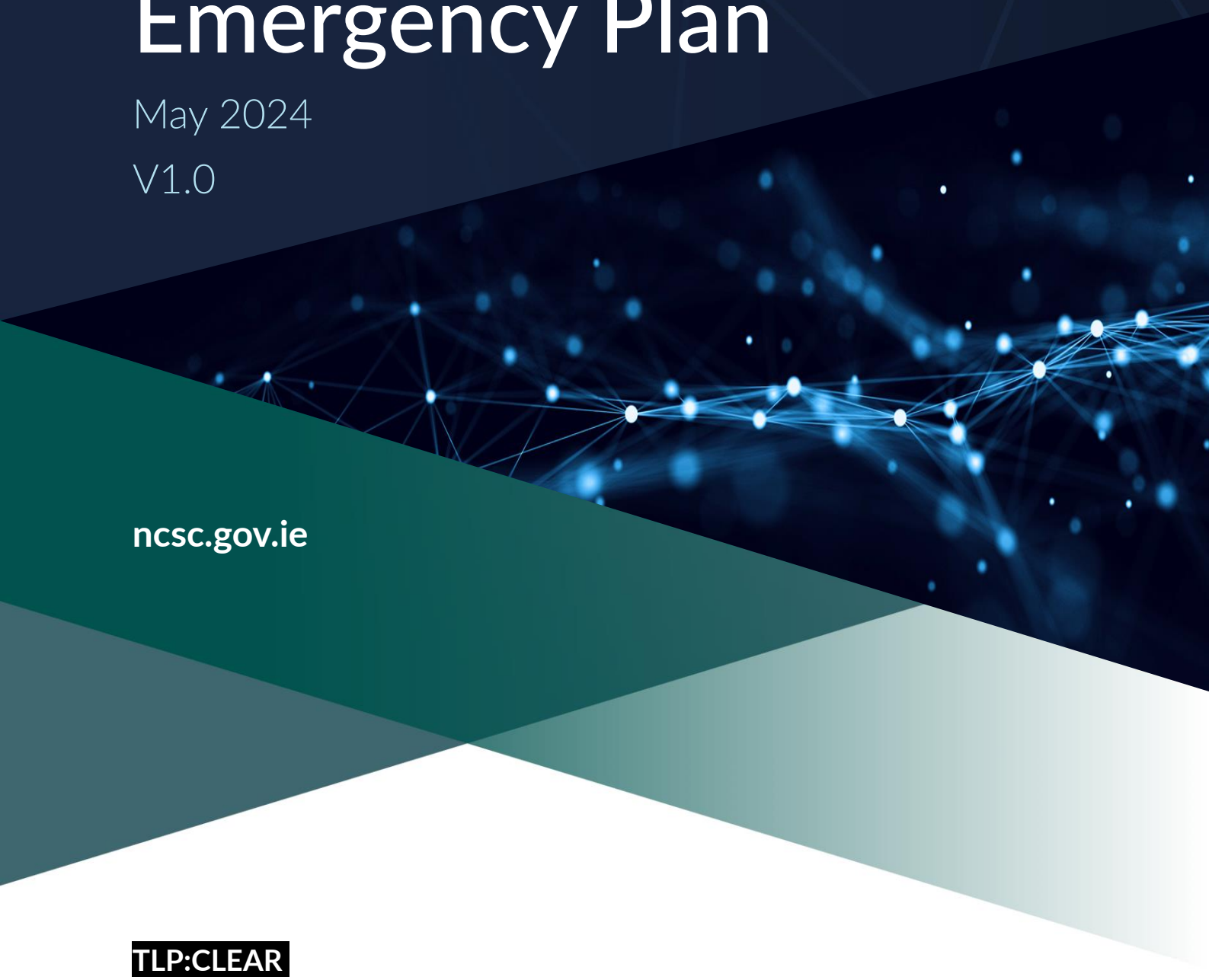
An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

National Cyber Emergency Plan

May 2024

V1.0



ncsc.gov.ie

TLP:CLEAR

Rialtas na hÉireann
Government of Ireland

Rialtas na hÉireann
Government of Ireland

Tom Johnson House, Beggar's Bush, Dunlin 4, Ireland, D04 K7X4
T +353 (0)1 678 2333 **E** info@ncsc.gov.ie
ncsc.gov.ie

An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

Version Control

Version Number	Purpose/Change	Author	Date
0.1	Initial Draft	Vincent O'Brien	Sept 2022
0.2	Second draft following NCEP Exercise Nov 23	Vincent O'Brien	Feb 2024
1.0	Final version incorporating stakeholder obs	Vincent O'Brien	May 2024

1. Introduction

1.1 Purpose

The national approach to emergency management is established in the '**Strategic Emergency Management (SEM) National Structures and Framework**'[1]. This is designed primarily to enhance the protection, support, and welfare of the public in times of emergency by ensuring that fit-for-purpose national structures and procedures are in place to deal with a broad spectrum of emergencies, whether of internal or external origin. These arrangements are also designed to enhance national resilience so that disruption to the functioning of society and the economy is minimised.

While most cyber security incidents are an ongoing challenge that can be managed without a significant societal or economic consequence, certain incidents can pose significant risk to economic and social activity. Responding to cyber security emergencies effectively at a national level is a complex undertaking due to the very wide range of potential incidents, and the diverse nature, extent and consequences associated with these. An effective response process requires substantial planning and resources, and this capability needs to be exercised on a regular basis.

The **National Cyber Emergency Plan** (NCEP) sets out the national approach for responding to serious cyber security incidents that affect the confidentiality, integrity, and availability of nationally important information technology and operational technology systems and networks.

The NCEP is designed to outline the process by which a National Cyber Emergency might be effectively declared, managed and coordinated. It is also designed to ensure that stakeholders understand their roles and responsibilities during a cyber emergency, and the means by which the Government's approach to incidents is explained and communicated to the public.

Developed in alignment with the Strategic Emergency Management National Structure and Framework, which sets out the structures used to prepare for, respond to and recover from crises requiring national level coordination, the NCEP outlines the structures for coordinating a "whole of Government" approach to preparing for and responding to a cyber emergency. The NCEP establishes an architecture for coordinating the government response in accordance with Irish and European legislation and policy.

