Comparative Assessment of the DHS *Harmonization of Cyber Incident Reporting to the Federal Government* Report and the Rules on Incident Reporting in the *EU Directive on Measures for a High Common Level of Cybersecurity Across the Union (NIS 2 Directive)*

The United States Department of Homeland Security and

The European Commission Directorate-General of Communications Networks, Content and Technology

Homeland Security

European Commission

Disclaimer - The present report provides a factual overview of the DHS Report recommendations and EU legal frameworks on incident reporting under Directive (EU) 2022/2555. This document is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or equity by any party against the United States, its departments, agencies, or entities, it officers, employees, or agents, or any other person. The present report does not recommend any action within the scope of binding provisions of Union law, nor does it seek to interpret those binding provisions. Where there appears to be a conflict or overlap between the report and any binding provision of Union law, then the binding provision of Union law applies. The report neither represents legal advice nor an official position of the European Commission. It is not an official interpretation of EU law, which is the prerogative of the Court of Justice of the European Union.

I. Introduction

In January 2023, the EU's Directive (EU) 2022/2555 on measures for high level of cybersecurity across the Union (NIS 2 Directive) entered into force, giving EU Member States 21 months to transpose it into national law. NIS 2 builds on the requirements of its predecessor, Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (the NIS Directive), in force since 2016, but it raises the EU common level of ambition on cybersecurity, through a wider scope, clearer rules and stronger supervision tools. NIS 2 harmonizes, strengthens, and streamlines security and incident reporting requirements for a larger number of entities, which are critical for the European economy and society.[1] The new Directive introduces more precise provisions on the process for incident reporting, content of the reports and timelines. NIS 2 seeks to strike the right balance between the need for swift reporting to avoid the potential spread of incidents, and the need for in-depth reporting to draw valuable lessons learned from individual incidents. The NIS 2 Directive is going to repeal the NIS Directive with effect from 18 October 2024.

The Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) established the Cyber Incident Reporting Council (CIRC), led by the Department of Homeland Security (DHS) to address the potential duplication arising from current and future Federal cyber incident reporting regimes in the United States.[2] In a September 2023 report entitled "Harmonization of Cyber Incident Reporting to the Federal Government,"[3] DHS, informed by the expertise and work of more than 30 Federal agencies on the CIRC, outlined a series of actionable recommendations on how the U.S. Government can streamline and harmonize the reporting of cyber incidents to better protect the nation's critical infrastructure. These recommendations were informed by extensive consultation with U.S. industry with an eye toward ensuring that relevant government agencies have access to sufficient information about incidents to support legitimate governmental purposes while minimizing the administrative burden on reporting entities so that they can focus their efforts on mitigating the impacts of the incident.[4]

To inform the ongoing implementation of CIRCIA and the NIS 2 Directive by the respective authorities and to support entities active in multiple jurisdictions in their efforts to respond to cyber incidents, DHS and DG CONNECT are publishing the present joint report that identifies the main similarities and divergences in the DHS Report's recommendations and the NIS 2 Directive.[5]

II. Mapping of Elements from the DHS Report and NIS 2 Directive Incident Reporting

For the purpose of this comparison exercise, DHS and DG CONNECT identified six main areas for comparative analysis between the DHS Report and the NIS 2 Directive: (i) definitions and reporting thresholds, (ii) timelines, triggers and types of cyber incident reporting, (iii) contents of cyber incident reports, (iv) reporting mechanisms, (v) aggregation of incident data, and (vi) public disclosure of cyber incident information. Each of the six areas of comparative analysis includes a schematic comparison of the frameworks that adheres to the actual texts, followed by general conclusions on similarities and differences.

Please note that additional technical comparisons on areas (i) and (ii) are available in an annex to this report on page 10.

I. DEFINITIONS & REPORTING THRESHOLDS

DHS Report – Recommendation[6]	NIS 2 Directive
What would have to be reported	**What has to be reported**
A **reportable cyber** incident	A **significant** incident
Reporting threshold If the incident leads or (if still under the covered entity's investigation[7]) could lead to: (1) a substantial loss of confidentiality, integrity, or availability of a covered information system, network, or operational technology; (2) a disruption or significant adverse impact on the covered entity's ability to engage in business operations or deliver goods, or services, including those that have a potential for significant impact on public health or safety or may cause serious injury or death; (3) disclosure or unauthorized access directly or indirectly to non-public personal information of a significant number of individuals; or (4) potential operational disruption to other critical infrastructure systems or assets.	***Reporting threshold*** The incident is considered significant if it has: (1) caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned; (2) affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage. An 'incident' is 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 (see Art 6, point (6) NIS 2)).

