Council of the European Union
General Secretariat

Brussels, 16 August 2022

WK 10961/2022 INIT

LIMITE

CSC
CYBER
CSCI
CIS

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

WORKING DOCUMENT

From: To:	General Secretariat of the Council Security Committee
N° Cion doc.:	7474/22, 7670/22
Subject:	Proposal for a Regulation laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union: preparation of the CSC opinion on security of information aspects - Comparison to the Proposal for a Regulation of the European Parliament and of the Council on information security

For your information and in order to prepare the opinion of the Council Security Committee, delegations will find attached a comparison table of provisions of the proposal for a Regulation laying down measures for a high common level of **cybersecurity** at the institutions, bodies, offices and agencies of the Union and the proposal for a Regulation of the European Parliament and of the Council on **information security**.

ANNEX

Comparative table – Proposals for Regulation on Cybersecurity and Information Security

	Proposal for a Regulation on Cybersecurity 2022/0085 (COD) (Cyber proposal)	Objectives	Proposal for a Regulation on Information Security 2022/0084 (COD) (Infosec proposal)	Objectives	Interaction between 2 proposals
1	**Art.4**	Each UIBA (Union Institutions, bodies and agencies) shall establish an internal cybersecurity framework on risk management, governance and control – such framework concerns the entirety of IT environment.	**Art.5**	Each UIBA shall establish an information security risk management process, steps are provided and mandatory factors to be considered in this process.	While the Cyber proposal lays down an obligation for UIBAs to establish their own cybersecurity framework on risk management, the Infosec proposal regulates in more detail the risk management process only for the protection of information they handle, without touching the other cybersecurity aspects. Cybersecurity requires a framework for rules that are easy to adapt to the rapidly evolving cyber threat landscape and can be tailored to the needs of heterogeneous organisations. Information security, in contrast, requires a stable approach that is translated into a common baseline of standards applicable uniformly in a community of organisations, thus enabling trust and secure exchange of information. These two approaches are reflected in the two proposals and complement each other.

Comparative table – Proposals for Regulation on Cybersecurity and Information Security

	Proposal for a Regulation on Cybersecurity 2022/0085 (COD) (Cyber proposal)	Objectives	Proposal for a Regulation on Information Security 2022/0084 (COD) (Infosec proposal)	Objectives	Interaction between 2 proposals
2	**Art.5**	Each UIBA shall adopt cybersecurity measures and a baseline (set of minimum cybersecurity rules) to address the risks identified under the frameworks established in line with article 4.	Obligations in InfoSec proposal are prescriptive, as explained below in the **relevant boxes under row 3**.		The Cyber proposal lays down an obligation for UIBAs to adopt cybersecurity rules on the domains listed in Annex I, while the InfoSec proposal regulates some of these domains with specific rules relevant for the security of information in view of facilitated trusted and secure exchanges of information. Provisions are complementary. In practice: 1. Information is assessed and a certain level of confidentiality is assigned, 2. If processed in a CIS, mandatory measures provided by InfoSec proposal apply 3. These are complemented by the necessary measures established in the framework of the cyber proposal.

Comparative table – Proposals for Regulation on Cybersecurity and Information Security

	Proposal for a Regulation on Cybersecurity 2022/0085 (COD) (Cyber proposal)	Objectives	Proposal for a Regulation on Information Security 2022/0084 (COD) (Infosec proposal)	Objectives	Interaction between 2 proposals
3	**Annex I - Domains to be addressed by each UIBA in their cybersecurity baseline**	Cybersecurity policy, including objectives and priorities for:			Different remits, which are fully complementary
		(a)Security of network and information systems (NISs)	Non-classified communication and information systems (CISs) are covered by **Chapter 3 and art.15-17 of Chapter 4**		While NISs are broadly defined as any devices performing automatic processing of digital data, the CISs are a specific subset of NISs, with different security needs as they are primary focused on the confidentiality of the information handled and stored. As an example, a CIS of the Commission handling non-classified information can be deployed over a NIS regulated by the cybersecurity regulation (the Commission's data centre in Luxembourg).
		(b)Cloud computing services	**Art.15(3)**	UIBAs shall set contractual safeguards for the protection of non-classified information processed by outsourced services.	Provisions are complementary, Infosec proposal being more specific on the obligations to UIBAs from an information security perspective.
		(c)Technical arrangements for teleworking	**Annex I – point 10,11**	Specific obligations for UIBAs to ensure the protection of sensitive non-classified (SNC) information by appropriately securing the relevant equipment and applications	Provisions are complementary as the Cyber proposal lays down the obligation for UIBAs to address the teleworking arrangements while the Infosec proposal prescribes the specific obligation.