The primary audience for the NCEP are officials from Government Departments/Agencies who have a role in the response to national cyber emergencies and potential victim organisations (providers of essential and important services), including but not limited to senior officials, communications staff, and personnel who have responsibilities relating to incident response within their organisation.

This is a guidance document which does not place binding obligations on any party and is without prejudice to pre-existing statutory requirements in areas such as safety, risks to life and the right to privacy.

[1] Strategic Emergency Management – National Structures and Framework

National Security considerations may override aspects of this document.

1.2 Cyber Emergency

Cyber security incidents are diverse by their nature. For example, a National Cyber Emergency could occur as a consequence of an incident affecting IT systems owned directly by Government, those owned by private sector operators of critical infrastructure, or in systems owned by organisations which provide services to either or both of the above.

Furthermore, the proximate cause of the incident may be in IT infrastructure that is physically located in the State or is located in other jurisdictions (either inside or outside the EU), or is shared across several jurisdictions.

Also, in some cases incidents occur where the cyber component is readily managed but impacts in the physical domain require a Strategic Emergency Management process in a specific sector.

As such, there are a vast range of potential scenarios where the NCEP process may be initiated, in turn requiring a very flexible response process in all aspects of its construction, including inception and close out.

A **cyber emergency** is defined as any **cyber incident**[2] which causes or threatens to cause:

- death or serious injury or damage to property, the environment or the economy or significant incidents[3] impacting **two or more** critical sectors[4].
- and which requires the activation of the National Emergency Coordination Group (NECG Cyber) to ensure an effective coordinated response for containment, mitigation and/or recovery.

[2] NIS2 Article 6(6) 'incident' means an event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems

[3] NIS2 Article 23(3) Significant Incidents:
An incident shall be considered to be significant if:
(a) it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned;
(b) it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.

[4] NIS2 EU 2022/2555 Critical Sectors Annex I and II

2. National Cyber Security Emergency Plan (NCEP)

The activities described in the NCEP rely upon three cooperation modes:

- Permanent Mode
- Warning Mode
- Full Activation Mode

The following sections describe the procedures and activities associated with each mode.

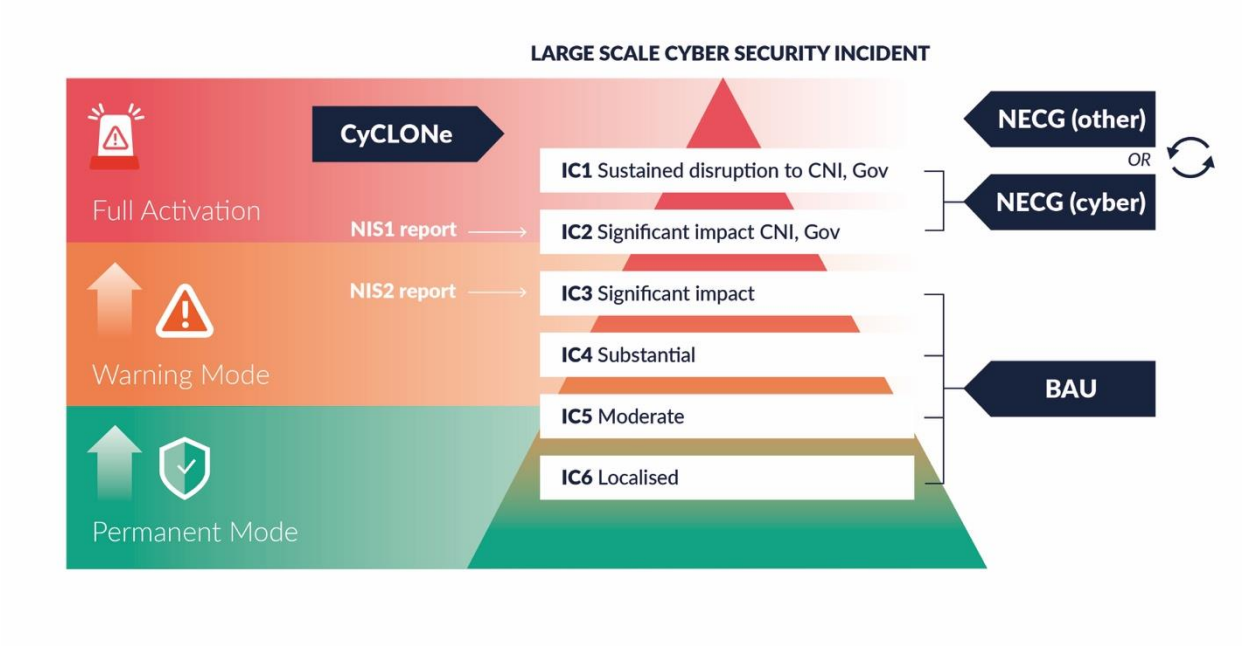


Fig 1. Three NCEP Cooperation Modes. IC categories are described in Appendix A.

2.1 Permanent Mode

This relates to the normal course of business, during which situational awareness is maintained and incident preparedness activities are carried out. Communications is maintained through usual reporting formats.

The responsibility for identifying incidents which have the potential to meet the threshold of a national cyber emergency sits with both:

- The Lead Government Department (LGD) or Agency overseeing/regulating the affected entities and
- The National Cyber Security Centre (NCSC)

These organisations receive reports from the public, from entities they oversee, or from technical capabilities that identify incidents which may lead to a cyber emergency.

2.2 Warning Mode

Warning Mode will be activated on receipt of evidence and/or inputs received by the NCSC from its constituents, the CyCLONe (Cyber Crisis Liaison Organisation Network) network, other international peer organisations or threat intel partners which indicates that there is a **heightened risk** of a '**cyber emergency**' type incident emerging in a specific sector or sectors. This mode involves communications with stakeholders across government and in the private sector as appropriate to reinforce information exchanges and cooperation to prevent possible spread of the incident.

This mode is also a filter to decide if escalation to Full Activation Mode is necessary.

