8 Measures relating to national cyber security

8.1 The term 'cyber security' refers to the full range of measures designed to protect information and communications technology (ICT) systems and ensure the confidentiality, integrity and availability of data services. It encompasses the body of technologies, processes and practices designed to protect networks, devices, programmes and data from attack, damage or unauthorised access.

8.2 Disruption to critical information infrastructure and networks has been noted as a discrete strategic risk in the annual National Risk Assessment since 2014. In 2017, the assessment noted that "*the fact that Ireland is home to a large number of international data centres means that a serious attack or cyber-security failure could have a damaging impact not just on our reputation, but also on our economy*".[1]

8.3 Cyber attacks on critical systems are an ongoing threat globally. Such attacks include the December 2015 Ukrainian power grid attack and the May 2017 global cyber incident caused by the 'WannaCry2' worm. The former impacted 230,000 people who were left without power for up to six hours. The latter affected ICT systems globally; in the UK, the National Health Service was reduced to running emergency-only services in some locations as a result. In Ireland, a HSE-funded facility in Wexford was affected by 'WannaCry2'.

8.4 The Department of Communications, Climate Action and Environment (the Department) is responsible for cyber security policy in Ireland. It is also responsible for coordinating the governmental emergency response to any national-level cyber security incidents. The Department discharges these responsibilities through the National Cyber Security Centre.

8.5 The Department published the *National Cyber Security Strategy 2015-2017* in 2015. The strategy presents a framework for ensuring "*safe, secure and reliable*" interactions within cyberspace.

8.6 In July 2016, the European Union adopted a directive — the Directive on Security of Network and Information Systems (the Directive) — with a view to achieving a high common level of security within the EU. The Directive requires that the laws, regulations and administrative provisions necessary to comply with the Directive be adopted and published by 9 May 2018. The Minister for Communications, Climate Action and Environment (the Minister) gave effect to the Directive on 18 September 2018.[2]

8.7 This examination reviews the progress which has been made since the establishment of the National Cyber Security Centre.

1 Chapter 5: Technological Risks; *National Risk Assessment 2017, Overview of Strategic Risks*, Department of the Taoiseach, 29 August 2017.

2 Statutory Instrument number 360 of 2018, *European Union (Measures for a high common level of security of network and information systems) regulations 2018.*

National Cyber Security Centre

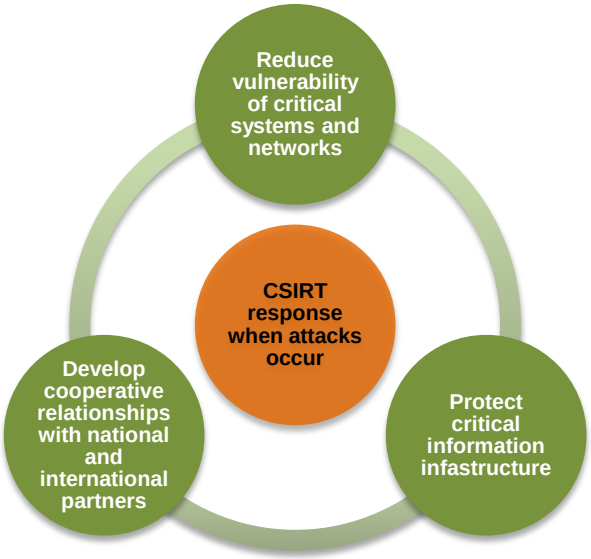
Mandate

8.8 The National Cyber Security Centre was established in 2011 following a Government decision.[1] The Centre is largely located in rental accommodation on the UCD campus. The Centre's primary focus is on securing government networks, on assisting industry and individuals in protecting their own systems and on securing critical national infrastructure.[2]

8.9 The National Cyber Security Centre contains the State's national/governmental Computer Security Incident Response Team (CSIRT-IE). Its functions include the enhancement of 'situational awareness' and the provision of incident response for national cyber security incidents.[3] The Computer Security Incident Response Team received 'Trusted Introducer' accreditation on 28 November 2017.[4]

8.10 The National Strategy sets out the mandate for the National Cyber Security Centre (see Figure 8.1).

Figure 8.1 National Cyber Security Centre mandate



Source: National Cyber Security Strategy 2015 — 2017

Resourcing

8.11 In the 2011 Government decision approving the National Cyber Security Centre, an initial resource allocation of €800,000 a year was approved. The allocation was to be used to set up the National Cyber Security Centre and the Computer Security Incident Response Team.

