
# Prioritising security-related Internet standards and ICT best practices

An IS3C toolkit by the

Working Group 5 Advisory Panel

4 December 2023

# 1. Introduction

The UN Internet Governance Forum's Dynamic Coalition on Internet Standards, Security and Safety (IS3C) has compiled a list, called 'Checklist of Internet standards for secure communications', of the most important and critical security-related Internet standards which the coalition's members believe that all public administrations and private organisations should require to be integrated in the design of the ICT products, services or devices which they procure.

This finalisation of the list follows a round of public consultations on a draft compilation of key standards undertaken by an advisory panel of senior experts and a presentation at the annual Internet Governance Forum held in Kyoto in October 2023. The panel's decisions were made on a rough consensus basis concerning the scope of this list and unanimity on the categories and standards to be included in it. No additional categories or individual Internet standards were proposed in the consultation process[1].

## *IS3C*

IS3C is a UN Internet Governance Forum Dynamic Coalition with the goal of making online activity and interaction more secure and safer by achieving more widespread and rapid deployment of existing, security-related Internet standards and best practices.

IS3C has recently published reports on security by design in the Internet of Things, on cybersecurity education and skills, and on procurement and supply chain management. You can find more information on IS3C, its reports and upcoming work on emerging technologies, data governance and data privacy, and ICT security by design decision making at https://is3coalition.org/.

## *Aim of IS3C's Working Group 5: Prioritising and listing security-related standards*

The aim of WG5, is to provide decision-takers and procurement managers with a list containing the most important security-related Internet standards such as HTTPS (Hypertext Transfer Protocol Secure) and DNSSEC (Domain Name System Security Extensions) and relevant best practices such as MANRS (Mutually Agreed Norms for Routing Security) and the OWASP (Open Web Application Security Project) top 10 on critical security risks. The IS3C list is intended to be a tool to enable them to take into account Internet security and safety requirements and to procure ICT products, services and devices that are secure by design. This will make their organisations as a whole more secure and safer.

As a first step, WG 5 convened an advisory panel of the following cybersecurity experts to develop the proposed list:

[1] One suggestion was made but this did not fit the current scope of this project.

- Adam Burns, Senior Technologist Free2go
- André Melancia, cybersecurity consultant
- Bart Knubben, Project Manager, Netherlands Standardisation Forum
- Nicolas Fiumarelli, Software and Networks Engineer, LACNIC (Internet registry for the Latin American and Caribbean regions)
- Nitin Walia, Director Xgenplus India
- Sam Goundar, Professor RMIT Vietnam
- Sankalp Basavaraj, Service Manager Zeiss Group
- Steven Tan, Senior Consultant, Cyber Security Agency of Singapore
- Zaher Qassrawi, cybersecurity consultant
- Wout de Natris, IS3C coordination and support

The panel started its work on the basis that in order to become more proactive where prevention of online harms is concerned, organisations should require the deployment of security standards and relevant best practices in their relationships with suppliers and service providers. At some point, all these standards and best practices need to be deployed because they contribute to a more secure Internet and safer ICT services, devices and products, thus a safer and more secure organisation. Furthermore, this will progressively reduce the level of costs required to mitigate the impact of cybersecurity threats and incidents.

The advisory panel accordingly focused on this question: how can decision-takers and procurement managers be assisted in taking decisions with security as a priority without having to navigate the increasingly complex range of international standards, norms and compatibility issues etc.? Their solution is to provide them with a list of the most relevant and critical security-related Internet standards and related best practices.

The project was funded by the RIPE NCC Community Projects Fund.

# 2. Background

## *Why is the Internet not secure by design?*

It is important to understand that most of the standards that make up the Internet were created in a time before it evolved as a global communication and information medium, at a time when only the military and employees of a limited number of U.S. universities communicated with each other through Internet connections. As “the father of the Internet” Vint Cerf explains:

> “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[2]".

The protocols or Internet standards were therefore created without security as a priority[3].

This mindset changed in the mid-1990s when the rest of the world started to go online and in particular when commercial businesses started to connect with people as consumers through their online marketing etc. Flaws in the standards that enable the Internet to function became rapidly apparent and exploitation of these flaws for criminal abuse became widespread. The existing Internet protocols needed updating and the technical community has worked hard to provide these updates and security enhancements.