Information to support the decision-making process on the move to Warning Mode may come from a wide range of sources, including the NCSC's own incident detection/response or forensic capabilities or from information received from third parties within or outside the state.

2.2.1 Activate Warning Mode

Warning Mode can be triggered by two means:

1. The first of these is at the behest of a national actor (either a Lead Government Department or the NCSC). The NCSC can trigger this mode on receipt of an incident report, or intelligence to the effect that an incident is underway or imminent. A Lead Government Department may also commence such a process where they have specific information that an entity or entire sector is at risk of a particular incident.
2. The second is through EU Cyclone process in respect of an incident in another EU Member State.

The Office of Emergency Planning (OEP) will notify NCEP stakeholders by email when Warning Mode is activated.

During the period in which Warning Mode is in place, the NCSC would likely be engaged with a potential victim or victims in supporting incident response and would be sharing information relating to this in a number of directions. Technical details, including the result of forensic analyses of any affected devices or networks, would be shared with other potential victims in the state and potentially also via relevant EU and NATO information sharing networks. Information relating to potential risks to services or infrastructure in the state would be shared also with key security stakeholders and with Lead Government Departments or other Departments as appropriate.

It is likely that regular virtual or in-person briefings of members of the NECG (Cyber) would take place to maintain situational awareness and prepare for any escalation to full activation mode.

The **EU CyCLONe**[5] [6] process is a member state led European incident response and coordination mechanism, that aims to bring together at a senior level, national cyber incident response entities to

[5] NIS2 Article 16 European cyber crisis liaison organisation network (EU-CyCLONe)

[6] https://www.enisa.europa.eu/topics/incident-response/cyclone

coordinate and support decision making for '**large-scale cybersecurity incidents**'[7] affecting one or more Member State. The Cyclone network moves through a similar Permeant, Warning and Full Activation Mode sequence as that set out in this plan. If a Cyclone Warning or Full Activation Mode is activated in respect of an incident in another Member State or Member States, then the national level shall automatically be set to that cooperation mode in respect of the sector or sectors affected by the incident in question.

2.2.2 Exit Warning Mode

During Warning Mode, either the NCSC or the Lead Government Department may organise meetings or briefings to discuss the ongoing incident response process required to either contain the spread of the incident and stand down Warning Mode or escalate to Full Activation Mode:

- The first of these is if the risk to the critical sector is deemed to be successfully eradicated, mitigated or contained and Warning Mode can be exited, with remaining follow up actions to be taken by the victim, the NCSC or the lead government department in question.
- The second possible outcome is that either risks continue to grow and no likely mitigation can be foreseen in the short term, or the incident is causing or capable of causing severe operational disruption for a critical sector. In either case the decision will be taken to activate the National Emergency Coordination Group (NECG) process[8].

The OEP will notify NCEP stakeholders by email when Warning Mode is Exited/Stood Down.

[7] NIS2 Article 6(7) 'large-scale cybersecurity incident' means an incident which causes a level of disruption that exceeds a Member State's capacity to respond to it or which has a significant impact on at least two Member States.

[8] Strategic Emergency Management, Guideline 1 – National Emergency Coordination Group