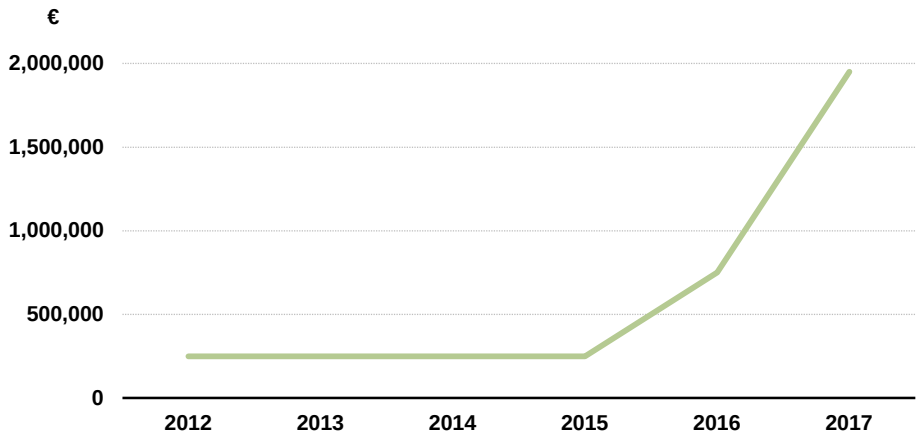
1 Government decision S180/20/10/481.

2 Critical national infrastructure comprises critical elements necessary for the delivery of essential services such as electricity, water, transportation, telecommunication, commerce and health.

3 Situational awareness is the perception of environmental factors and events in order to understand how information, events, and one's own actions will impact the environment immediately and in the future.

4 Trusted Introducer is a body established by the European Computer Emergency Response Team (CERT) community. It signifies to the bodies that the National Cyber Security Centre works with that the CSIRT has reached a required level of maturity and operational capacity.

Figure 8.2 National Cyber Security Centre budget allocation 2012 to 2017

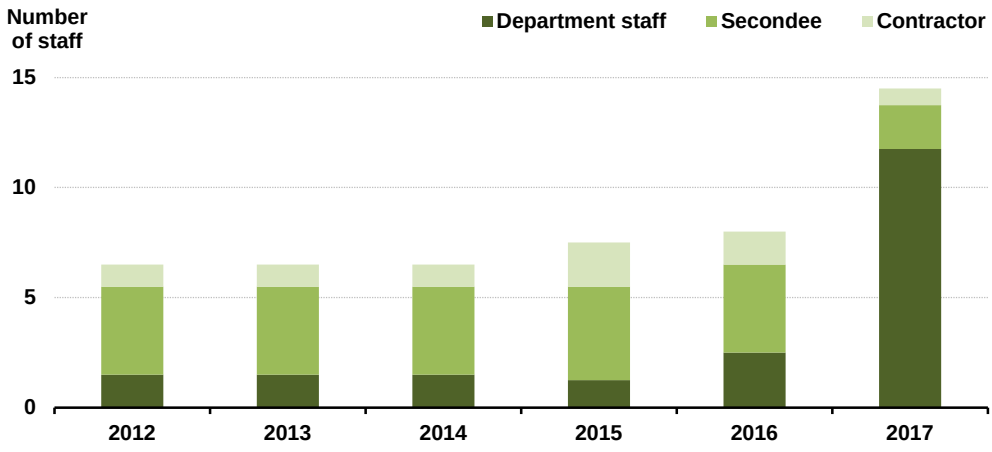


Source: Department of Communications, Climate Action and Environment

8.12 The Department's funding allocation for cyber security in the period 2012 to 2015 was less than a third of the amount approved in the 2011 Government decision (see Figure 8.2). In 2017, the allocation increased to €1.95 million. However, the Department does not routinely compile or publish expenditure relating to the National Cyber Security Centre.