Comment:

The DHS Report and NIS2 use different language to define what is or would be reportable cyber incidents or otherwise describe the threshold of what is or would be reportable. The NIS 2 Directive requires entities to report "significant incidents," while the DHS Report uses the term "reportable cyber incidents," to describe what would be reportable.

Although there are differences in definitions, there are several commonalities across the DHS Report and NIS2 definitions. For example, both definitions of an incident include criteria related to the Confidentiality, Integrity, and Availability (CIA) triad or operational disruption of services.

II. TRIGGERS, TIMELINES FOR AND STAGES OF CYBER INCIDENT REPORTING

DHS Report – Recommendation[6]	NIS 2 Directive
Trigger	**Trigger**
From when the covered entity **reasonably believes that a reportable cyber incident has occurred.**	From when the covered entity **becomes aware of the significant incident.**
Timelines	**Timelines**
72 hours[8]	72 hours, preceded by an early warning within max 24 hours. Final report - not later than one month after the submission of the incident notification.
Stages of reporting	**Stages of reporting**
• **Initial Incident Report** • **Supplemental Incident Report** • **Incident Update** • **Final Incident Report (optional)**	• **Early Warning** • **Incident Notification** • **Intermediate Report** • **Final Report** • **Progress Report**

Comment:

The NIS 2-defined "early warning" and "incident notification" reports could be compared to the DHS Report's suggested "initial incident report," which are recommended to generally be required within 72 hours. However, per NIS 2, the "early warning" must occur within 24 hours. Separately, the intermediate report which is only required as part of NIS 2 when a CSIRT or competent authority request such a report, is comparable to the DHS Report's suggested "supplemental" and "incident update" reports to make the initial report more complete or correct information that has already been submitted. A final report is detailed as optional in the DHS Report's recommendation but required as part of NIS 2 within one month of the submission of the incident notification. NIS 2 provides for the submission of a progress report, in the event of an ongoing incident at the time of submission of the final report.

The DHS Report suggests exceptions for the recommended timeline and trigger for those incidents that necessitate an earlier reporting timeline such as disruption or degradation of the delivery of national critical functions (i.e., within less than 72 hours) and incidents that may include a longer timeline such as the loss of personal information without further impact on business operations (i.e., longer than 72 hours). Although there is a general overlap in the 72-hour timeline, the DHS Report and NIS 2 differ on the trigger language used to describe when an initial report should be made. NIS 2 uses "becoming aware" of the significant incident whereas the DHS Report uses "upon reasonable belief" that a reportable cyber incident has occurred.

III. CONTENTS OF CYBER INCIDENT REPORTS

DHS Report – Recommendation[6]	NIS 2 Directive
Initial Incident Report An initial incident report provides information about a reportable incident. Would be mandatory if the incident meets the definition of a reportable incident. **Supplemental Incident Report:** A supplemental incident report to an initial incident report makes the report more complete. Would be mandatory if the reporting entity becomes aware of significant new information. **Incident Update:** An incident update to an incident report corrects or amends the information previously provided to make the report more accurate. Would be mandatory if reporting entity realizes that significant previously submitted information was erroneous. **Final Incident Report** An optional final report is one submitted by the reporting entity to affirmatively complete the record or communicate that it considers the incident resolved. A final report would be mandatory if the incident may impact delivery of national critical functions (NCFs), vital goods or services to the public.	**Early Warning:** whether the significant incident is suspected of being caused by unlawful or malicious acts or could have a cross-border impact; Mandatory. **Incident Notification** Update of the information from the early warning; an initial assessment of the significant incident, severity and impact, where available, the indicators of compromise; Mandatory. **Intermediate Report** Relevant status updates. Upon request of CSIRT or competent authority. **Final Report** A mandatory final report must include (i) a detailed description of the incident, including its severity and impact; (ii) the type of threat or root cause that is likely to have triggered the incident; (iii) applied and ongoing mitigation measures; (iv) where applicable, the cross-border impact of the incident;

Comment:

The content across both documents appears comparable at a thematic level. The DHS Report offers recommendations for how to align content of cyber incident reports and to move toward a model reporting form or common data elements wherever practicable.[9] While NIS 2 uses different terminology for the types of reports, the above table demonstrates the approximate parallels.