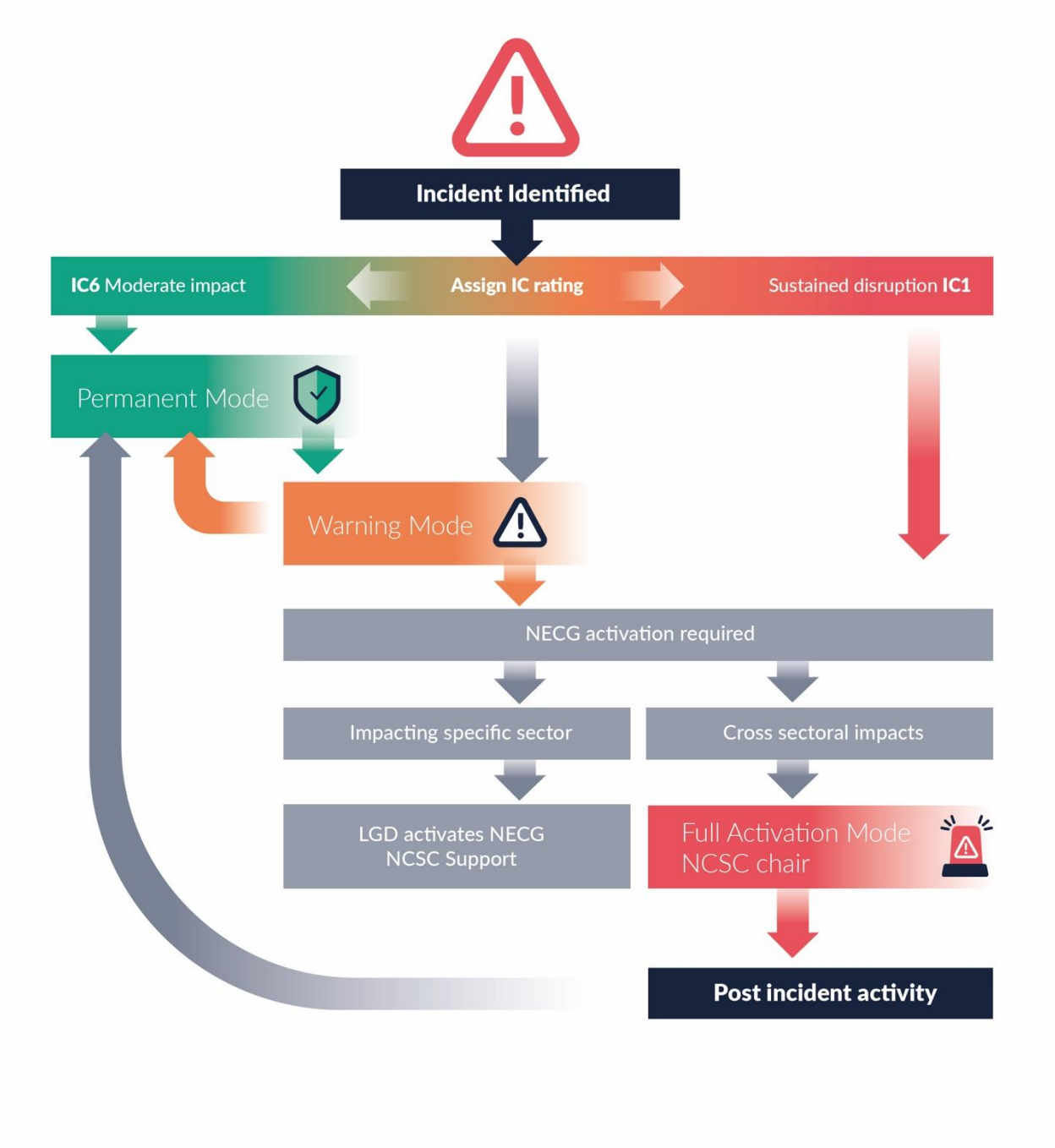


Fig 2. National Cyber Emergency Plan cooperation modes and escalation path.

2.2.3 Activate NECG

The Strategic Emergency Management, Guideline 1 document sets out the various steps involved in coordinating a national-level response to emergencies. **Annex A** of the **SEM National Structures and Framework**[9] document identifies the Lead Government Department (LGD) responsible for leading the response for various emergency/incident types. The following guidance is provided to help decide which government department is best placed to assume the LGD role for emergencies where the **root cause is a 'cyber incident'** (see Section 1.2, for the definition of a cyber incident)

- Where impacts are limited to a particular sector, the LGD identified in Annex A will lead the NECG process, with the NCSC in a support role providing specialist advice for the cyber domain. The NCSC will work through the Gov-CORE group to empower all government departments to develop scenario specific emergency response plans for cyber emergencies in their sectors.
- Where cyber incidents impact **two or more** critical sectors, the NCSC will lead the NECG process, and enter Full Activation mode. Scenario examples include incidents impacting government networks, or an incident exploiting a vulnerability in a technology product or service which is used by several government departments etc.

2.3 Full Activation Mode

This mode will be activated if an incident occurs that meets the threshold of a national '**cyber emergency**' which requires the activation of the National Emergency Coordination Group (NECG Cyber) chaired by the NCSC to ensure an effective coordinated multi agency and cross government response for containment, mitigation and/or recovery.

The decision to move to Full Activation Mode will be taken by the NCSC, or by the Minister for the Department of the Environment, Climate and Communications. This decision may follow a period in which Warning Mode has been active. However, it is also possible that a decision could be made to move directly to Activation Mode if an incident presents as being sufficiently serious at first reporting.

In the event of a national **cyber emergency declaration**, the Office of Emergency Planning (OEP) shall convene the National Emergency Coordination Group (NECG) for Cyber Incidents at the National Emergency Coordination Centre within one hour (as per Para 6.7 SEM), under the chair of the Director of the NCSC or Deputy Director (representing LGD DECC for Cyber incidents), and supported by the impacted LGD's who will manage the sectoral impacts within their remit..

This mode may also be activated if a '**large-scale cybersecurity incident**' is identified by the CyCLONe network at EU level or other international Peer organisations.

See Appendix A for the NCSC Cyber Incident Classification table, which describes Incident Categories IC1 – IC6 based on impacts, who responds and responsibilities.

[9] Strategic Emergency Management National Structures and Framework

For incidents where **national security** concerns arise an NECG meeting may not be called, and the incident could instead be dealt with by other means as appropriate.

2.3.1 Exit Full Activation Mode

When Full Activation Mode has been convened following a National Cyber Emergency declaration, a key task will be to identify the objectives required to exit the 'Cyber Emergency'. See **Appendix E** for a NECG (cyber) sample agenda. It is envisaged that Full Activation Mode will end and the cyber emergency stood down when the 'essential services' of the impacted entities can resume at acceptable levels. However, response activities to fully remediate and harden all systems will often continue long after the initial 'emergency' period has passed.

Emergency exit criteria will typically require meeting conditions such as:

- Information systems underpinning essential services are functional
- Priority network communications are reconnected
- Backups are in working order
- The root cause that gave rise to the incident has been identified and a remediation plan initiated.
- The NECG members have reached a consensus that the objectives to end the emergency have been achieved and that acceptable services levels have been restored.
- The NECG chair is handed over to an alternative LGD, if for example the cyber specific elements of the incident are contained but sectoral impacts are ongoing.

2.3.2 Post incident activity

When the cyber emergency is stood down the experiences and lessons learned will be captured in an After Action Report (AAR), and also used to update the National Cyber Emergency Plan and other incident response playbooks as appropriate, in order to drive continual improvements to the response processes.

The NCSC will also perform periodic exercises in collaboration with the wider stakeholder community to test the National Cyber Emergency Plan as well as the cyber response plans of other sectoral departments and agencies/entities. The output from such exercises will be used to continually refine and improve the response to cyber incidents at the entity, sector and National and International level.

3. Roles and Responsibilities

Figure 3 below shows the key participants in the National Emergency Coordination Group (cyber), followed by a description of the participants role. The NECG (cyber) group is aligned with the Strategic Emergency Management National Structures and Framework model.