8.13 Figure 8.3 indicates staffing levels for the National Cyber Security Centre since its establishment. The centre had a staff of 14.5 whole time equivalents (WTE) during 2017. In 2016, a permanent Head of Incident Response was appointed and a programme of recruitment for 2017 was agreed by the Department. The Department stated that approval was given in 2018 for the appointment of 16 further staff including a permanent Director and Chief Technical Officer.

Figure 8.3 Staffing (WTE) of the National Cyber Security Centre 2012 to 2017 [a,b]



Source: Department of Communications, Climate Action and Environment

Notes:
a WTE (whole time equivalent).
b Department staff includes time spent by principal officers in the Internet Policy Division (part of a WTE up to 2017 and 1 WTE since then).

8.14 The Department states that ensuring the National Cyber Security Centre had the correct mix of skills to deal with a dynamic and challenging area was difficult, as was the challenge of plotting a growth model for the organisation. As such, it states that the increase in staff numbers in 2017 was with reference to the developing understanding of the skills required.

National Cyber Security Strategy 2015-2017

8.15 The National Cyber Security Strategy (published July 2015) sets out 12 measures to be achieved over the lifetime of the strategy. A National Cyber Security Strategy Implementation Plan was also developed in 2015, setting out key targets and notes that reaching these targets will ensure all measures will be addressed.

8.16 An assessment of progress in achieving the measures set out in the strategy, based on the targets set out in the implementation plan, is summarised in Figure 8.4. As at May 2018, four measures had been completed, four measures had been partially implemented, and four measures had not been implemented.

8.17 The existing strategy covers the period 2015 to 2017. The Department has indicated that it expects to publish a new National Cyber Security Strategy by the end of 2018.

Figure 8.4 Progress assessment of strategy measures, as at May 2018

Establish the National Cyber Security Centre (NCSC) within the Department ▪ Accreditation of the Computer Security Incident Response Team — completed	●
Network and information security for public bodies ▪ Three specific training programmes were envisaged for key personnel in government departments. These programmes had not been rolled out. ▪ A security incident and event management system was not in place ▪ Provision of threat information through an 'alerts and advisory' mechanism to public sector participants was in place	◐
Coherent international engagement ▪ Contribution to the board of management of European Agency for the Security of Network and Information Systems was in place ▪ Bilateral engagement ongoing. NCSC participates in a number of working groups and workstreams	●
Fully implement the EU Directive by primary legislation ▪ The deadline for transposition was 9 May 2018. Transposition was achieved on 18 September 2018.	○
National security and policing ▪ The Strategy committed to a memorandum of understanding with An Garda Síochána — not completed	○
Cybercrime ▪ The Strategy committed to a memorandum of understanding with An Garda Síochána — not completed	○
Civil-military cooperation ▪ Service level agreement and a memorandum of understanding in place with the Department of Defence and Defence Forces	●
Protection of critical national infrastructure ▪ No mandatory reporting obligations as the Directive had not been transposed ▪ Provision of threat information through an 'alerts and advisory' mechanism in place ▪ The establishment of a Critical Information Infrastructure Initiative — a forum of critical system operators — not achieved	◐
Information sharing ▪ Engagement with industry and public sector bodies through agreed and established information sharing mechanisms ▪ Public engagement delivered by the Department's Press Office	●
Education and training ▪ Development of accredited training programmes with academic partners — not delivered ▪ Structured exercises for critical national infrastructure operators ongoing	◐
Public awareness ▪ 'Make IT secure' website was operational during the period from 2012 to early 2018 ▪ Further campaigns to raise public awareness — outstanding	◐
Relationship with third-level institutions ▪ A 'cyber security group' to be developed to lead interaction within the sector — not achieved ▪ The "use of memoranda of understanding…to support the developing research agenda in [the] sector" was envisaged, but had not been provided ▪ Relationship with UCD Centre for Cyber Crime Investigation not formalised	○

Source: National Cyber Security Strategy Implementation Plan 2015. Analysis by the Office of the Comptroller and Auditor General.