Many of the standards on the IS3C list are the required updates and some have been in existence for over 20 years. However, their deployment in products and services remains far from effective and universal. The most likely explanation for this is that the Internet generally functions exceedingly well. It is almost always there. So why the need to pay for additional security. However, the counter argument is that not deploying the updated security standards puts every individual Internet user at risk.

Internet users are largely not aware of the importance of these standards because they are "under the hood", i.e. like the engine of a car, hidden from view. Additionally, economic network effects prevent users from fully benefiting immediately. There is a "first mover disadvantage" in the form of increased costs that are incurred for the organisation that deploys these standards in isolation. Therefore, to increase the scale of adoption, it is not only necessary to make it more transparent that the new and updated Internet standards are being used, but also to underscore the clear security benefits involved.

Cooperation and collective action is needed to achieve the critical mass of widespread deployment of these standards. Several open source testing tools are described below which IS3C believes will help to achieve this.

## *How can procurement help?*

The research published by IS3C's Working Group 3 based on the limited number of procurement documents that are publicly available, confirm that procurement contracts are generally not used to acquire products that are explicitly secure by design[4]. Imagine however a world where only those suppliers who are able to provide products that are secure by design are awarded contracts by public administrations and corporate businesses. It would be expected then that all vendors would scramble to provide products that comply with those security standards.

[2] Quartz https://qz.com/1703322/internet-pioneer-vint-cerf-on-what-we-need-to-do-to-fix-the-web/ (accessed 7-11-2019)
[3] Setting the standard. For a more secure and trustworthy Internet. Wout de Natris with Marten Porte (Haarlem, 2020)
[4] Procurement, supply chain management and the business case, Mallory Knodel, Liz Orembo, Wout de Natris, IS3C 2023. https://is3coalition.org/docs-category/research-reports/

If large organisations therefore start using their buying power to require up-to-date security as part of their procurement process for Internet products, devices and services, pressure would as a result be put on the designers, product developers, manufacturers and service providers to provide this enhanced level of security. If organisations around the world make the same requirements, they will as a consequence become available for individual users as well. It is often stated in developing countries that they can only receive off-the-shelf ICT products and services or nothing at all. This renders institutions and citizens vulnerable and insecure online. Indeed it is not that much different in developed countries. Only through cooperation and collaboration on a global level, starting with tools such as IS3C's 'Checklist of Internet standards for secure communications' can governments and commercial organisations start to take a stand on requiring products and services that are secure by design.

Many government administrations fail to recognise the importance of open standards in providing greater security and safety in their services to citizens and in their own internal processes. As a result they overlook the inclusion of specific standards requirements when drawing up their procurement contracts with vendors and suppliers.

Procurement processes can make a huge difference to levels of security and safety and IS3C's list is offered as a reference tool for decision-takers who need to decide on a higher level of ICT security.

### *Current lists of security standards provided by governments*

As far as WG5's advisory panel is aware[5], the Dutch government is the only one with a mandatory list of Internet standards that all levels of government have to comply with when procuring ICT products and services. This is called the 'Pas-Toe-Leg-Uit-Lijst' (translation: 'comply or explain list').

There are other governments with similar lists but they are not directly related to procurement. Examples are:

- **Denmark**: "Minimum technical requirements for government agencies"
- **Norway**: "Standards for the public sector"
- **India**: "Guidelines on Information Security Practices for Government Entities"
- **UASG**: "UASG 009 Quick Guide to Tender and Contractual Documents EN"

## 3. Scope and format of the IS3C list

### *Scope*

After an initial round of sharing ideas, it became clear that scoping needed to be the advisory panel's first task in order to establish the required basis for a practicable tool. The panel

[5] Ibidem

decided to focus therefore on Internet standards meeting the following criteria: 1) Interoperability; 2) Security-related; 3) Open process; and 4) Proven track record.

*1) Interoperability*

The open standards that this document focuses on make systems interoperable. For example, they enable providing secure connections to transport and route traffic securely over the Internet.

Due to network effects the value of these open standards increases with their usage. A standard will become increasingly effective when other stakeholders also deploy them. This means that there is an interdependency for these standards to be effective. The usage is needed both on the sender and receiver side. When an organisation deploys for example DNSSEC (signing), it makes itself secure but is not protected when others with whom it connects have not deployed DNSSEC (validation). So there are economic network effects that prevent users from fully benefiting immediately ("first mover disadvantage"). This is why mass adoption is important, the rationale behind all IS3C's working groups.

