An Roinn Comhshaoil,
Aeráide agus Cumarsáide
Department of the Environment,
Climate and Communications

NATIONAL CYBER SECURITY CENTRE

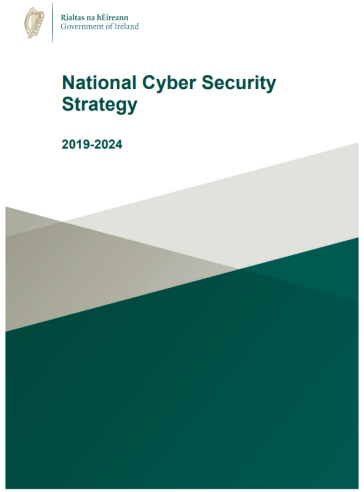
NCSC Work Update-
INEX 14th December 2023

An Roinn Comhshaoil,
Aeráide agus Cumarsáide
Department of the Environment,
Climate and Communications

OVERVIEW OF THE NATIONAL CYBER SECURITY CENTRE (2023)

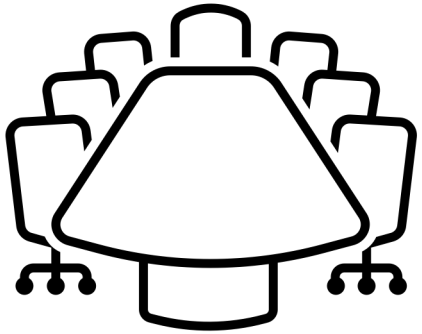
Mission

Leading Ireland's Response to Cyber Risk



National Cyber Security Strategy

Government Priority



Inter-Departmental Committee on Cyber Security

Reports to

National Cyber Security Centre

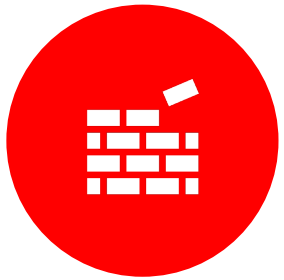
What we do

NATIONAL INCIDENT DETECTION & RESPONSE

RISK ANALYSIS & SITUATIONAL AWARENESS

ENGAGEMENT

CYBER RESILIENCE



NATIONAL CAPACITY DEVELOPMENT & RESEARCH

NCSC Growth

2011

- 4 staff
- Annual Budget €250k
- No infrastructure or formalised Incident Response Processes

2015

- 7 staff
- Annual Budget €750k
- First National Cyber Security Strategy
- Semi-formalised approach to IR
- Developing infrastructure with some automated analytics

2019

- 25 Staff
- Annual Budget €1.7m
- Second National Cyber Security Strategy
- NIS Directive implemented
- CSIRT accredited

  Full IR model

  Full infrastructure with several automated analysis tools

2023

- ~60 Staff
- Annual Budget €10.9m
- Mid term Review of 2nd National Cyber Security Strategy complete
- 3 year Technology Strategy underway
- Secure Facility
- Formalised information sharing arrangements in place
- National Cyber Risk Assessment conducted
- Public Sector Baseline Standard published.
- National Cyber Emergency Plan implemented.

NCSC Teams

Operations

- Security Operations
- Security and Liaison
- Risk Operations
- Active Cyber Defence
- Engineering

Resilience

- Capacity Development & Education
- Strategic Risk Management
- Compliance
- Engagement
- Certification
- Project Management

An Roinn Comhshaoil,
Aeráide agus Cumarsáide
Department of the Environment,
Climate and Communications