Note: ● Complete ◐ Partial progress ○ Not complete

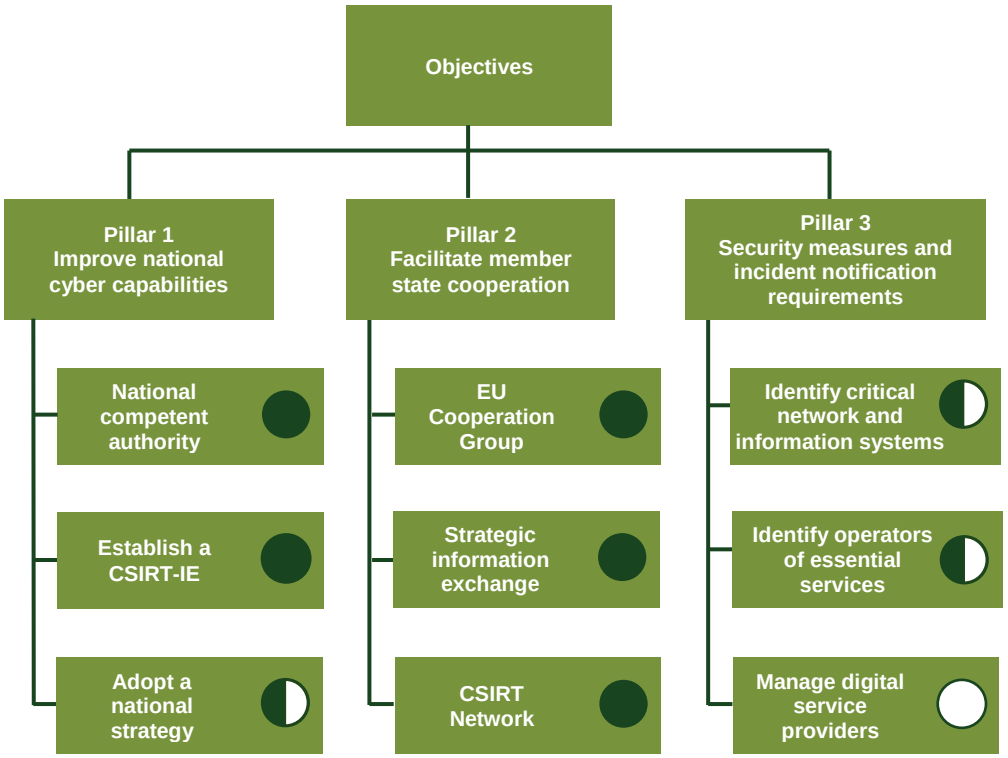
Network and Information Systems Directive

8.18 The EU Network and Information Systems Directive aims to improve the resilience of key network and information systems by addressing the following (referred to as 'pillars')

- improving cyber security capabilities of EU member states
- facilitating cooperation on cyber security among EU member states
- introducing security measures and incident reporting obligations for key sectors.[1]

8.19 The structure envisaged in the Directive for achieving these objectives is outlined in Figure 8.5.

Figure 8.5 Directive — Implementation approach



Source: Directive (EU) 2016/1148 of the European Parliament — Network and Information Systems Directive. Analysis by the Office of the Comptroller and Auditor General.

Notes: ● Complete.
◐ Partially implemented.
○ Not implemented.

1 Reporting requirements are not limited solely to cyber security incidents. The Directive defines an incident as any event having an actual adverse effect on the security of network and information security. For example, incidents relating to power and hardware failures, malware, intrusions, viruses or environmental hazards may be reported.

