Draft compromises - LIBE opinion on the NIS2 Directive

Rapporteur: Lukas MANDL

Chapters I and II

RECITALS 1-26

CA27	Covers AMs 1 (rapp), 2 (rapp), 3 (rapp), 4 (rapp), 5 (rapp), 6 (rapp), 7 (rapp), 8 (rapp), 9 (rapp), 10 (rapp), 11 (rapp), 12 (rapp), 13 (rapp), 85 (ID), 86 (S&D), 87part (S&D), 88 (S&D), 89 (ID), 90 (ID), 92 (ECR), 95 (S&D), 96part (ECR), 97 (S&D), 100 (S&D), 101 (S&D), 134 (RE) Fall: AMs 91 (ECR), 93 (ECR), 94 (Greens), 98 (ECR), 99 (Greens) (1) Directive (EU) 2016/1148 of the European Parliament and the Council[11] aimed at building cybersecurity capabilities across the Union, mitigating threats to network and information systems used to provide essential services in key sectors and ensuring the continuity of such services when facing cybersecurity incidents, thus contributing to the Union's ***security and to the effective functioning of its*** economy and society to function effectively. (AMs 1R, 85) (2) Since the entry into force of Directive (EU) 2016/1148 significant progress has been made in increasing the Union's level of cybersecurity resilience. The review of that Directive has shown that it has served as a catalyst for the institutional and regulatory approach to cybersecurity in the Union, paving the way for a significant change in mind-set. That Directive has ensured the completion of national frameworks by defining national cybersecurity strategies, establishing national capabilities, and implementing regulatory measures covering essential infrastructures and actors identified by each Member State. It has also contributed to cooperation at Union level through the establishment of the Cooperation Group and a network of national Computer Security Incident Response Teams ('CSIRTs network'). Notwithstanding those achievements, the review of Directive (EU) 2016/1148 has revealed inherent shortcomings that prevent it from addressing effectively contemporaneous and emerging cybersecurity challenges. ***Moreover, the expansion of online activities in the context of the COVID-19 pandemic has highlighted the importance of cybersecurity, which is essential for EU citizens to be able to trust innovation and connectivity, as well as large-scale education and training thereon. The Commission should therefore support Member States in the design of educational programmes on cybersecurity with a view to enable important and essential entities to recruit cybersecurity experts who allow them to comply with the obligations arising from this Directive. (AM 134) (AM 86, 101, 134)*** (3) Network and information systems have developed into a central feature of everyday life with the speedy digital transformation and interconnectedness of society, including in cross-border exchanges. That development has led to an expansion of the cybersecurity threat landscape, bringing about new challenges, which require adapted, coordinated and innovative responses in all Member States. The number, magnitude, sophistication, frequency and impact of cybersecurity incidents are increasing, and present a major threat to the functioning of network