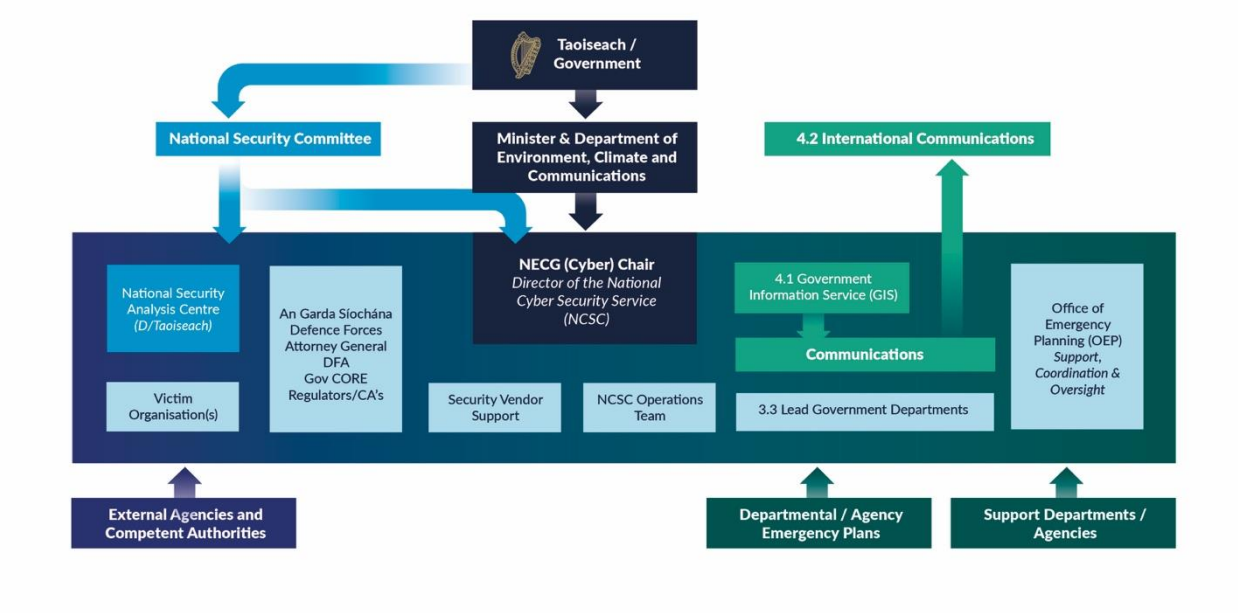


Fig 3. Overview of the NECG (cyber)

3.1 National Emergency Coordination Group

The NECG is the national structure which is put in place to coordinate and obtain the necessary support and advice from identified support Departments and Agencies in a threatened or ongoing emergency. The OEP will convene the NECG on behalf of the NCSC within one hour of a cyber emergency declaration. (SEM[10] Para 6.7).

During a National Cyber Emergency, a key role of the NECG will be maintain overall situational awareness of the incident and to coordinate a whole of government response to a cyber emergency with cross Government and/or Cross Sector implications.

When the NECG (cyber) is convened when the conditions for a 'cyber emergency' declaration, all GTF members of the group are obliged to attend the first meeting (SEM Para 6.9). Attendance at subsequent meetings is managed in the light of the nature of the emergency, and at the discretion of the NCSC chair. The Chair may establish Sub-Groups to deal with specific issues (as per SEM Para 6.14) which arise or are expected to arise in dealing with the emergency.

The NECG Chair will initially inform all GTF members that a National Cyber Emergency has been declared and will then convene a refined NECG (cyber) group which shall consist of:

[10] GTF - The Government Task Force on Emergency Planning (SEM National Structures & Framework)

- NCSC chair (NCSC Director or deputy) - representing LGD DECC for Cyber incidents
- National Security Analysis Centre (NSAC)
- Victim organisation(s) as required
- Government Information Services (GIS)
- Attorney General's Office (AGO)
- Department of Foreign Affairs (DFA)
- Department of Justice
- An Garda Síochána (AGS)
- Defence Forces (DF)
- Private cyber security vendors as required
- Office of Emergency Planning (OEP)(support, coordination, oversight)
- Lead and Support Government Department as required (varies dependent on incident type and sectoral impacts)
- Gov CORE[11] Chair
- Regulators and Competent Authorities (inc. DPC[12]) as required

See **Appendix D** for an overview of how the EU Cyber Crisis Management structures.

See **Appendix E** for a suggested NECG (Cyber) agenda.

3.2 NECG Chair

The NECG will be chaired by the Director or senior official of the National Cyber Security Centre (NCSC). The chair of the NECG needs to have overall situational awareness of all efforts related to the national cyber emergency.

The NCSC, representing DECC as the LGD for National Cyber Emergency incidents, has the mandate and responsibility to coordinate all national level activity in the State during a national cyber emergency and shall be designated as the competent authority responsible for the management of **large-scale cybersecurity incidents** and crisis under NIS2[13]. During an emergency, Department of Environment, Climate and Communications through the NCSC has overall responsibility for managing the government response with political oversight provided by the Minister for Environment, Climate and Communications.

The NECG Chair, will decide on the frequency of meetings, prepare the agendas, provide papers as appropriate and record the main decisions and recommendations made (as per Para 6.10). The NECG Chair

[11] Gov-CORE - Government Cyber Security **Co**ordination and **Re**sponse Network

[12] where an incident involves personal data.

[13] NIS2 Article 9 National cyber crisis management frameworks.

will ensure that appropriate decisions are made in a timely fashion. In bringing the group to a decision, the Chair will try to establish a consensus among the NECG members present.

The NECG cannot take a decision which is vested by statute in another government department or agency or other public authority, without agreement of that department or agency.

When an issue must be decided urgently, or a specific issue between departments requires deconfliction, the NECG chair will try to establish a consensus among the NECG members present. If a consensus cannot be reached, having heard the views of the NECG members, the Chair will refer the issue for immediate decision to the appropriate Ministers or the Government, detailing the difference in opinion and the recommendation of the NECG Chair *(as per SEM 3.2 - Where it is necessary to secure Ministerial approval for any proposed measures, the matter is to be referred to the Minister in charge of the LGD. Where the matter is cross-Departmental and is not concluded at NECG, it is to be referred to the relevant Ministers, and if necessary, the Taoiseach.)*

3.3 Lead Government Departments during a cyber emergency

Lead government departments (LGDs), and where relevant agencies, are responsible for managing the impacts of the cyber emergency for its assigned emergency types, as set out in Annex A in the SEM National Structures and Framework document. LGDs are required to manage any physical response and recovery operations in their assigned sectors resulting from a national cyber emergency. LGDs must also have overall situational awareness of all ongoing efforts related to the national cyber emergency and will likely be required to provide regular briefings to senior officials and supporting agencies under their aegis.