Pillar 1 — Improve national cyber capabilities

8.20 The Minister is designated as the national competent authority in the State in respect of operators of essential services (OESs) and digital service providers (DSPs).[1]

8.21 Structural requirements under pillar 1 have been put in place, but gaps remain in strategic planning. Figure 8.6 identifies the requirements for a national strategy specified in the Directive and indicates where Ireland's existing national strategy satisfies or meets the Directive requirement.

Figure 8.6 Requirements for a national strategy

The objectives and priorities for the management of cyber security in the national domain	●
A governance framework that defines the roles and responsibilities of relevant stakeholders	○
Identification of measures of preparedness, response and recovery, including cooperation between the public and private sectors	◐
An indication of the public engagement, education and training programmes relating to the national strategy	●
An indication of research and development plans relating to network and information systems strategy	●
A risk assessment plan to identify risks ▪ A general comment on risks is provided in the existing strategy	◐
A list of the various actors involved in the implementation of the national strategy on the security of network and information systems	○

Source: EU Directive on the Security of Network and Information Systems and National Cyber Security Strategy 2015–2017.

Notes: ● Present in existing strategy.
◐ Partial crossover with existing strategy.
○ No crossover with existing strategy.

1 The Central Bank of Ireland is designated as a competent authority in respect of operators of essential services in the banking and financial market infrastructure sectors.

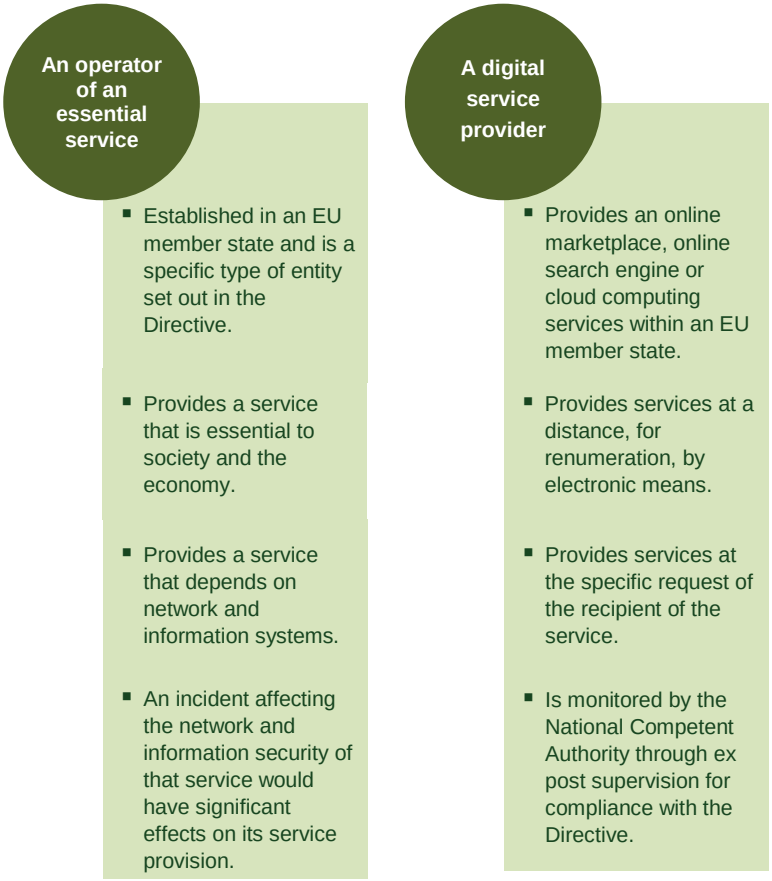
Pillar 2 — Facilitate member state cooperation

8.22 The EU Agency for Network and Information Security (ENISA) supports the development and implementation of the EU's policy and law in relation to network and information systems. The National Cyber Security Centre contributes two members to the board of ENISA in addition to participating in the core European working and cooperation groups, EU Co-operation Group and CSIRT Network. This facilitates the sharing of best practice regarding strategic, technical and other measures. In addition, the National Cyber Security Centre also conducts bilateral engagement with other National Cyber Security Centres and Computer Security Incident Response Teams.