	and information systems. As a result, cyber incidents can impede the pursuit of economic activities in the internal market, generate financial losses, undermine user confidence~~, and~~ cause major damage to the Union economy, ~~and~~ the functioning of our ***democracy, and the values and freedom on which our*** society ***is based***. Cybersecurity preparedness and effectiveness are therefore now more essential than ever to ***the Union's security and*** the proper functioning of the internal market ***in light of the digital transformation of day-to-day activities across the Union. This requires closer cooperation of authorities within and between Member States as well as between national authorities and responsible Union bodies.*** (AMs 87part, 88) (4) *[...] COM proposal* (5) All those divergences entail a fragmentation of the internal market and are liable to have a prejudicial effect on its functioning, affecting in particular the cross-border provision of services and level of cybersecurity resilience due to the application of different standards. ***Ultimately, these divergences can lead to higher vulnerability of some Member States to cybersecurity threats, with potential spillover effects across the Union, both with regard to its internal market and its overall security.*** This Directive aims to remove such wide divergences among Member States, in particular by setting out minimum rules regarding the functioning of a coordinated regulatory framework, by laying down mechanisms for the effective ***and real time*** cooperation among the responsible authorities in each Member State***, between the competent authorities of the Member States***, by updating the list of sectors and activities subject to cybersecurity obligations and by providing effective remedies and sanctions which are instrumental to the effective enforcement of those obligations. Therefore, Directive (EU) 2016/1148 should be repealed and replaced by this Directive. (AM 2, 89) (6) This Directive leaves unaffected the ability of Member States to take the necessary measures to ensure the protection of the essential interests of their ***national*** security, to safeguard public policy and public security, and to allow for the ***prevention,*** investigation, detection and prosecution of criminal offences, in compliance with Union law. In accordance with Article 346 TFEU, no Member State is to be obliged to supply information the disclosure of which would be contrary to the essential interests of its public security. In this context, national and Union rules for protecting classified information, non-disclosure agreements, and informal non-disclosure agreements such as the Traffic Light Protocol[14], are of relevance. (AMs 3, 90) (7) *[...] COM proposal* (8) ***The responsibility of Member States*** in accordance with Directive (EU) 2016/1148for determining which entities meet the criteria to qualify as operators of essential services ('identification process') ***has led to*** wide divergences among Member States in that regard***. Without prejudice to the specific exceptions provided in this Directive***, a uniform criterion should be established that determines the entities falling within the scope of application of this Directive ***to eliminate these divergences and ensure legal certainty regarding the risk management requirements and reporting obligations for all relevant entities***. That criterion should consist of the application of the size-cap rule, whereby all medium and large enterprises, as defined by Commission Recommendation 2003/361/EC[15] , that

	operate within the sectors or provide the type of services covered by this Directive, fall within its scope. Member States should not be required to establish a list of the entities that meet this generally applicable size-related criterion. (AM 4) (8a) ***Taking into consideration the differences in the national public administration frameworks, Member States retain their decision-making capacity regarding the designation of entities within the scope of this Directive. (AM 92)*** (9) Small or micro entities fulfilling certain criteria that indicate a key role for the economies or societies of Member States or for particular sectors or types of services ***based on a risk-assessment, including entities defined as critical entities or entities equivalent to critical entities under Directive (EU) XXX/XXX of the European Parliament and the Council[1a]***, should also be covered by this Directive. Member States should be responsible for establishing a list of such entities, and submit it to the Commission. (AM 5) (10) The Commission, in cooperation with the Cooperation Group, ***should*** issue guidelines on the implementation of the criteria applicable to micro and small ***entities***. (AM 6) (11) *[...] COM proposal* (AM 93 falls) (12) Sector-specific legislation and instruments can contribute to ensuring high levels of cybersecurity, while taking full account of the specificities and complexities of those sectors. Where a sector–specific Union legal act requires essential or important entities to adopt cybersecurity risk management measures or to notify incidents or significant cyber threats of at least an equivalent effect to the obligations laid down in this Directive, those sector-specific provisions, including on supervision and enforcement, should apply. The Commission ***should*** issue guidelines in relation to the implementation of the lex specialis. This Directive does not preclude the adoption of additional sector-specific Union acts addressing cybersecurity risk management measures and incident notifications. This Directive is without prejudice to the existing implementing powers that have been conferred to the Commission in a number of sectors, including transport and energy. (AM 7) (13) *[...] COM proposal* (14) In view of the interlinkages between cybersecurity and the physical security of entities, a coherent approach should be ensured between Directive (EU) XXX/XXX of the European Parliament and of the Council[17] and this Directive***, wherever possible and appropriate***. To achieve this, Member States should ensure that critical entities, and equivalent entities, pursuant to Directive (EU) XXX/XXX are considered to be essential entities under this Directive. Member States should also ensure that their cybersecurity strategies provide for a policy framework for enhanced coordination between the competent ***authorities within and between Member States,*** under this Directive and the one under Directive (EU) XXX/XXX in the context of information sharing on ***cyber*** incidents and cyber threats and the exercise of supervisory tasks. Authorities under both Directives ***within and between Member States*** should cooperate and exchange information, particularly ***on*** relation to the identification of critical entities, cyber threats, cybersecurity risks, incidents affecting critical entities as well as on the cybersecurity measures taken by ***competent authorities under this Directive relevant for*** critical entities. Upon request of competent authorities under Directive (EU) XXX/XXX, competent