Tasks for LGDs includes risk assessment, planning and preparedness, prevention, mitigation, response, and recovery. LGDs will also identify the specific roles which it expects Support Departments/Agencies to undertake in an emergency, and work with them in the planning and preparedness phase.

3.4 NCSC Operations Team

The pro-active prevention of cybersecurity incidents and managing them when they occur is a core activity performed by the NCSC Operations Team. During the response to a cyber incident, the NCSC Operations Team and those supporting them will be focussed on technical remediation and shall have the independence to take appropriate operational decisions, informing the NECG of progress through regular updates to the chair.

The NCSC incident response process includes 5 phases – 1. Preparation, 2. Detection and analysis, 3. Containment, 4. Eradication and recovery, 5. Post-event activity.

During a national cyber emergency, the NCSC Operations Teams and those supporting them will:

- identity the scope, impacts and implications of the cyber security incident on Ireland, and work to contain incidents as they occur.

- analyse, enrich and share indicators of compromise and other technical details with the appropriate stakeholders and peer organisations, nationally and internationally, e.g., relevant Competent Authorities.
- guide and support victim organisations and their response team during a cyber incident to enable them to remediate and resolve the incident.
- capture the technical and non-technical details of the incident and use that information to manage and communicate ongoing cybersecurity risks in the State.
- The NCSC Operations Team may request Government Departments, Public Sector Bodies or operators of Critical National Infrastructure to take certain actions, for example isolate their network, preserve logs, in response to the incident.
- provide reports and analysis on incidents to assist law enforcement and national security authorities.
- For actual or suspected incidents with all-island implications, there will be bilateral coordination and communication between the NCSC-IE and NCSC-UK in the first instance. After the initial stages of an incident there will be 3-way communications between the NCSCs and the Northern Ireland Executive.

3.5 Victim organisations

Victim organisations will in the first instance own the incident response process within their own organisations, with the NCSC providing a support role as described in Section 3.4. The role of victim organisations prior to and during an incident will include the following:

- Swiftly report the incident or sign of suspicious activity to the NCSC Operations team.
- Organisations should also report to other National Authorities and agencies as required, e.g., DPC[14], AGS, CBI
- Engage the services of a specialist Incident Response form if required.
- Provide binaries or executable samples, data, metadata, or logs and also systems and networks to the NCSC Operations Team, if necessary, who will use this data to perform analysis and further enrichment of the data.

[14] Wherever an incident within the scope of the NCEP affects or has some impact on the personal data processed by the entity who suffered the incident, the controller for that personal data has certain obligations under the GDPR, specifically under Art 33 about notification to a Data Protection Authority, and notification of affected data subjects in high-risk situations.

3.6 Private Cyber Security Vendors

Technical specialists assisting in the response may come from the NCSC, other agencies, and the private sector. During a cyber security incident, the NCSC may connect the affected entity with appropriate private cyber security vendors to provide the affected entity the cyber security expertise and resources needed to mitigate an incident as quickly as possible. Unless otherwise stated, the NCSC accepts no liability for the actions of private cyber security vendors on victim organisation networks, which is a matter for contractual arrangements between the victim organisation and the private sector provider.

3.7 Law Enforcement

A cybersecurity incident is commonly a criminal act, and affected organisations should report incidents to An Garda Síochána (AGS) or other regulatory agencies or competent authorities as required under general or specific sectoral legislation (e.g., ComReg, DPC etc)

The priority during any national cyber emergency is the restoration of services critical to functioning of the State and ending the national cyber emergency. The NCSC and supporting entities will work with Law Enforcement to support their response to the incident and will endeavour to ensure their technical response includes the forensically sound capture of evidential material prior or in parallel to the recovery of systems, ensuring any destruction of evidential material via remediation is avoided or minimised. If there are conflicting objectives between law enforcement and technical response personnel that cannot be resolved at an operational level, the issue will be brought to the NECG for deconfliction.

An Garda Síochána have the primary responsibility for the investigation and subsequent prosecution of any criminal acts in relation to the national cyber emergency. An Garda Síochána may also be involved in the disruption of cybercrime activities through the seizure of digital assets or infrastructure. Given the international nature of most cybercrime, An Garda Síochána is responsible for liaison with international policing organisations such as EUROPOL or INTERPOL.

AGS and the NCSC often share relevant information relating to incident response processes, and it is likely that this will occur during any National Cyber Emergency. Such information may include cyber threat intelligence such as indicators of compromise, digital forensic imagery, and the results of investigations.

3.8 Defence

The 2015 White Paper on Defence outlines the role of the Defence Forces in cybersecurity; "*The primary focus of the Department of Defence and the Defence Forces will remain the protection of Defence networks … as in any emergency/crisis situation, once Defence systems are supported, the Department of Defence and Defence Forces will provide support to the [NCSC] team in so far as resources allow.*"

Through the NECG the NCSC chair may request support and assistance from the Defence Forces. Such assistance will depend on the nature of the cyber emergency but could include:

- Deploying technical staff to support the NCSC operations team in a surge capacity responding to the cyber emergency.
- The provision of ICT equipment and other materials to assist in the response.
- The provision of manpower and logistical support as required in the recovery.

3.9 Office of the Attorney General

The Office of the Attorney General will provide legal advice where necessary on any proposed decisions or actions taken by the NECG during the course of the incident lifecycle.

3.10 Intelligence and Security

Intelligence support during a national cyber emergency is provided by national authorities with the capability to do so, including the Defence Forces, NCSC, AGS, and the National Security Analysis Centre. The sharing of relevant intelligence with senior leadership in the government and those responding to the incident will be a priority for these organisations.

Intelligence and related supporting activities can play a crucial role in understanding and responding to a national cyber emergency. The NCSC and supporting organisations will utilise intelligence sources to build situational awareness; share related threat indicators and analysis of threats; identify and acknowledge gaps; and ultimately create a comprehensive picture of the incident.

Information and intelligence sharing initiatives that have been established at a sector level through public/private partnerships may also provide intelligence support, where available.