Pillar 3 — Security and incident notification requirements

8.23 The Directive requires the identification of entities/enterprises that qualify as OES or DSP based on specified criteria (see Figure 8.7). Certain obligations arise under the Directive depending on the criteria that organisations meet.[1] Reportable incidents arise when disruption significantly impacts service provision above a certain threshold.[2]

Figure 8.7 Categorisation criteria for service providers



Source: Directive (EU) 2016/1148 of the European Parliament — Network and Information Systems Directive

1 Digital Service Providers with less than 50 employees and whose balance sheet total and/or annual turnover does not exceed €10 million are exempt from the security and notification requirements.

2 Article 6 of the Directive outlines the factors that constitute a 'significant disruptive effect'.

8.24 To date, the National Cyber Security Centre has identified approximately 60 entities as potential OESs in seven sectors specified in the Network and Information Systems Directive. The Minister has not yet completed formal designation of these entities as OESs.

8.25 There are obligations on the Minister as national competent authority to establish and maintain a register of OESs. The register must be reviewed on a regular basis, at least every two years.

8.26 A DSP providing a service in another EU state but headquartered in Ireland is considered the responsibility of the Irish authorities for cyber security purposes.

8.27 The Department notes that the State is responsible for dealing with the security of services provided across the EU by multinational companies (deemed DSPs under the Directive), that have their European headquarters located in Ireland. As a result, Ireland will have additional financial and administrative responsibility associated with acting as the *de facto* European security regulator, which will impact on resourcing requirements in the future.

8.28 The Minister has authority to require both OESs and DSPs to provide all information needed in order to assess the security of their network and information systems.

8.29 Furthermore, the Department published draft security measures and incident reporting guidelines for OESs and DSPs on 16 November 2017 for consultation. It is intended that these will be finalised following transposition of the Directive.

Governance and oversight

8.30 The Government decision in July 2011 approving the National Cyber Security Centre also approved the setting up of an interdepartmental committee to set and implement policy in relation to addressing the challenges of cyber security in Ireland. The group first met in December 2013. Minutes of only one meeting, dated February 2014 (noted as the third meeting) were available for review. The Department has indicated that its records suggest that the group met five times.

8.31 The National Cyber Security Centre Strategy Implementation Plan (2015) states that the overarching governance structure for the National Cyber Security Centre will remain the interdepartmental high level steering group, indicating the group would be reoriented to function as the oversight mechanism for all the work of the National Cyber Security Centre. The Department states that the committee has not met since the strategy was published in 2015.

8.32 The Department states that the committee consisted of an Assistant Secretary from the Department and the Department of the Taoiseach, an Assistant Commissioner from An Garda Síochána, a Principal Officer of the Department of Justice and Equality, a Colonel from the Defence Forces and a Counsellor from the Department of Foreign Affairs and Trade.

8.33 The Department stated that the Assistant Secretary with responsibility for telecommunications has policy and operational responsibility for the National Cyber Security Centre. The Secretary General is also briefed regularly on developments. There were no minutes or other evidence provided as to the regularity of briefings.

8.34 The Department stated that its Management Board considers cyber security from time to time. The Department provided the relevant extracts from the minutes of Management Board meetings (summarised in Figure 8.8).

Figure 8.8 Summary of Management Board minutes 2015 — June 2018

Meeting dates	Points recorded as having being discussed
2015 — June	Memo for Government relating to publishing the cyber security strategy. Delivery of the associated implementation plan.
2016 — January	Update provided on attacks on Government websites
2017 — Jan, Feb, Mar, May	Update from HR on progress with recruitment competitions for cyber security functions
2018 — April	Strategic priorities were discussed and agreed that the next presentation in May would cover cyber security
— May	Detailed presentation on the National Cyber Security Centre (NCSC) and its operations to date
— June	Update on accommodation and reference to additional NCSC staff

Source: Department of Communications, Climate Action and Environment

8.35 The Department further stated that a component for the next strategy will be the governance and oversight arrangements for the unit, based on international best practice and a draft organisation structure has already been considered by the Department.