	authorities under this Directive should be allowed to ***assess the cybersecurity of*** essential entity identified as critical. Both authorities should cooperate and exchange information ***in real time*** for this purpose. (AM 8) (15) *[...] COM proposal* (AM 94 falls) (16) *[...] COM proposal* (17) *[...] COM proposal* (18) Services offered by data centre service providers may not always be provided in a form of cloud computing service. Accordingly, data centres may not always constitute a part of cloud computing infrastructure. In order to manage all the risks posed to ***cyber***security, this Directive should cover also providers of such data centre services that are not cloud computing services. For the purpose of this Directive, the term 'data centre service' should cover provision of a service that encompasses structures, or groups of structures, dedicated to the centralised accommodation, interconnection and operation of information technology and network equipment providing data storage, processing and transport services together with all the facilities and infrastructures for power distribution and environmental control. The term 'data centre service' does not apply to in-house, corporate data centres owned and operated for own purposes of the concerned entity. (AM 9) (19) *[...] COM proposal* (20) Those growing interdependencies are the result of an increasingly cross-border and interdependent network of service provision using key infrastructures across the Union in the sectors of energy, transport, digital infrastructure, drinking and waste water***, food production, processing and distribution***, health, certain aspects of public administration, as well as space in as far as the provision of certain services depending on ground-based infrastructures that are owned, managed and operated either by Member States or by private parties is concerned, therefore not covering infrastructures owned, managed or operated by or on behalf of the Union as part of its space programmes. Those interdependencies mean that any disruption, even one initially confined to one entity or one sector, can have cascading effects more broadly, potentially resulting in far-reaching and long-lasting negative impacts in the delivery of services across the internal market. The ***intensified attacks against information systems during the*** COVID-19 pandemic ***have*** shown the vulnerability of our increasingly interdependent societies in the face of low-probability risks. ***Therefore, further investments in cybersecurity are required. (AMs 10, 95)*** ***(20a) It is crucial to raise cyber-awareness and cyber-resilience in all critical and important entities, including public administration entities.*** (AM 96part) (21) In view of the differences in national governance structures and in order to safeguard already existing sectoral arrangements or Union supervisory and regulatory bodies, Member States should be able to designate more than one national competent authority responsible for fulfilling the tasks linked to the security of the network and information systems of essential and important entities under this Directive. Member States should be able to assign this role to an existing authority ***and ensure that it has adequate resources to carry out its tasks effectively and efficiently.*** (AM 97)

	(22) In order to facilitate cross-border cooperation and communication among authorities and to enable this Directive to be implemented effectively, it is necessary for each Member State to designate a national single point of contact responsible for coordinating issues related to ***cybersecurity*** and cross-border cooperation at Union level. (AM 11) (23) Competent authorities or the CSIRTs should receive notifications of incidents from entities in an effective and efficient way. The single points of contact should be tasked with forwarding incident notifications ***in real time*** to the single points of contact of ***all*** other Member States. At the level of Member States' authorities, to ensure one single entry point in every Member States, the single points of contacts should also be the addressees of relevant information on incidents concerning financial sector entities from the competent authorities under Regulation XXXX/XXXX which they should be able to forward, as appropriate, to the relevant national competent authorities or CSIRTs under this Directive. (AM 12) (25) As regards personal data, CSIRTs should be able to provide, in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council[19] ***and with Directive 2002/58/EC***, on behalf of and upon request by an entity under this Directive, ~~a proactive scanning of the network and information systems used for the provision of their services.~~ ***a security scan of the information systems and the network range used for the provision of their services to identify, mitigate or prevent specific threats***. Member States should aim at ensuring an equal level of technical capabilities for all sectorial CSIRTs. Member States may request the assistance of the European Union Agency for Cybersecurity (ENISA) in developing national CSIRTs. ***Furthermore, cybersecurity risks should never be used as a pretext for violations of fundamental rights.*** (AM 13, 100) (26) *[...] COM proposal*

