAL/2021/2021-0007/PublicProcurementAct2021_1.pdf

ECS. (2021). *System security and certification considerations*. European Cybersecurity Organisation: WG 1 – Standardisation, certification and supply chain management. Retrieved Sept 28, 2023, from https://ecs-org.eu/ecso-uploads/2022/10/61ebc4a13b567.pdf

ENISA. (2020). *PROCUREMENT GUIDELINES FOR CYBERSECURITY IN HOSPITALS*. European Commission. Retrieved May 19, 2023, from https://ec.europa.eu/futurium/en/system/files/ged/procurement_guidelines_for_cybersecurity_in_hospitals.pdf

Government of India. (2019). *Public Procurement (prefference to make in India) for Cybersecurity Products*. https://www.meity.gov.in/. https://www.meity.gov.in/writereaddata/files/Public_Procurement_(Preference_to_make_in_India)_order_2019_for_Cyber_Security_Products.pdf

Government of Taiwan. (2019). *Government Procurement Act*. Laws & Regulations Database of The Republic of China (Taiwan). Retrieved May 19, 2023, from https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=A0030057

Kingdom of Netherlands. (2022, January 12). *Non-paper on the principles of a Cyber Resilience Act*. The Netherlands at International Organisations. Retrieved May 12, 2023, from https://www.permanentrepresentations.nl/permanent-representations/pr-eu-brussels/documents/publications/2022/01/12/non-paper-on-the-principles-of-a-cyber-resilience-act

National Cyber Security Centre. (n.d.). *Supply Chain Cybersecurity*. National Cyber Security Centre. Retrieved May 19, 2023, from https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-Supply-Chain-Cyber-Security.pdf

National Institute for Standards and Technology. (2018, February 14). *Draft NISTIR 8200, Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT)*. NIST Computer Security Resource Center. Retrieved May 19, 2023, from https://csrc.nist.gov/csrc/media/publications/nistir/8200/draft/documents/nistir8200-draft.pdf

New Zealand Government. (n.d.). *Supply Chain Cybersecurity*. National Cyber Security Centre. Retrieved May 19, 2023, from https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-Supply-Chain-Cyber-Security.pdf

Purser, S. (2014). Standards for Cyber Security. In *Best Practices in Computer Network Defense: Incident Detection and Response* (Vol. 35, pp. 97-106). IOS Press. 10.3233/978-1-61499-372-8-107

Republic of Poland. (n.d). *Narodowe Standardy Cyberbezpieczeństwa - Baza wiedzy - Portal Gov.pl*. Gov.pl. Retrieved June 25, 2023, from https://www.gov.pl/web/baza-wiedzy/narodowe-standardy-cyber

UK Government. (2018). *Supply chain security guidance - NCSC.GOV.UK*. National Cyber Security Centre. Retrieved May 19, 2023, from https://www.ncsc.gov.uk/collection/supply-chain-security