National Security Committee (NSC)

The NSC is chaired by the Secretary General to the Government, and it comprises representatives at the highest level from the Departments of Justice, Defence, Foreign Affairs, the Environment, Climate and Communications and from An Garda Síochána and the Defence Forces. The secretariat to the Committee is provided by the National Security Analysis Centre in the Department of the Taoiseach. The committee is concerned with ensuring that the Government and the Taoiseach are advised of high-level security issues and the responses to them.

National Security Analysis Centre (NSAC)

The NSAC was established in 2019 by the Government and its primary remit is to provide high-quality, strategic analysis to the Taoiseach and Government of the key threats to Ireland's national security. The strategic analysis of threats is undertaken by personnel seconded from the various Departments and other State bodies with functions in the security area, and through liaison and close co-ordination with those partner Departments and agencies, including with the National Cyber Security Centre.

3.11 Attribution and Cyber Diplomacy

The attribution of cyber-attacks to a specific threat actor, particularly other States, can be particularly challenging. Attribution has many aspects—technical, political, diplomatic, legal and policy. Authorities such as the NCSC and AGS, as well as private cybersecurity vendors, can often provide technical attribution to varying degrees of confidence, based upon technical indicators gathered during the remediation and investigation of the cyber emergency. However, these entities are not well placed to consider the political, diplomatic, legal and policy implications and thus public attribution of such attacks should be conducted by Government assisted by the advice of the NCSC.

Cyber Security Emergencies often contain a diplomatic element particularly if the incident is cross-border in nature, and the Department of Foreign Affairs lead on cyber diplomacy issues. The **EU Cyber Diplomacy Toolbox**[15] which was adopted in 2017 provides a way of coordinating the diplomatic responses of EU member states to malicious cyber activities at the EU level. Furthermore Member States expressed their intention to establish an **EU hybrid toolbox**[16], which would focus on (1) identifying complex and multifaceted hybrid campaigns, and (2) coordinate tailor-made and cross-sectoral responses to them. Acting as an overall framework, its intention is to bring together other relevant response mechanisms and instruments, such as the cyber diplomacy toolbox and the proposed **Foreign Information Manipulation and Interference (FIMI) toolbox**[17] to improve the effectiveness and coherence of different actions, and therefore bring added value to the EU's capabilities in responding to **hybrid threats**.

[15] Revised Implementing Guidelines of the Cyber Diplomacy Toolbox

[16] Council conclusions on a Framework for a coordinated EU response to hybrid campaigns

[17] The development of the Foreign Information Manipulation and Interference (FIMI) toolbox was part of the actions presented in the EU Strategic Compass for Security and Defence. Read more at https://www.consilium.europa.eu/en/press/press-releases/2022/03/21/a-strategic-compass-for-a-stronger-eu-security-and-defence-in-the-next-decade/

4. Communications

THE NCSC will use the Traffic Light Protocol (TLP) V2.0 when sharing information. TLP is a set of designations used to ensure that sensitive information is shared with the appropriate audience. It employs four colours to indicate expected sharing boundaries to be applied by the recipient(s). **Appendix C** describes the 4 TLP sharing categories.

4.1 National Communications

During a national cyber emergency, it is vital that coherent and unified communications are maintained when issuing information and advisories to the public, victim organisations and other stakeholders involved in managing the response. Therefore, an initial task of the NECG will be to convene a Communications Subgroup which will be chaired by the NCSC and supported by GIS and OEP as per SEM Guideline 2 (Emergency Communications)[18]. The NECG will work closely with GIS on the preparation and delivery of communications on all issues related to the emergency.

The NECG will provide regular updates, through GIS, to the public, and will engage closely with the spokespeople and Communications Teams from other Lead Government Departments and agencies to ensure consistent and coordinated messaging on any public communications. The NCSC will also continue to issue technical security advisories and guidance through its usual channels targeted at the public or specific sectors.

4.2 International Communications and Cooperation

The NCSC and supporting departments will coordinate with their international counterparts, sharing relevant information with other Government departments to assist in the response. Supporting departments will include the NCSC and Department of Foreign Affairs on international communications relevant to responding to the national cyber emergency. Communications at Technical, Operational, Strategic and Political levels will occur through existing EU structures such as Computer Security Incident Response Team Network (CSIRT network), Cyber Crisis Liaison Organisation Network (EU-Cyclone) network, the Network and Information Systems Directive Cooperation Group (NIS CG) and Single Point Of Contact networks, the EU structures such as the Horizontal Working Party on Cyber Issues (HWPCI), the Permanent Representatives Committee (COREPER) and the Integrated Political Crisis Response (IPCR) mechanism. Relevant Justice and Home Affairs (JHA) structures including the Standing Committee on Operational Cooperation on Internal Security (COSI). Cooperation at international level will be through bilateral arrangements with peer organisations.

[18] Strategic Emergency Management Guideline 2 - Emergency Communications

The CNI Cyber Coordination Working Group (C3WG) is established to strengthen cooperation between officials in the UK (Stormont and Westminster) and Irish Government in relation to cyber incident response and cross border CNI cyber dependencies.

AGS will be responsible for any international law enforcement engagement.

5. Incident Handover

If at any stage during the incident response life cycle, it is deemed that it is no longer necessary or appropriate for the NCSC (representing DECC) to lead the recovery, the management of the recovery shall be handed over to an agreed alternative Government Department or agency (SEM Para 7.5[19]).

Reasons for this could be that the incident is contained within a single sector, the incident severity is assessed as no longer meeting the threshold or an IC1 or IC2 category incident, the root cause is due to a non-malicious event such as systems failure or human error, etc.

6. Post Incident Review

Following an incident, a review will be carried out at the conclusion of the NECG response, chaired by DECC as per SEM Para 6.15 to review the incident and identify lessons learned. This may include inter-departmental reviews and briefings for operational personnel and senior officials, as well as more in-depth post emergency reports.

Responsibility for the review will rest with LGD and will be brought to GTF (SEM Paras 6.15 to 6.18).