ARTICLES 1-11

CHAPTER I - General provisions (Art. 1-4)

Article 1 - subject matter Falls: AM 137 (ECR) 1. This Directive lays down measures with a view to ensuring a high common level of cybersecurity within the Union. 2. To that end, this Directive: (a) lays down obligations on Member States to adopt national cybersecurity strategies, designate competent national authorities, single points of contact and computer security incident response teams (CSIRTs); (b) lays down cybersecurity risk management and reporting obligations for entities of a type referred to as essential entities in Annex I and important entities in Annex II;

CA1	**Article 2 - scope**

	Covers AMs 39 (rapp), 40 (rapp), 138part (RE), 139 (Greens), 145 (Left), 146 (Greens), 147 (Greens), 150 (Left), 152part (Left), 153part (S&D), 155 (RE), 156 (Greens) Fall: AMs 38 (rapp), 140 (Left), 141 (ECR), 142 (ECR), 143 (Greens), 144 (ECR), 149 (Left), 151 (ECR), 154 (S&D), 157 (ECR) 1. This Directive applies to public and private entities of a type referred to as essential entities in Annex I and as important entities in Annex II. This Directive does not apply to entities that qualify as micro and small enterprises within the meaning of Commission Recommendation 2003/361/EC[28]***. Article 3 Paragraph 4 of the Annex to Commission Recommendation 2003/361/EC is not applicable***. (AM 139 part) 2. However, regardless of their size ***and based on a risk assessment in accordance with Article 18***, this Directive also applies to entities referred to in Annexes I and II, where: ***(AM 39)*** (a) the services are provided by one of the following entities: (i) public electronic communications networks or publicly available electronic communications services referred to in point 8 of Annex I; (ii) trust service providers referred to point 8 of Annex I; (iii) top–level domain name registries and domain name system (DNS) service providers referred to in point 8 of Annex I; (b) the entity is a public administration entity as defined in point 23 of Article 4; (c) the entity is the sole provider of a service ***at national or regional level***; (AM 145) (d) a ~~potential~~ disruption of the service provided by the entity could have an impact on public safety, public security or public health; (AM 146) (e) a ~~potential~~ disruption of the service provided by the entity could induce systemic risks, in particular for the sectors where such disruption could have a cross-border impact; (AM 147) (f) the entity is critical because of its specific importance at regional or national level for the particular sector or type of service, or for other interdependent sectors in the Member State; (g) the entity is identified as a critical entity pursuant to Directive (EU) XXXX/XXXX of the European Parliament and of the Council[29] [Resilience of Critical Entities Directive], or as an entity equivalent to a critical entity pursuant to Article 7 of that Directive. Member States shall establish a list of entities identified pursuant to points (b) to (f) and submit it to the Commission by [6 months after the transposition deadline]. Member States shall review the list, on a regular basis, and at least every two years thereafter and, where appropriate, update it. 3. This Directive is without prejudice to the competences of Member States concerning the maintenance of public security, defence and national security in compliance with Union law.