The NIS 2 Directive requires E U Member States to submit to ENISA every three months a summary report on significant incidents, incidents, cyber threats and near misses. In order to contribute to the provision of comparable information, ENISA is in the process of drafting technical guidance on the parameters of the information to be included in the summary report (see Article 23 (9) NIS 2). Until this document is finalized, the available reference document for the templates is a non-binding reference document for national competent authorities and/or the CSIRTs "Guidelines on notification of Operators of Essential Ser- vices incidents (formats and procedures)" adopted under the NIS Directive by the NIS Cooperation Group in 2018. In its chapter 5, the document recommends the templates to use by EU Member States- one for the national incident notification procedure and one for annual summary reporting.[10]

The DHS Report's model reporting form and the NIS Cooperation Group reference document both include information on **identifying the reporting entity** (e.g., point of contact, name of the enti- ty, and other identifiers); **information on assistance** (e.g., parties involved as part of information sharing and coordinating response actions); **incident impacts** (e.g., sector or critical infrastructure, number of individuals affected); **cyber threat activity and discovery** (e.g., malware used, inside/ outside actor, indicators of compromise, discovery and status of incident); and **reporting entity response actions** (e.g., actions taken or ongoing to mitigate the incident).

Moreover, because of its application and effects across all EU Member States, NIS 2 requires information related to "cross-border" impact, which is not explicitly requested in the DHS model reporting form. However, the DHS Report does suggest asking for any known or potential secondary or cascading impacts, which could be interpreted to have similar meanings (i.e., cross-border impacts).

IV. REPORTING MECHANISMS

DHS Report – Recommendation[6]	NIS 2 Directive
Report Recommendation 5: The Federal Government should assess how best to streamline the receipt and sharing of cyber incident reports and cyber incident information, including through improvements to existing reporting mechanisms or the potential creation of a single portal.	The Commission may adopt implementing acts further specifying the type of information, the format and the procedure of a notification submitted pursuant to paragraph 1 of this Article and to Article 30 and of a communication submitted pursuant to paragraph 2 of this Article. Art 23 (11) NIS 2: According to Recital (106), in order to simplify the reporting of information required under this Directive as well as to decrease the administrative burden for entities, **Member States should provide technical means such as a single entry point, automated systems, online forms, user-friendly interfaces, templates, dedicated platforms for the use of entities, regardless of whether they fall within the scope of this Directive, for the submission of the relevant information to be reported.** Union funding supporting the implementation of this Directive, in particular within the Digital Europe programme, established by Regulation (EU) 2021/694 of the European Parliament and of the Council (21), could include support for single entry points. Furthermore, entities are often in a situation where a particular incident, because of its features, needs to be reported to various authorities as a result of notification obligations included in various legal instruments. Such cases create additional administrative burden and could also lead to uncertainties with regard to the format and procedures of such notifications. Where a single entry point is established, Member States are encouraged also to use that single entry point for notifications of security incidents required under other Union law, such as Regulation (EU) 2016/679 and Directive 2002/58/EC. The use of such single entry point for reporting of security incidents under Regulation (EU) 2016/679 and Directive 2002/58/EC should not affect the application of the provisions of Regulation (EU) 2016/679 and Directive 2002/58/EC, in particular those relating to the independence of the authorities referred to therein. ENISA, in cooperation with the Cooperation Group, should develop common notification templates by means of guidelines to simplify and streamline the information to be reported under Union law and decrease the administrative burden on notifying entities.

Comment:

A variety of reporting mechanisms are used by governing institutions in the U.S., the EU, and Member States. These could consist of web forms, web portals, secure file transmission systems, forms submitted via email, etc. Other mechanisms may include email messages, mail, fax, or phone communications to receive cyber incident reports in narrative form without any required format.

While the DHS Report recommends the adoption of a model reporting form or "common data elements" to harmonize reporting requirements and reduce burden on regulated entities, it also recommends assessing the feasibility of developing a single portal to receive incident reporting.

