Press release

Guidelines on Cyber Security Specifications published

From Department of the Environment, Climate and Communications (/en/organisation/department-of-the-environment-climate-and-communications/)
Published on 1 June 2023
Last updated on 8 June 2023

Minister Ossian Smyth publishes guidance issued in relation to best practice cyber security requirements as part of an ICT procurement process

The Minister of State at the Department of the Environment, Climate and Communications, Ossian Smyth, today (1 June) published Guidelines on Cyber Security Specifications (ICT Procurement for Public Service Bodies) in line with the National Cyber Security Strategy 2019-24.

The guidelines have been prepared by Grant Thornton Ireland under contract with the National Cyber Security Centre (NCSC). This document is the first cyber security guidance issued to Irish Public Service Bodies (PSB) in relation to specific best practice cyber security requirements as part of an Information Communications Technology (ICT) procurement process.

The NCSC, Grant Thornton and relevant stakeholders worked collaboratively in the compilation of an authoritative "Guidelines on Cyber Security Specifications (ICT Procurement for Public Service Bodies)" for distribution and use throughout the Public Service. In addition, this document will be publicly available to support Small and Medium Enterprises (SMEs) where similar cyber security procurement concerns would apply.

Speaking today, Minister Smyth said:

"I welcome the publication of the Cyber Security Guidelines for ICT Procurement in Public Service Bodies. This marks a new departure in providing specific cyber security guidance to help assist Public Sector Bodies to embed cyber resilience into their ICT procurement planning and delivers on measures previously set out in the current National Cyber Security Strategy. These guidelines build on existing National Cyber Security Centre guidance, to further promote cyber security best practices as an integral consideration for Public Sector Bodies, helping to improve the resilience and security of public sector IT systems to better protect the services and the data that our people rely upon."

This publication reflects engagement with multiple stakeholders including relevant government, public bodies, policy makers, regulators, service providers, manufacturers, suppliers and cyber security experts which reflect a representative sample of subject matter experts. This advisory work is the first cyber security guidance issued to Irish PSBs in relation to specific best practice cyber security specifications as part of an ICT procurement process. These guidelines are dynamic in nature and will be subject to amendment and review in line with best practice and technical advances within the ICT ecosystem.

The guidelines aim to provide organisations with an improved understanding of cyber security risks and challenges to be addressed when specifying their requirements for ICT goods and services thereby helping raise the level of awareness in this area. They provide an easily understandable set of specifications that can be straightforwardly referenced by PSBs when they are planning the procurement of ICT goods and services. It addresses a range of cyber security domains including organisational practices, supply chain security (including risks such as data leaks, supply chain breaches, and malware attacks), evaluation considerations, and attestation information that may be required from suppliers when procuring ICT goods and services throughout the Plan, Source and Manage phase of the procurement process.

These guidelines aim to reinforce the Cyber Security Baseline Standards and current and future EU legislative proposals including the Network and Information Security (NIS) Directive and the NIS directive revision (NIS2) (https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333) and the EU Cyber Security Act Regulation. The publication also considers ongoing EU legislative proposals including the Cyber Resilience Act (https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act) which aim to address market needs and protect consumers from insecure products by expanding cybersecurity rules

to increase security on hardware and software products. The guidelines can be accessed on the Department of the Environment, Climate and Communications website. (/en/policy-information/5e101b-network-and-information-security-cyber-security/)

ENDS

Part of

Policies

Communications and Digital (/en/policy/435802-communications-and-digital/)

Rialtas na hÉireann
Government of Ireland

Manage cookie preferences

Manage preferences