	4. This Directive applies without prejudice to Council Directive 2008/114/EC30 and Directives 2011/93/EU[31] and 2013/40/EU[32] of the European Parliament and of the Council. ***4a. Any processing of personal data pursuant to this Directive shall comply with Regulation (EU) 2016/679 and with Directive 2002/58/EC and shall be limited to what is strictly necessary and proportionate for the purposes of this Directive. (AM 40, 138part, 150, 153part, 156)*** 5. Without prejudice to Article 346 TFEU, information that is confidential pursuant to Union and national rules, such as rules on business confidentiality, shall be exchanged with the Commission and other relevant authorities only where that exchange is necessary for the application of this Directive. The information exchanged shall be limited to that which is ***necessary*** to the purpose of that exchange. The exchange of information shall preserve the confidentiality of that information and protect the security and commercial interests of essential or important entities. (AM 152) 6. Where provisions of sector–specific acts of Union law require essential or important entities either to adopt cybersecurity risk management measures or to notify incidents or significant cyber threats, and where those requirements are at least equivalent in effect to the obligations laid down in this Directive, the relevant provisions of this Directive, including the provision on supervision and enforcement laid down in Chapter VI, shall not apply. 6a. ***Before 31 December 2022, the Commission shall publish a legislative proposal to include Union institutions, offices, bodies and agencies (EUIs) in the overall EU-wide cybersecurity framework, with a view to achieving a uniform level of protection through consistent and homogeneous rules. (AM 155)***

Article 3 - Minimum harmonisation (no AMs tabled = COM text)

CA2	**Article 4 - Definitions** Covers AMs 41 (rapp), 42 (rapp), 43 (rapp), 159 (Left), 162 (Left) Fall: AMs 158 (Greens), 160 (Greens), 161 (Greens), 163 (ECR), 164 (ECR), 165 (ECR), 166 (ECR), 167 (ECR), 168 (ECR) For the purposes of this Directive, the following definitions apply: (1) ‘network and information system’ means: (a) an electronic communications network within the meaning of Article 2(1) of Directive (EU) 2018/1972; (b) any device or group of inter–connected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data***, and that are integrated into the IT system and used for the provision of their intended services***; (AM 41) (c) digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance;

	(2) 'security of network and information systems' means the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems; (3) 'cybersecurity' means cybersecurity within the meaning of Article 2(1) of Regulation (EU) 2019/881 of the European Parliament and of the Council[33]; (4) 'national strategy on cybersecurity' means a coherent framework of a Member State providing strategic objectives and priorities on the ***cybersecurity*** in that Member State; (AM 42) (5) 'incident' means any event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the related services offered by, or accessible via, network and information systems; (6) 'incident handling' means all actions and procedures aiming at detection, analysis and containment of and a response to an incident; (7) 'cyber threat' means a cyber threat within the meaning Article 2(8) of Regulation (EU) 2019/881; (8) 'vulnerability' means a weakness, susceptibility or flaw of an asset, system, process or control that can be exploited by a cyber threat; (9) 'representative' means any natural or legal person established in the Union explicitly designated to act on behalf of i) a DNS service provider, a top-level domain (TLD) name registry, a cloud computing service provider, a data centre service provider, a content delivery network provider as referred to in point 8 of Annex I or ii) entities referred to in point 6 of Annex II that are not established in the Union, which may be addressed by a national competent authority or a CSIRT instead of the entity with regard to the obligations of that entity under this Directive; (10) 'standard' means a standard within the meaning of Article 2(1) of Regulation (EU) No 1025/2012 of the European Parliament and of the Council[34]; (11) 'technical specification' means a technical specification within the meaning of Article 2(4) of Regulation (EU) No 1025/2012; ~~(12) 'internet exchange point (IXP)' means a network facility which enables the interconnection of more than two independent networks (autonomous systems), primarily for the purpose of facilitating the exchange of internet traffic; an IXP provides interconnection only for autonomous systems; an IXP does not require the internet traffic passing between any pair of participating autonomous systems to pass through any third autonomous system, nor does it alter or otherwise interfere with such traffic;~~ (AM 159) (13) 'domain name system (DNS)' means a hierarchical distributed naming system which allows end-users to reach services and resources on the internet; (14) 'DNS service provider' means an entity that provides recursive or authoritative domain name resolution services to internet end-users and other DNS service providers; (15) 'top–level domain name registry' means an entity which has been delegated a specific TLD and is responsible for administering the TLD including the registration of domain names under the TLD and the technical operation of the