The NIS 2 Directive recommends to EU Member States to use technical means such as a single-entry point, automated systems, online forms, user-friendly interfaces, templates, dedicated platforms for the use of entities. The NIS 2 Directive specifies that the Commission may adopt implementing acts further specifying the type of information, the format, and the procedure of a notification submitted.

V. AGGREGATION OF INCIDENT DATA

Aggregation of incident data and the subsequent statistical analysis yields important insights into the ongoing trends when it comes to incidents and provides a much-needed different situational awareness picture, namely that is coming from the reporting entities themselves. At the same time, having public access to aggregated incident data contributes to raising the public awareness of the significance of incident reporting and to improving the overall cybersecurity maturity of entities. Understanding the benefits of incident reporting leads to better public acceptance of the need for such a mechanism and could incentivize more entities to participate in reporting incidents, without fearing the potential reputational risk of doing so.

According to Article 23(9) NIS 2, EU Member States have to submit to ENISA every three months a summary report, including anonymized and aggregated data on significant incidents, as well as on incidents, cyber threats and near misses, which are subject to voluntary notification. ENISA has to inform the NIS Cooperation Group and the CSIRTs network about its findings on notifications received every six months.

Aggregation of incident data was acknowledged as a challenge in the DHS Report as narrative fields are less useful for agencies that seek to structure data and perform trend analysis.

VI. PUBLIC DISCLOSURE OF CYBER INCIDENT INFORMATION

DHS Report – Recommendation[6]	NIS 2 Directive
Model language for delayed public notification (a) Public disclosure required by this regulation may be delayed when the Attorney General, Secretary of Homeland Security, or an appropriate law enforcement official informs a covered entity that public disclosure required by this regulation would pose a significant risk of impeding or compromising an ongoing or potential criminal investigation or cause damage to public safety, national security, or critical infrastructure. Such risk includes the potential for an adverse result, as provided by 18 U.S.C. § 2705(a)(2), or an emergency situation, as provided by 18 U.S.C § 3125(a)(1). If a delay longer than 30 days is needed, it must be specified in a written statement provided to the covered entity. (b) The Attorney General, Secretary of Homeland Security, or an appropriate law enforcement official shall inform the covered entity of the duration of the delay requested under paragraph (a) and may extend the period of delay for additional periods of up to 30 days if that official determines that disclosure continues to pose a significant risk in accordance with paragraph (a). The covered entity may notify appropriate U.S. regulatory agencies of such a request for delay.	**Art 23 (7) NIS 2:** Where public awareness is necessary to prevent a significant incident or to deal with an ongoing significant incident, or where disclosure of the significant incident is otherwise in the public interest, a Member State's CSIRT or, where applicable, its competent authority, and, where appropriate, the CSIRTs or the competent authorities of other Member States concerned, may, after consulting the entity concerned, inform the public about the significant incident or require the entity to do so.

Comment:

NIS 2 includes the possibility for EU Member States' authorities or CSIRTs to inform the public of a significant incident or to require the entities to do so, where public awareness is necessary to prevent a significant incident or to deal with it.

The DHS Report notes that most existing laws and regulations requiring public disclosure of certain types of cyber incidents allowed for a covered entity to delay disclosure at the request of an appropriate law enforcement official who determined that the disclosure could impede a criminal investigation or cause damage to public safety or national security. In accordance with this, the DHS Report recommends a model provision that is geared towards protecting ongoing criminal investigations or preventing disclosure of incidents that pose a significant risk to public safety, national security, or critical infrastructure. It also specifically calls out the Attorney General, Secretary of Homeland Security, or other appropriate law enforcement official as officials that can delay public disclosure under said circumstances.

III. Summary of findings

In comparing the NIS 2 Directive and the DHS Report, several key areas of divergence or commonality were specified. In area (i), the Directive and the Report use different language to define reportable cyber incidents or otherwise describe the threshold of what is reportable. Similarly, area (ii) notes different timelines and triggers for notifications. Nevertheless, area (iii) notes that the content of incident reports across both documents appears comparable at a thematic level. Similarly, area (iv) notes the documents seek to reduce unnecessary complications or technical difficulties entities may encounter when trying to file a report. Area (v) outlines the (recommended or actual) requirements for including aggregated and anonymized incident data in reports under the NIS 2 Directive, while the DHS Report acknowledges this inclusion may be of benefit, but the inclusion of similarly aggregated data was not included in the recommendations issued. Finally, area (vi) details the similarities and differences in each document's provisions for public disclosure of certain cyber incidents.