Mid – Term Review of the National Cyber Security Strategy-

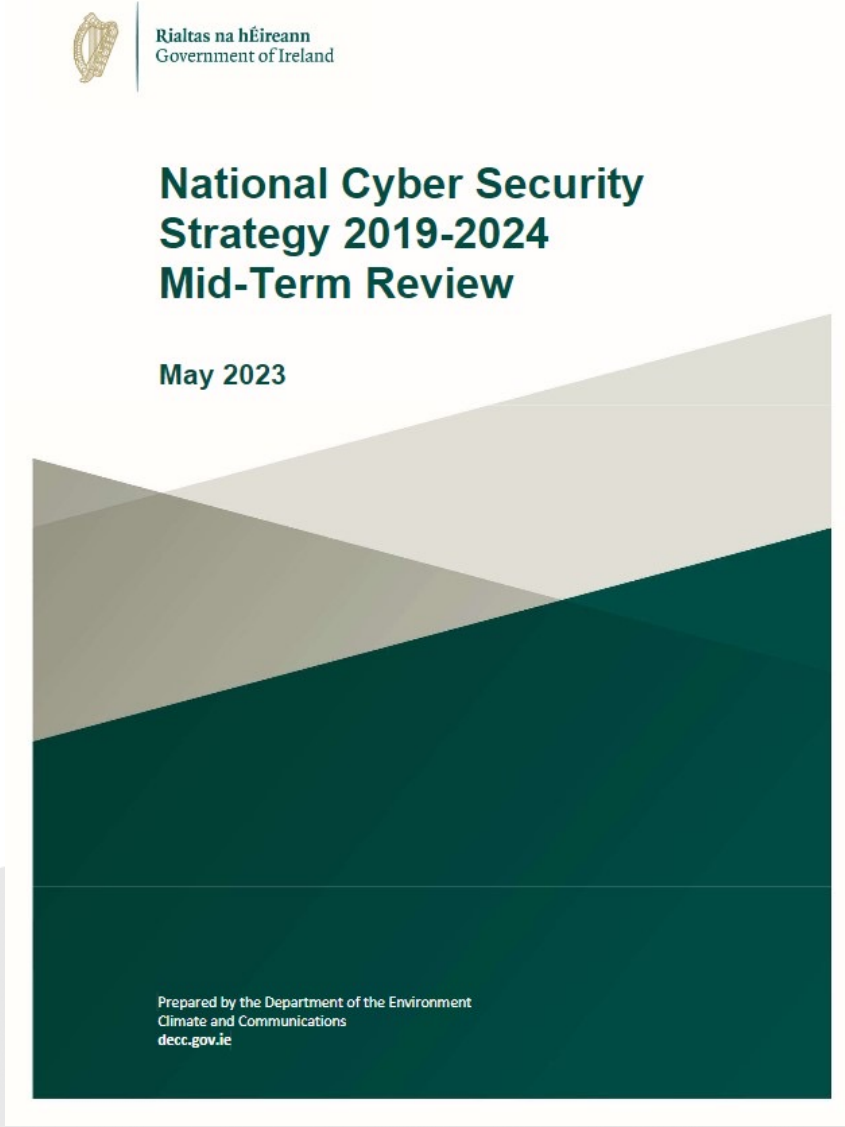
Measures to be Taken

Mid Term Review

The Mid-Term Review agreed by Government and launched on 28 June 2023.

Includes 18 New Measures to be implemented before the end of 2024.

Additional measures for oversight and accountability.



New Measures	
Measure 1	Continue to invest in the National Cyber Security Centre to expand its capacity to fulfil its mandate and ensure the NCSC has the required legal authority and technical capability to fully implement the revised Network and Information Security (NIS2) Directive from October 2024.
Measure 2	Continue to develop NCSC's ability to actively detect and defeat cyber threats targeting critical infrastructure and critical networks, including Government.
Measure 3	The NCSC will establish and lead a National Counter-Ransomware Task Force to coordinate efforts to respond to this severe cyber threat.
Measure 4	Develop an expanded programme of joint training and exercises between the NCSC, An Garda Síochána and the Defence Forces, to foster collaboration and enhance organisational capacity.
Measure 5	Develop further sectoral information sharing networks with relevant operators of critical national infrastructure and important industry sectors including Digital Infrastructure and Energy Sectors
Measure 6	Conduct an inter-agency risk assessment on supply chain risks including risk associated with relevant vendors in critical infrastructure, important industry sectors and the public sector[1], and make recommendations for Government on an appropriate policy response.
Measure 7	Establish a supervisory and enforcement regime for the revised EU Network and Information Security Directive (NIS2) and designate relevant bodies as National Competent Authorities and the Single Point of Contact.
Measure 8	Provide the NCSC with the necessary legal authority and technical capabilities to carry out security assessments of ICT systems for the handling of sensitive and confidential data.
Measure 9	Facilitate the ongoing development of a centralised repository of educational and apprenticeship courses in cybersecurity at all levels and throughout the country, and use this data to develop materials for schools, guidance counsellors and others to raise awareness of careers in cyber security and learning pathways.
Measure 10	Undertake market analysis for cyber skills to better understand supply and demand, the effectiveness of current interventions and priorities for future policy and strategy.
Measure 11	Support the development of the Irish cyber security research community to develop its capacity with a view to delivering a significant initiative in Cyber Security Research (Measure 14 of the 2019 Strategy).
Measure 12	Within the framework of the Government's strategy for digital, develop a whole-of-Government strategy for the development of the cyber security industry in Ireland to ensure the sector achieves its potential for growth.
Measure 13	Implement a financial support programme for SMEs and other societal stakeholders, in accordance with EU provisions, to improve cybersecurity resilience and facilitate innovation
Measure 14	Develop a voluntary cyber security standard for Irish SMEs aligned with relevant international standards
Measure 15	Publish Ireland's national position on the application of international law in cyberspace, to contribute to international efforts to clarify the applicable legal framework and promote responsible State behaviour in cyberspace.
Measure 16	Develop and publish on a more frequent basis tailored advice and guidance documents on steps that can be taken by citizens, SMEs, schools and educational institutions, and community and voluntary organisations to prevent and mitigate cyber security risks.
Measure 17	Establish an NCSC Advisory Council to be drawn from the cyber security industry and research community, as well as representatives of key stakeholders, to provide independent perspectives and input on strategy and policies.
Measure 18	From 2023, publish an annual update on the implementation of this Strategy, to ensure accountability and transparency in the delivery of these Measures.