	TLD, including the operation of its name servers, the maintenance of its databases and the distribution of TLD zone files across name servers; (16) 'digital service' means a service within the meaning of Article 1(1)(b) of Directive (EU) 2015/1535 of the European Parliament and of the Council[35]; (17) 'online marketplace' means a digital service within the meaning of Article 2 point (n) of Directive 2005/29/EC of the European Parliament and of the Council[36]; (18) 'online search engine' means a digital service within the meaning of Article 2(5) of Regulation (EU) 2019/1150 of the European Parliament and of the Council[37]; (19) 'cloud computing service' means a digital service that enables on-demand administration and broad remote access to a scalable and elastic pool of shareable and distributed computing resources; (20) 'data centre service' means a service that encompasses structures, or groups of structures, dedicated to the centralised accommodation, interconnection and operation of information technology and network equipment providing data storage, processing and transport services together with all the facilities and infrastructures for power distribution and environmental control; (21) 'content delivery network' means a network of geographically distributed servers for the purpose of ensuring high availability, accessibility or fast delivery of digital content and services to internet users on behalf of content and service providers; ~~(22) 'social networking services platform' means a platform that enables end-users to connect, share, discover and communicate with each other across multiple devices, and in particular, via chats, posts, videos and recommendations);~~ (AM 162) (23) 'public administration entity' means an entity in a Member State that complies with the following criteria: (a) it is established for the purpose of meeting needs in the general interest and does not have an industrial or commercial character; (b) it has legal personality; (c) it is financed, for the most part, by the State, regional authority, or by other bodies governed by public law; or it is subject to management supervision by those authorities or bodies; or it has an administrative, managerial or supervisory board, more than half of whose members are appointed by the State, regional authorities, or by other bodies governed by public law; (d) it has the power to address to natural or legal persons administrative or regulatory decisions affecting their rights in the cross-border movement of persons, goods, services or capital. Public administration entities that carry out activities in the areas of public security, law enforcement, defence or national security are excluded. (24) 'entity' means any natural ***person or any*** legal person created and recognised as such under the national law of its place of establishment, which may, acting under its own name, exercise rights and be subject to obligations; (AM 43) (25) 'essential entity' means any entity of a type referred to as an essential entity in Annex I;

	(26) 'important entity' means any entity of a type referred to as an important entity in Annex II.

CHAPTER II - Coordinated cybersecurity regulatory frameworks (Art. 5-11)

CA3	**Article 5 - National cybersecurity strategy** Covers AMs 44 (rapp), 45 (rapp), 169 (Greens), 171 (Greens), 172 (Greens), 173 (ECR), 174 (RE), 175 (S&D), 176part (Greens), 177 (S&D), 178 (ID) Falls: AM 170 (ECR) 1. Each Member State shall adopt a national cybersecurity strategy defining the strategic objectives and appropriate policy and regulatory measures, with a view to achieving and maintaining a high level of cybersecurity. The national cybersecurity strategy shall include, in particular, the following: (a) a definition of objectives and priorities of the Member States' strategy on cybersecurity, ***taking into account the general level of cybersecurity awareness amongst citizens as well as on the general level of security of consumer connected devices; (AM 169)*** (b) a governance framework to achieve those objectives and priorities, including the policies referred to in paragraph 2 and the roles and responsibilities of public bodies and entities as well as other relevant actors; (c) an assessment to identify relevant assets and cybersecurity risks in that Member State; (d) an identification of the measures ensuring preparedness, response and recovery to incidents, including cooperation between the public and private sectors; (e) a list of the various authorities and actors involved in the implementation of the national cybersecurity strategy; (f) a policy framework for enhanced coordination between the competent authorities under this Directive and Directive (EU) XXXX/XXXX of the European Parliament and of the Council38 [Resilience of Critical Entities Directive], ***both within and between Member States,*** for the purposes of information sharing on incidents and cyber threats and the exercise of supervisory tasks. (AM 44) 2. As part of the national cybersecurity strategy, Member States shall in particular adopt the following policies: (a) a policy addressing cybersecurity in the supply chain for ICT products and services used by essential and important entities for the provision of their services; (b) guidelines regarding the inclusion and specification of cybersecurity-related requirements for ICT products and service in public procurement***, including but not limited to encryption requirements and the promotion of the use of open source cybersecurity products***; (AM 171) (c) a policy to promote and facilitate coordinated vulnerability disclosure within the meaning of Article 6;