8.36 The National Cyber Security Strategy Implementation Plan commits to publishing an annual report and to conducting a formal impact assessment of their work in late 2017. These are outstanding, though the work of the Centre is outlined in the Department's annual report.

8.37 The Department's Strategy Statement 2016 — 2019 outlines two performance indicators related to the work of the National Cyber Security Centre

- implementation of the EU Network and Information Systems Directive
- services response capacity developed to be able to engage in cyber security actions.

8.38 An assessment of the Centre's performance was formally requested from the Department. No evidence of an assessment having been carried out was provided. The Department stated that performance assessment of the work of the National Cyber Security Centre formed part of the normal performance management and corporate governance of the Department.

Conclusions and recommendations

National Cyber Security Centre

8.39 The National Cyber Security Centre performs a critical "whole-of-government" function. However, the level of resourcing in the first four years was significantly less than that initially envisaged.

Recommendation 8.1

It is recommended that the Department conducts a review of the resourcing of the National Cyber Security Centre in order to ensure that it is adequate to meet its obligations and development objectives.

Accounting Officer response

Agreed.

Reviews of the resourcing (people and ICT) of the National Cyber Security Centre have been conducted on a regular basis as part of the annual estimates process and most recently in 2017 as part of the assessment of requirements for the implementation of EU Directive on the Security of Network and Information Systems. Additional staff were recruited to the National Cyber Security Centre in 2017, and in line with the Department's 2018 Workforce Plan, a further significant cohort of staff, including a Director and Chief Technology Officer, will be recruited in 2018/2019. The issue of resourcing will be examined again in the context of the 2018 National Cyber Security Strategy.

8.40 The overall strategic direction of the National Cyber Security Centre is not clear. There is no strategic plan currently in place. Not all objectives in the previous strategy were achieved. The new timelines for delivery of these objectives and the relative priorities have not been set down. Where resources are limited, such clarity is particularly important.

Recommendation 8.2

It is recommended that an updated strategy document be finalised, which sets out objectives and related key performance indicators aligning them to planned and available resources.

Accounting Officer response

Agreed.

The context in which the 2015 Strategy was drafted ceased to apply very quickly. In the first instance, while the Strategy anticipated the Network and Information Systems Directive itself, the finalised Directive was substantially different from the draft that existed in mid-2015, both in terms of how critical infrastructure was to be treated and critically, due to the inclusion of the DSPs components.

The National Cyber Security Centre has always sought to benchmark itself against international best practice. The model outlined in the 2015 Strategy represented best practice given the threat environment at the time, but this changed substantially thereafter. Nationally, we have been involved in responding to incidents that were entirely unanticipated at the time of drafting; it was clearly not possible to ignore these. Entities such as the National Cyber Security Centre have to remain flexible and adaptive in order to remain effective. This reflects international experience also — in the global CSIRT community, focus has shifted significantly in the last number of years and we have followed suit to target our resources at the most pertinent threats.

Within the international CSIRT community, there is large-scale adoption of open-source technology and in-house tool development, at least in part due to the need to avoid vendor risk. While other areas of the public sector can incur significant expenditure on consultancy and software licencing and support, the National Cyber Security Centre has adopted a policy of using open-source technology, where possible. The traditional notion that increased current or capital spending correlates directly with output or capacity does not hold true for CSIRTs and National Cyber Security Centres in general.