ENDNOTES

1 NIS 2 is a binding legal act, which must be transposed in the laws of all 27 EU Member States by 17 October 2024. It constitutes the horizontal baseline for cybersecurity across the EU. In addition, at an EU level, there is sectorial legislation, which also requires entities to report cybersecurity incidents, such as Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA Regulation).

2 *See generally* 6 U.S.C. § 681f.

3 September 2023 report.

4 Please note that the DHS Report is not legally binding. It is a report that contains recommendations, which if adopted by Federal agencies, could help to streamline and harmonize Federal cyber incident reporting requirements while increasing alignment in the approach of U.S. Departments and Agencies. The recommendations included in the report serve as models for harmonization but are not enforceable, and each U.S. Department and Agency would need to assess the feasibility of adopting the recommendations prior to doing so.

5 The DHS Report does not reflect any final decision regarding the content of in-process or future DHS rules. DHS will consider public comments and otherwise comply with the requirements of the Administrative Procedure Act before finalizing pending cyber-related rulemakings.

6 Informed by the Cyber Incident Reporting Council

7 For the purposes of the DHS Report, the term "covered entity" refers to an entity that is subject to a particular regulatory requirement to report cyber incidents to one or more Federal agencies. The identity of covered entities will vary from regulatory regime to regulatory regime based on the relevant authority and as determined by the regulator.

8 The proposed timeline includes certain exceptions. For incidents that may disrupt or degrade the delivery of national critical functions or the reporting entity's ability to deliver vital goods or services to the public, or impact public health or

safety, agencies may require covered entities to submit an initial report to the required agenc[ies] within *less than 72 hours*. For incidents that involve the loss of personal information without further impact on business operations, agencies may include a timeline *longer than 72 hours*.

9 **See the DHS Report Recommendation 4 on the use of a model reporting form or common data elements. *For more precise information on the recommended contents of the reports, please see the report Appendix C, "Widely Used Contents of Reports Across Current Requirements" and Appendix E, the Model Reporting Form and Reference Sheet. See also Appendix F: Potential Common Terminology for Types of Cyber Incident Reports.***

10 ***For more precise information on the recommended contents of the reports, see the*** *https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53677"*

ANNEX

Further details on the mapping of elements from the DHS Report Recommendations and NIS 2 Directive incident reporting framework

This annex provides further technical details, analysis, and comparisons of areas (i) definitions & reporting thresholds, and (ii) timelines, triggers for and types of cyber incident reporting.

DEFINITIONS & (RECOMMENDED OR ACTUAL) REPORTING THRESHOLDS

DHS Report Recommendation[6]	NIS 2 Directive
A **reportable cyber** incident is a cyber incident that leads to, or, if still under the covered entity's investigation, could reasonably lead to any of the following: (1) a substantial loss of confidentiality, integrity, or availability of a covered information system, network, or operational technology; (2) a disruption or significant adverse impact on the covered entity's ability to engage in business operations or deliver goods, or services, including those that have a potential for significant impact on public health or safety or may cause serious injury or death; (3) disclosure or unauthorized access directly or indirectly to non-public personal information of a significant number of individuals; or (4) potential operational disruption to other critical infrastructure systems or assets. The term "reportable cyber incident" includes, but is not limited to, indications of compromises of information systems, networks, or operational technologies of customers or other third parties as well as a business or operational disruption caused by a compromise of a cloud service provider, managed service provider, or other third-party data hosting provider.	Art 23(1) NIS2 requires Member States to ensure that essential and important entities notify, without undue delay, its CSIRT or, where applicable, its competent authority of any incident that has a significant impact on the provision of their services as referred to in paragraph 3 **(significant incident)**. The general NIS 2 definition of an 'incident' is 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 (see Art 6 (6) NIS2). According to Article 23 (3) NIS 2, 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.