	(d) a policy related to sustaining the general availability and integrity of the public core of the open internet; ***(da) a policy related to sustaining the use of open data and open source as part of security through transparency; (AM 172)*** ***(db) a policy promoting the privacy and security of personal data of users of online services; (AM 173)*** (e) a policy on promoting and developing cybersecurity skills, awareness raising and research and development initiatives, ***including the development of training programmes on cybersecurity to provide entities with specialists and technicians; (AM 174)*** (f) a policy on supporting academic and research institutions ***that contribute to the national cybersecurity strategy by developing and deploying*** cybersecurity tools and secure network infrastructure ***that contribute to the national cybersecurity strategy***, ***including specific policies addressing issues related to gender representation and balance in this sector***; (AM 175, 176part, 177) (g) a policy, relevant procedures and appropriate information-sharing tools to support voluntary cybersecurity information sharing between companies in compliance with Union law; (h) a policy addressing specific needs of SMEs, in particular those excluded from the scope of this Directive, in relation to guidance and support in improving their resilience to cybersecurity threats ***and their capability to respond to cybersecurity incidents***. (AM 45R, 178) 3. Member States shall notify their national cybersecurity strategies to the Commission within three months from their adoption. Member States may exclude specific information from the notification where and to the extent that it is strictly necessary to preserve national security. 4. Member States shall assess their national cybersecurity strategies at least every four years on the basis of key performance indicators and, where necessary, amend them. The European Union Agency for Cybersecurity (ENISA) shall assist Member States, upon request, in the development of a national strategy and of key performance indicators for the assessment of the strategy.

CA4	**Article 6 - Coordinated vulnerability disclosure and a European vulnerability registry** Covers AM 179 (Greens) Falls: 180 (ECR), 181 (Left) 1. Each Member State shall designate one of its CSIRTs as referred to in Article 9 as a coordinator for the purpose of coordinated vulnerability disclosure. The designated CSIRT shall act as a trusted intermediary, facilitating, where necessary, the interaction between the reporting entity and the manufacturer or provider of ICT products or ICT services. Where the reported vulnerability concerns multiple manufacturers or providers of ICT products or ICT services across the Union, the designated CSIRT of each Member State concerned shall cooperate with the CSIRT network.

	2. ENISA shall develop and maintain a European vulnerability registry. To that end, ENISA shall establish and maintain the appropriate information systems, policies and procedures with a view in particular to enabling important and essential entities and their suppliers of network and information systems to disclose and register vulnerabilities present in ICT products or ICT services, as well as to provide access to the information on vulnerabilities contained in the registry to all interested parties. The registry shall, in particular, include information describing the vulnerability, the affected ICT product or ICT services and the severity of the vulnerability in terms of the circumstances under which it may be exploited, the availability of related patches and, in the absence of available patches, guidance addressed to users of vulnerable products and services as to how the risks resulting from disclosed vulnerabilities may be mitigated. ***To ensure security and accessibility of the information included in the registry, ENISA shall apply state of the art security measures and make the information available in machine-readable formats through corresponding interfaces. (AM 179)***

CA5 **Covers only AM 182**	**Article 7 - National cybersecurity crisis management frameworks** **Covers AM 182 (Left)** **[...] par. 3** (a) objectives of national ***and, where relevant and applicable, regional and cross-border*** preparedness measures and activities; (AM 182)
	Article 8 - National competent authorities and single points of contact - no AMs were tabled. **Article 9 - Computer security incident response teams (CSIRTs)** No compromise is proposed on Article 9. Given that the ECR AMs 183 + 184 to Article 9 are consequential AMs linked to the different treatment of public administration entities, they should fall if the COMP on Article 1 is adopted; if the COMP falls and AM 137 is adopted, they should also be deemed adopted.