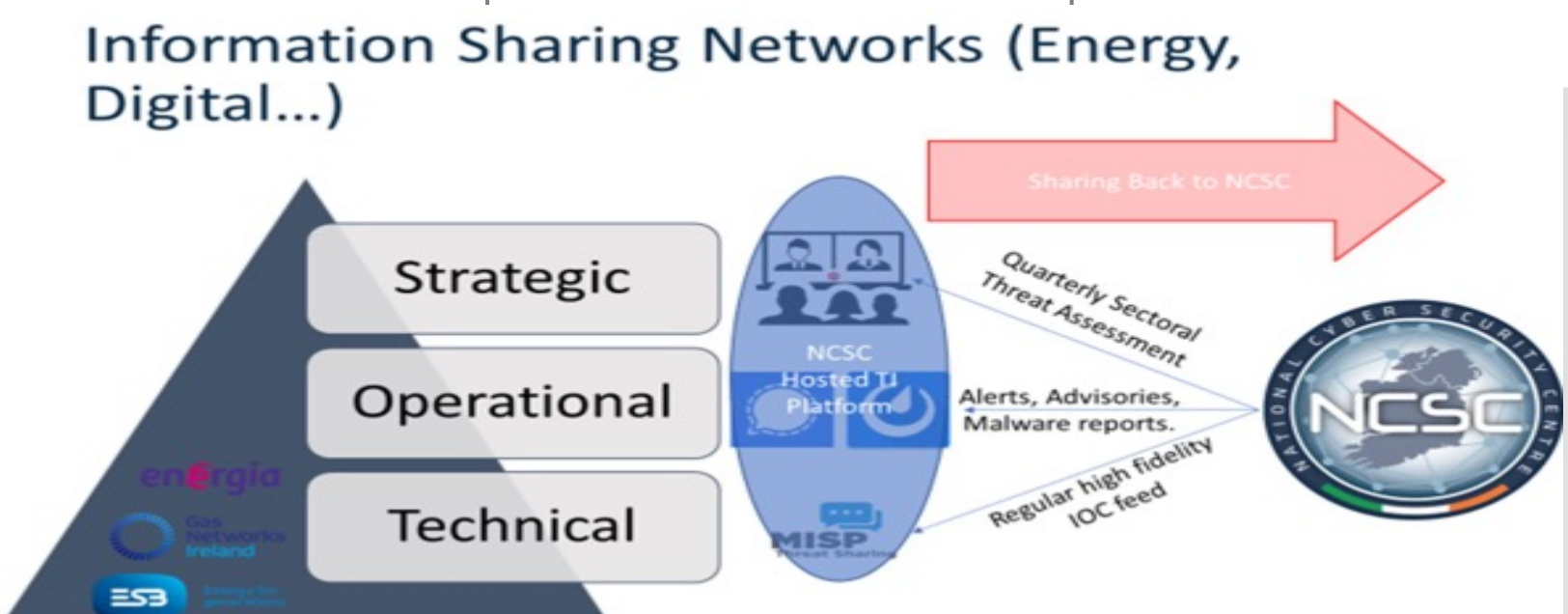
Measure 5	Develop further sectoral information sharing networks with relevant operators of critical national infrastructure and important industry sectors including Digital Infrastructure and Energy Sectors