[19] Strategic Emergency Management – National Structures and Framework – paragraph 7.5

Rialtas na hÉireann
Government of Ireland

Appendix A – NCSC Cyber Incident Categories

Category	Category definition (impacts)	Who responds	Responsibilities
IC1 **National Cyber Emergency**	A cyber attack which: • Causes sustained disruption of essential services or, • Affects national security, leading to severe economic or social consequences or to loss of life.	Immediate, rapid and coordinated cross-government response (escalated to NECG if necessary, as per NCEP). Strategic leadership from Government, tactical cross-government coordination by NCSC, working closely with Law Enforcement.	Coordinated on-site presence for evidence gathering, forensic acquisition and support. Collocation of NCSC, Law Enforcement, Lead Government Departments and others where possible for enhanced response.
IC2 **Highly Significant Incident**	A cyber attack which: • Has a serious impact on central government, or • Has a serious impact on essential services, or • Has a serious impact on a large proportion of the population, or • Has a serious impact on the economy.	Response typically led by NCSC (escalated to NECG if necessary), working closely with Law Enforcement as required. Cross-government response coordinated by NCSC.	NCSC will often provide on-site response, investigation and analysis, aligned with Law Enforcement criminal investigation activities.
IC3 Significant Incident	A cyber attack which: • Has a serious impact on a large organisation or, • Has a serious impact on wider/local government, or • Which poses a considerable risk to central government or,	Response typically led by NCSC, working with Law Enforcement as required.	NCSC will provide remote support and analysis, standard guidance; on-site NCSC or AGS support may be provided.

	• Which poses a considerable risk to essential services.		
IC4 Substantial **Incident**	A cyber attack which: • Has a serious impact on a medium-sized organisation, or • Which poses a considerable risk to a large organisation, or • Which poses a considerable risk to wider/local government.	Response led either by NCSC or by Law Enforcement, dependent on the incident.	NCSC or Law Enforcement will provide remote support and standard guidance, or on-site support by exception.
IC5 Moderate **Incident**	A cyber attack: • On a small organisation or, • Which poses a considerable risk to a medium-sized organisation, or, • Preliminary indications of cyber activity against a large organisation or, • Preliminary indications of cyber activity against the government.	Response led by the affected party, with NCSC/AGS support as required.	NCSC & AGS will provide remote support and standard guidance, with on-site response by exception.
IC6 Localised Incident	A cyber attack: • On an individual, or • Preliminary indications of cyber activity against a small or medium-sized organisation.	Local response led by affected party with NCSC support as required.	

Appendix B – Threat Types

Appendix B provides a non-exhaustive list of the threat types which have been identified as having the potential to activate the NCEP. Threats which are assessed as reaching IC1 or IC2 level impacts may trigger activation of the NCEP.

- **Disruption**: intentional temporary impairment of the accessibility of data, information systems or information services.
- **Sabotage**: intentional and very long-lasting impairment of the accessibility of data, information systems or information services, possibly resulting in destruction.
- **Data manipulation**: impairment of the integrity of information by means of the intentional editing of data.
- **Data theft**: impairment of the confidentiality of information by means of the copying or removal of data.
- **System manipulation**: impairment of information systems or information services targeting the confidentiality or integrity of these systems/services. These systems or services are subsequently used to carry out other attacks.
- **Breakdown/failure**: impairment of integrity or availability due to natural causes, technical difficulties or human error.

Rialtas na hÉireann
Government of Ireland

Appendix C – Traffic Light Protocol (TLP) V2.0

https://www.first.org/tlp/

The Traffic Light Protocol (TLP) was created to facilitate greater sharing of potentially sensitive information and more effective collaboration. Information sharing happens from an information source, towards one or more recipients. TLP is a set of four labels used to indicate the sharing boundaries to be applied by the recipients.

TLP:RED

For the eyes and ears of individual recipients only, no further disclosure.

Sources may use TLP:RED when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved. Recipients may therefore not share TLP:RED information with anyone else. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting.

TLP:AMBER

Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients.

Note that TLP:AMBER+STRICT restricts sharing to the organization only. Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note: if the source wants to restrict sharing to the organization only, they must specify TLP:AMBER+STRICT.

TLP:GREEN

Limited disclosure, recipients can spread this within their community.

Sources may use TLP:GREEN when information is useful to increase awareness within their wider community. Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. TLP:GREEN information may not be shared outside of the community. Note: when

"community" is not defined, assume the cybersecurity/defense community.

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.

Appendix D – EU Cyber Crisis Management

	Actors	Responsibilities
Strategic Level	• MS ministers responsible for cybersecurity • President of the European Council • Presidency of the Council • President or the delegated VicePresident/Commissioner of the European Commission • High Representative of the Union for Foreign Affairs and Security Policy	• Strategic and political management of both the cyber and non-cyber aspects of the crisis
Operational Level	• EU-CyCLONe	• Ensure enhanced cooperation and coordination • Prepare decision-making at the political level • Bridge the gap between the strategic and technical levels • Situational awareness • impact assessment • mitigation measures
Technical Level	• CSIRTs Network	• Incident handling during the cyber crisis • Incident monitoring and surveillance, including continuous analysis of threats and risks

Rialtas na hÉireann
Government of Ireland

Appendix E – Sample NECG (Cyber) Agenda

1. **Introduction**
    a. Decisions that need to be made immediately
    b. Governance
        i. Confirm Lead Agency
        ii. Agree Spokesperson(s)

2. **Situation update**
    a. Summary of incident
        i. severity assessment
        ii. sectoral impacts by LGDs
        iii. identify victim organisations
    b. Identify Government Departments to sit on NECG
    c. Identify other external support requirements to sit on NECG

4. **Confirm strategic purpose and priorities (this will inform decisions)**
    a. Agree Cyber emergency exit criteria (*NCEP 2.3.1 Exit Full Activation Mode*)
    b. Identify coordinating actions to be taken by Government Departments, supporting agencies and CNI operators to meet objectives

5. **Consideration of key risks and implications**

6. **Establish Communications subgroup (public information)**

7. **Support requirements and resources**
    a. Activation of appropriate plans and legislation
    b. Tasking of additional resources if required
    c. Activation of specialist support if required
    d. Support for Ministers

8. **Decisions and action items**

9. **Establish meeting schedule**
    a. DONM
    b. Subgroups