CA6	**Article 10 - Requirements and tasks of CSIRTs** Covers AM 187 (Left) Falls: AM 185 (ECR), 186 (Greens) 1. CSIRTs shall comply with the following requirements: (a) CSIRTs shall ensure a high level of availability of their communications services by avoiding single points of failure, and shall have several means for being contacted and for contacting others at all times. CSIRTs shall clearly specify the communication channels and make them known to constituency and cooperative partners; (b) CSIRTs' premises and the supporting information systems shall be located in secure sites;

	(c) CSIRTs shall be equipped with an appropriate system for managing and routing requests, in particular, to facilitate effective and efficient handovers; (d) CSIRTs shall be adequately staffed to ensure availability at all times; (e) CSIRTs shall be equipped with redundant systems and backup working space to ensure continuity of its services; (f) CSIRTs shall have the possibility to participate in international cooperation networks. 2. CSIRTs shall have the following tasks: (a) monitoring cyber threats, vulnerabilities and incidents at national level; (b) providing early warning, alerts, announcements and dissemination of information to essential and important entities as well as to other relevant interested parties on cyber threats, vulnerabilities and incidents; (c) responding to incidents; (d) providing dynamic risk and incident analysis and situational awareness regarding cybersecurity; (e) providing, upon request of an entity, a ~~proactive scanning of the network and~~ ***security scan of the*** information systems ***and network range*** used for the provision of their services ***to identify, mitigate or prevent specific threats***; ***the processing of personal data in the context of such scanning shall be limited to what is strictly necessary, and in any case to IP addresses and URLs; (AM 187)*** (f) participating in the CSIRTs network and providing mutual assistance to other members of the network upon their request. 3. CSIRTs shall establish cooperation relationships with relevant actors in the private sector, with a view to better achieving the objectives of the Directive. 4. In order to facilitate cooperation, CSIRTs shall promote the adoption and use of common or standardised practices, classification schemes and taxonomies in relation to the following: (a) incident handling procedures; (b) cybersecurity crisis management; (c) coordinated vulnerability disclosure.

CA7	**Article 11 - Cooperation at national level** Covers AM 46 (rapp), 47 (rapp) Fall: AM 188 (ECR) 1. Where they are separate, the competent authorities referred to in Article 8, the single point of contact and the CSIRT(s) of the same Member State shall cooperate with each other with regard to the fulfilment of the obligations laid down in this Directive. 2. Member States shall ensure that either their competent authorities or their CSIRTs receive notifications on incidents, and significant cyber threats and near misses submitted pursuant to this Directive. Where a Member State decides that its CSIRTs shall not receive those notifications, the CSIRTs shall, to the extent necessary to carry out their tasks, be granted access to data on incidents notified by the essential or important entities, pursuant to Article 20.

	3. Each Member State shall ensure that its competent authorities or CSIRTs inform its single point of contact of notifications on incidents, significant cyber threats and near misses submitted pursuant to this Directive. 4. To the extent necessary to effectively carry out the tasks and obligations laid down in this Directive, Member States shall ensure appropriate cooperation between the competent authorities and single points of contact and law enforcement authorities, data protection authorities, and the authorities responsible for critical infrastructure pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] and the national financial authorities designated in accordance with Regulation (EU) XXXX/XXXX of the European Parliament and of the Council39 [the DORA Regulation] within that Member State ***in line with their respective competences***. (AM 46R) 5. Member States shall ensure that their competent authorities regularly provide ***timely*** information to competent authorities designated pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive] on cybersecurity risks, cyber threats and incidents affecting essential entities identified as critical, or as entities equivalent to critical entities, pursuant to Directive (EU) XXXX/XXXX [Resilience of Critical Entities Directive], as well as the measures taken by competent authorities in response to those risks and incidents. (AM 47)