It is important to note that this scoping decision by the advisory panel excluded local measures that affect the end-user's security, such as having a firewall, logging of data flows and anti-virus provision. These sort of measures are all important but out of this scope.

*OWASP top 10*

One notable exception was made by the advisory panel with regard to the interoperability scoping, the OWASP top 10 (or 25) for website development. This is a security-related, open process that has a proven track record for closing security gaps. Although it is not directly aimed at interoperability, the panel considered its significance to be too great to ignore in the IS3C list.

*2) Security-related*

The deployment of all the standards prioritised in the IS3C list will make the Internet and ICT environment more secure and safer immediately and the threat level will become much lower as certain attacks abusing these Internet resources or standards would be no longer possible.

*3) Open process*

The standards listed by IS3C are developed in an open process conducted by established and open standards development organisations, e.g. IETF (Internet Engineering Task Force) and OWASP and are available for anyone to use. Standards that cannot be implemented freely because of intellectual property rights, such as vendor-specific proprietary standards or standards that are behind paywalls (e.g. ISO), are not included in IS3C's list.

*4) Proven track record*

All standards in the list are mature with a proven track record of deployment because they have already been implemented by vendors and are used by governments and other organisations.

## *Categories*

In the second phase the experts defined categories before looking at individual standards. They agreed on four categories: 1) data protection and privacy; 2) network and infrastructure security; 3) website and (web) application security and; 4) communication security.

It became clear that certain standards are applicable to more than one category. It was also agreed that cloud services should not be a separate category, as all four categories and most related standards are applicable to securing the cloud.

## *Standards v. Regulations*

The WG5 advisory panel considered the relationship between national, regional and international regulations and standards and decided not to include them in the IS3C list primarily because regulatory compliance is by definition mandatory whereas open standards are adopted and implemented on a voluntary basis.

For instance, while it was recognised that the EU's Global Data Protection Regulation (GDPR) has become a global benchmark for privacy and data governance, this does not make the GDPR an Internet standard. Furthermore, the GDPR does not create new standards that would lead to greater online privacy or a better data governance and in common with many regulations of this kind. Nonetheless several standards included in the IS3C list do assist GDPR compliance because they protect privacy and data on the Internet.

### *Consultation*

IS3C held an open consultation on the proposed list of standards from 8 October to 5 November 2023. The responses received generally endorsed the aims and approach taken by the advisory panel for developing the list and no changes were proposed for its scope, categories and the specific standards to be included in the list.

An additional proposal was to include environmental standards in the list. This was considered by the advisory panel and the consensus view was, that the list should focus specifically on Internet security and safety in its first iteration.

One respondent to the consultation reflected on how all standards inevitably come with potential downsides, e.g. as a result of human mistakes in their deployment. Although the advisory panel agreed this is a concern, this did not provide sufficient reason to disqualify important standards that are intended to deliver positive effects for online security.

# 4. Selected Internet standards and best practices

## *The List*

The final task of the advisory panel was to select individual Internet standards and ICT best practices under the identified categories. IS3C's advisory panel selected the following 23 security-related Internet standards and ICT best practices. IS3C recommends all organisations to adopt these standards in their ICT procurement processes decisions and related contractual requirements so they pro-actively close numerous attack vectors on and in their and other organisations' ICTs.

### Checklist of Internet standards for secure communications

| Category | Name | Specification | Standardisation organisation | Problem solved |
|---|---|---|---|---|
| Data protection and privacy | Referrer Policy | Referrer Policy | W3C | Prevention from sending info on the source URL to a visited web server |
| Data protection and privacy | DNS QNAME Minimisation | RFC 9156 | IETF | Less information to upstream authoritative name server |

| Category | Name | Specification | Standardisation organisation | Problem solved |
|---|---|---|---|---|
| Network and Infrastructure[6] Security | TLS1.2/1.3 | RFC 8446<br>RFC 5246 | IETF | Encryption of connections |
| Network and Infrastructure Security | IPv6 | RFC 8200 | IETF | IP address that is not hindered by scarcity |
| Network and Infrastructure Security | DNSSEC | RFC 4033 | IETF | Provides integrity validation |
| Network and | RPKI | RFC 3779 | IETF | Authorisation |