As such, the strategic direction of the National Cyber Security Centre is entirely clear, and the general thrust of the 2015 strategy holds — to build capacity and to prepare for the entry into force of the Network and Information Systems Directive. However, circumstances have required that the roles and functions of the National Cyber Security Centre develop in somewhat different ways to that envisaged in the 2015 strategy. A National Cyber Security Strategy is one of the requirements of the Network and Information Systems Directive, and work is already underway on a revised strategy which is expected to be completed by the end of 2018. A steering group will be established to bring all relevant stakeholders together in order to fully inform the process. This strategy will capture developments in the cyber security area, and within the National Cyber Security Centre, and will set out governance arrangements for the centre, including how the National Cyber Security Centre functions with regard to the Government's Cabinet Committee F.

8.41 The memorandum of understanding with An Garda Síochána envisioned in the National Cyber Security Strategy remains outstanding. Clarification regarding the roles of each entity should facilitate effective and efficient investigation of cyber crimes and national security incidents.

Recommendation 8.3

It is recommended that the Department agree a memorandum of understanding with An Garda Síochána in order to ensure that resources and capabilities can be deployed in a targeted and efficient manner.

Accounting Officer response

Agreed.

A draft memorandum of understanding was sent by the Department to An Garda Síochána in 2017, and discussions are ongoing with a view to its finalisation as soon as possible.

However, operational effectiveness is not impeded, in any way, by the absence of a formal memorandum of understanding and there is ongoing and positive engagement with An Garda Síochána, particularly in the areas of cyber crime and national security. There is also ongoing shared training and a member of An Garda Síochána is currently on secondment to the National Cyber Security Centre, with a second member to be seconded in the near future.

Network and Information Systems Directive

8.42 The EU Network and Information Systems Directive was formally adopted in 2016 and aims to achieve a high common level of security of network and information systems across the EU. The deadline for transposition of the Directive into Irish law was 9 May 2018. Transposition was achieved on 18 September 2018.

8.43 A requirement of the Directive is to adopt a national strategy that contains a number of requirements. No national strategy is currently in place and the previous strategy did not include some of the required elements such as: a risk assessment plan, a listing of various stakeholders and a governance framework.

Recommendation 8.4

The Department should ensure that its updated strategy meets all the requirements of the Directive.

Accounting Officer response

Agreed.

Work is already underway on a revised strategy which is expected to be completed by the end of 2018. A steering group will be established to bring all relevant stakeholders together in order to fully inform the process.

Accountability and oversight

8.44 Although governance structures were described in the strategy implementation plan, in practice, it is not clear what structures are in place. A key role of such structures is to look at the overall strategic direction of the National Cyber Security Centre and to review, monitor and oversee how available resources are being used.

Recommendation 8.5

The Department should implement an appropriate governance framework for the National Cyber Security Centre.

Accounting Officer response

Agreed.

The National Cyber Security Centre is an operational unit within the Internet Policy Division of the Department and complies with the Department's corporate governance framework. It is not a separate entity, but rather forms an integral part of the Department.

Cross-government arrangements have further developed since the 2015 National Cyber Security Strategy. This has led to an improvement in bilateral co-operation and overall governance structures relating to cyber security matters in the State. The Government's Cabinet Committee F and the related Senior Officials Group provide an overarching forum at senior level to engage on cyber security issues. This formal interdepartmental and Cabinet level structure was not anticipated in 2015, and presents a far more coherent and central forum for the discussion of policy matters relating to cyber security.

The governance framework will be assessed and reviewed in the context of the forthcoming National Cyber Security Strategy.

8.45 The overall cost attributed to cyber security is not reported separately in the appropriation account of the Department. As a result, there is a lack of transparency around the availability and use of resources.

Recommendation 8.6

The Department should disclose separately the activity relating to the National Cyber Security Centre in its estimate and appropriation account.

Accounting Officer response

Agreed.

Expenditure relating to the National Cyber Security Centre is reported in the appropriation account under the Communications Programme in line with the Department's vote structure.

The Department seeks to prevent operational information relating to the operations and work of the Centre from becoming public due to operational security concerns. However, the Department will work towards separately identifying cyber security expenditure in an appropriate manner in the 2019 or 2020 revised estimates for public services.