(chart continued on next page)

DEFINITIONS & (RECOMMENDED OR ACTUAL) REPORTING THRESHOLDS (CONTINUED)

DHS Report Recommendation[6]	NIS 2 Directive
The term "reportable cyber incident" does not include: (i) any lawfully authorized activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States, including activities undertaken pursuant to a warrant or other judicial process; (ii) any event where the cyber incident is perpetrated in good faith by an entity in response to a specific request by the owner or operator of the information system; or (iii) the threat of disruption as extortion, as described in CIRCIA section 2240(14)(A). Note: In adopting this model definition of a reportable cyber incident, Federal agencies may choose to incorporate or tailor some or all of sub-elements (1) through (4) above, including, to ensure consistency with their statutory mandates. Federal agencies will also need to independently determine within their rules what constitutes a "covered entity," a "covered information system," and a "significant" number of impacted individuals.	This is further elaborated in Recital (101), according to which the NIS 2 Directive lays down a multiple-stage approach to the reporting of significant incidents in order to strike the right balance between, on the one hand, swift reporting that helps mitigate the potential spread of significant incidents and allows essential and important entities to seek assistance, and, on the other, in-depth reporting that draws valuable lessons from individual incidents and improves over time the cyber resilience of individual entities and entire sectors. In that regard, this Directive should include the reporting of incidents that, **based on an initial assessment carried out by the entity concerned, could cause severe operational disruption of the services or financial loss for that entity or affect other natural or legal persons by causing considerable material or non-material damage. Such initial assessment should take into account, inter alia, the affected network and information systems, in particular their importance in the provision of the entity's services, the severity and technical characteristics of a cyber threat and any underlying vulnerabilities that are being exploited as well as the entity's experience with similar incidents. Indicators such as the extent to which the functioning of the service is affected, the duration of an incident or the number of affected recipients of services could play an important role in identifying whether the operational disruption of the service is severe.** The Commission is empowered to adopt the so-called **implementing acts** further specifying the cases in which an incident shall be considered to be significant for all entities in the NIS2 Directive scope. By **17 October 2024**, the Commission shall adopt such implementing act with regard to DNS

	service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines and of social networking services platforms (see Art 23(11) NIS2).

(RECOMMENDED OR ACTUAL) TIMELINES, TRIGGERS FOR AND TYPES OF CYBER INCIDENT REPORTING

DHS Report Recommendation[6]	NIS 2 Directive
A covered entity that experiences a reportable cyber incident shall submit an **initial written report** to the required agency or agencies within 72 hours of when the **covered entity reasonably believes** that a reportable cyber incident has occurred. Note: For incidents that may disrupt or degrade the delivery of national critical functions or the reporting entity's ability to deliver vital goods or services to the public, or impact public health or safety, agencies may require covered entities to submit an initial report to the required agenc[ies] within less than 72 hours. Note: For incidents that involve the loss of personal information without further impact on business operations, agencies may include a timeline longer than 72 hours. Such a requirement should consider the potential national or economic security implications of the loss of personal information and the ability of individuals to mitigate harm from the compromise of their information. **Multiple stage approach:** **Initial Incident Report:** Mandatory if the incident meets the definition of a reportable incident. **Supplemental Incident Report:** Mandatory if the reporting entity becomes aware of significant new information. **Incident Update:** Mandatory if reporting entity realizes that significant previously submitted information was erroneous. **Final Incident Report:** An optional final report is one submitted by the reporting entity to affirmatively complete the record or communicate that it considers the incident resolved.	**Multiple stage approach:** **Early warning** ***Timeline:*** Without undue delay and in any event within **24 hours** of becoming aware of the significant incident ***Trigger:*** From **becoming aware of the significant incident** **Incident notification** ***Timeline:*** without undue delay and in any event within 72 hours of becoming aware of the significant incident. ***Trigger:*** From **becoming aware of the significant incident** ***Intermediate report:*** Report on relevant status updates ***Trigger:*** request of a CSIRT or, where applicable, the competent authority **Final report** ***Timeline:*** not later than one month after the submission of the incident notification ***Trigger:*** incident notification **Progress report:** in the event of an ongoing incident at the time of the submission of the final report referred to in point (d), Member States shall ensure that entities concerned provide a progress report at that time and a final report within one month of their handling of the incident. ***Trigger:*** ongoing incident at the time of the submission of the final report