[6] TLS 1.3 is the most secure version. However, TLS 1.2 can also be used sufficiently secure and can still be needed for interoperability reasons as not all systems offer TLS 1.3 support. Note that IETF only has 'deprecated' earlier TLS versions (1.0 and 1.1): https://www.rfc-editor.org/rfc/rfc8996.

| Category | Name | Specification | Standardisation organisation | Problem solved |
|---|---|---|---|---|
| Infrastructure Security | | RFC 6482<br>RFC 6811 | | for routing, preventing route leaks and hijacks |
| Network and Infrastructure Security | MANRS (including BCP38) | MANRS | Internet Society | Best practice for secure Internet routing preventing route incidents |
| Network and Infrastructure Security | DNS over HTTPS (DoH) | RFC 8484 | IETF | Encryption connection with name servers |
| Network and Infrastructure Security | DNS over TLS | RFC 7858 | IETF | Encryption connection with name servers |

| Category | Name | Specification | Standardisation organisation | Problem solved |
|---|---|---|---|---|
| Website and Web Application Security | HTTPS/HSTS | RFC 9011 | IETF | Secure, encrypted website connection |
| Website and Web Application Security | Content Security Policy (CSP) | CSP 2<br>CSP 3 | W3C | Guards a website against content injection attacks including cross-site scripting (XSS) |
| Website and Web Application Security | security.txt | RFC 9116 | IETF | Publishing contact information for security vulnerability reports |
| Website and Web Application | SAML | SAML | OASIS | Authentication and authorisation of users, including support for |

| Category | Name | Specification | Standardisation organisation | Problem solved |
|---|---|---|---|---|
| Security [7] | | | | single sign on |
| | OpenID Connect | OIDC | Open ID Foundation | Authentication of users, including support for single sign on |
| | OAuth 2.0 | RFC 6749 | IETF | Authentication and authorization for access to web applications |
| Website and Web Application Security | OWASP top 10 | OWASP top 10 | OWASP | Standard awareness document for developers and web application security |

| Category | Name | Specification | Organisation | Problem solved |
|---|---|---|---|---|
| Communication Security | SPF | RFC 7208 | IETF | Protection against email spoofing |
| Communication Security | DKIM | RFC 6376 | IETF | Protection against email spoofing |
| Communication Security | DMARC | RFC 7489 | IETF | Protection against email spoofing |
| Communication Security | STARTTLS/DANE | RFC 7672 | IETF | Authenticated encryption of email transport |
| Communication Security | OpenPGP | RFC 4880 | IETF | Email signing and email encryption |
| Communication | S/MIME | RFC 8551 | IETF | Email signing |

[7] All three standards in principle solve the same problem, which is single sign on and eventually authentication. The use cases will help decide which one best suits individual requirements. For example OpenID Connect is more suitable for mobile applications than SAML.

| Category | Name | Specification | Organisation | Problem solved |
|---|---|---|---|---|
| Security | | | | and email encryption |
| Communication Security | The Messaging Layer Security (MLS) Protocol | RFC 9420 | IETF | Encrypted (group) chat |

# 5. Compliance testing tools

## *Internet.nl*

The Dutch government offers Internet.nl (https://Internet.nl), a tool it developed with representatives of the Dutch technical Internet community. The software was developed as open source and is available for all to use. Based on the source code of Internet.nl Australia (https://aucheck.com.au), Brazil (https://top.nic.br) and Denmark (https://sikkerpånettet.dk) have launched test tools as well.

In November 2023 the Dutch government announced that Internet.nl has released a new version on GitHub[8]. "It makes deploying, developing, testing and scaling the code base much easier[9]. IS3C recommends that all governments do research into the applicability of the tool for testing Internet security and safety in their respective countries.

## *Internet.nl dashboard*

The dashboard of Internet.nl allows you to bulk scan in a single request modern Internet standards relating to thousands of Internet domains (including reports). (https://dashboard.Internet.nl/#/).

## *Internet Hygiene Portal*

The Singapore government offers the Internet Hygiene Portal (https://ihp.csa.gov.sg).

## *Webcheck.pt*

The Portuguese government in cooperation with the .pt registry maintains (https://webcheck.pt/).

*KINDNS*

KINDNS is an ICANN initiative to promote voluntary security best practices for authoritative and recursive DNS operators (https://kindns.org/)..

[8] https://github.com/internetstandards/Internet.nl/blob/main/documentation/Docker.md
[9] For more information, read here: https://en.internet.nl/article/release-1.8/