Rialtas na hÉireann
Government of Ireland

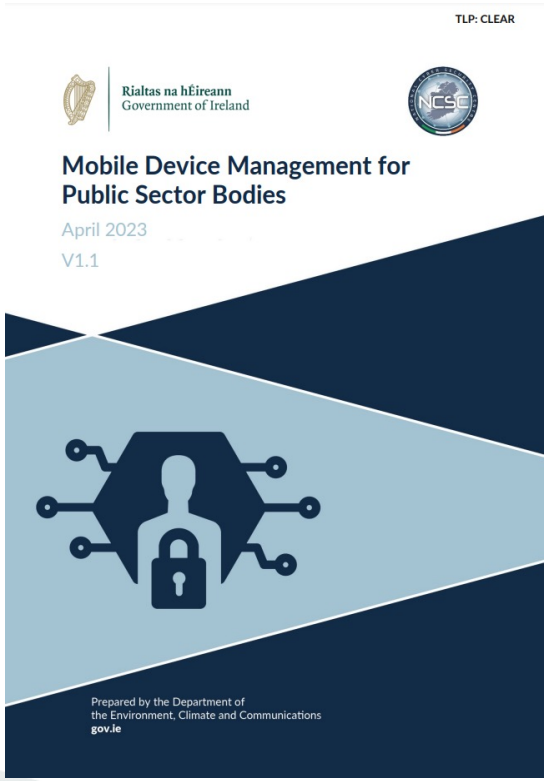
National Cyber Security Strategy

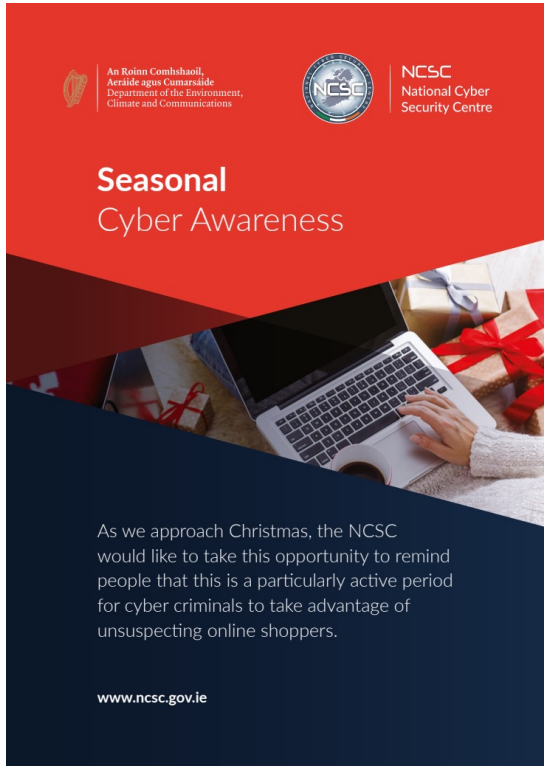
2019-2024

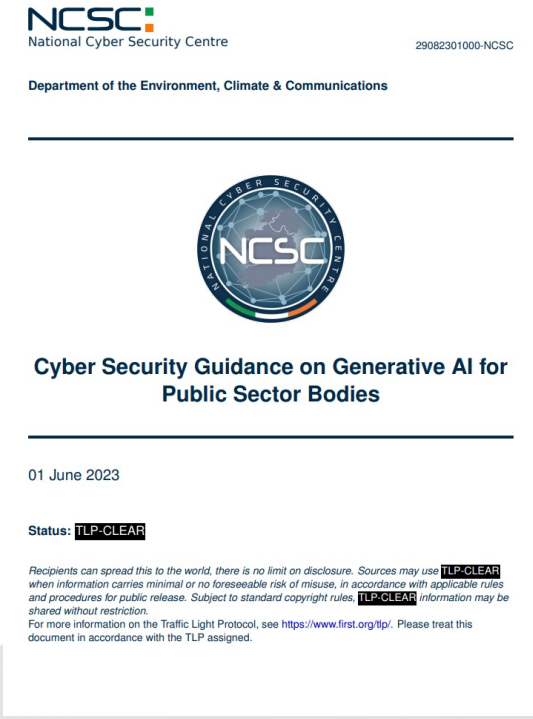
10	A Government IT Security Forum will be created, open to all Heads of IT Security across Government, to facilitate information sharing on best practice for cyber security and to allow the NCSC support the deployment of the baseline security standard.



Measure 16	Develop and publish on a more frequent basis tailored advice and guidance documents on steps that can be taken by citizens, SMEs, schools and educational institutions, and community and voluntary organisations to prevent and mitigate cyber security risks.






NCSC
National Cyber Security Centre

29082301000-NCSC

Department of the Environment, Climate & Communications

Cyber Security Guidance on Generative AI for Public Sector Bodies

01 June 2023

Status: TLP-CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP-CLEAR *when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules,* TLP-CLEAR *information may be shared without restriction.*
For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Measure 2	Continue to develop NCSC's ability to actively detect and defeat cyber threats targeting critical infrastructure and critical networks, including Government.

Active Cyber Defence 2024

Measure 7	Establish a supervisory and enforcement regime for the revised EU Network and Information Security Directive (NIS2) and designate relevant bodies as National Competent Authorities and the Single Point of Contact.

NCSC Role & Responsibility

- Registration of Essential and Important Entities
- Single Point of Contact
- Setting national cyber security standards and assisting NCAs
- All incident reports through NCSC / CSIRT
- Coordinated Vulnerability Disclosure (CVD)
- Information Sharing
- NIS Coop Gp, CyCLONe, CNW,

An Roinn Comhshaoil,
Aeráide agus Cumarsáide
Department of the Environment,
Climate and Communications

Q&A