Comparative table – Proposals for Regulation on Cybersecurity and Information Security

	Proposal for a Regulation on Cybersecurity 2022/0085 (COD) (Cyber proposal)	Objectives	Proposal for a Regulation on Information Security 2022/0084 (COD) (Infosec proposal)	Objectives	Interaction between 2 proposals
				used in telework.	
		Organisation of cybersecurity, including the definition of roles and responsibilities	**Art.8 - Organisation of information security**	All UIBAs are required to set a Security Authority and other specific authorities, with clear responsibilities in the field of information security.	Provisions are complementary as the Cyber proposal lays down the obligation for UIBAs to address the organisation of cybersecurity roles and responsibilities, while Infosec proposal prescribes the obligation of UIBAs to establish the relevant information security authorities, regulating security of information.
		Asset management, including IT asset inventory and IT network cartography	**No corresponding provision**		
		Access control	**Art.11(2)**	UIBAs shall identify the CISs users to grant them access to the information handled within.	The Infosec proposal includes a common baseline of high-level safeguards, targeted to the protection of information handled in CISs in view of ensuring easy interconnection between systems processing information at the same level. Such safeguards are the minimum required to ensure a consistent approach and trust between institutions. They are technology neutral and relate to standard practices in the information security community. They aim at ensuring information
			Art.11(3)	UIBAs shall maintain their security logs for all CISs for investigation purposes.	
			Art.11(4)(e)	UIBAs are require adopting measures restricting the access to information of contractor's personnel.	

Comparative table – Proposals for Regulation on Cybersecurity and Information Security

	Proposal for a Regulation on Cybersecurity 2022/0085 (COD) (Cyber proposal)	Objectives	Proposal for a Regulation on Information Security 2022/0084 (COD) (Infosec proposal)	Objectives	Interaction between 2 proposals
			Art.17(1)(a)	Obligation for UIBAs to implement strong authentication for accessing SNC in CIS and to encrypt SNC in transmission and in storage.	security.
			Art.17(1)(h)	UIBAs shall implement measures based on the principles of need-to-know and zero trust to minimise access to sensitive non-classified information by service providers and contractuals.	
		Operations security	**No corresponding provision**		
		Communications security	**Annex I – point 16**	Obligation for UIBAs to protect SNC by using encryption in transit and crypto mechanisms.	Provisions are complementary as the Cyber proposal lays down the obligation for UIBAs to address the security of communications, while Infosec proposal prescribes an explicit obligation to use crypto mechanisms for the protection of information.
		System acquisition, development and maintenance	**No corresponding provision**		
		Supplier relationship	**Art.17(1)(d)**	This article imposes UIBAs to have contractual provisions for	Provisions are complementary as there is a specific obligation related to the

Comparative table – Proposals for Regulation on Cybersecurity and Information Security

	Proposal for a Regulation on Cybersecurity 2022/0085 (COD) (Cyber proposal)	Objectives	Proposal for a Regulation on Information Security 2022/0084 (COD) (Infosec proposal)	Objectives	Interaction between 2 proposals
				the security of information in any outsourcing contracts.	contractual provisions in the InfoSec proposal.
		Incident management and cooperation with CERT-EU	**Art.11(5)(d)**	Obligation for UIBAs to formally follow up the Infosec incidents in accordance with the cybersecurity Regulation.	Provisions are complementary as an information security incident need to be managed in respect of the requirements laid down in the Cyber proposal.
			Art.15 (1)	Obligation for UIBAs to set procedures for managing the incidents related to the non-classified information.	Provisions are complementary, one general applicable to all cybersecurity incidents and one specific, related to information security.
		Business continuity management and crisis management	**Art.5(3)f**	When performing the infosec risk management process, each UIBA is required to consider the business continuity.	Provisions are complementary as the Cyber proposal lays down the obligation for UIBAs to address the business continuity management and crisis management, while Infosec proposal prescribes an explicit obligation to consider business continuity when performing a risk management process (in terms of information security).
		Cybersecurity education, awareness-raising and training programmes	**Art.4 (6)**	UIBAs shall provide training and awareness activities on handling and storing non-classified information.	While the Cyber proposal lays down an obligation for UIBAs to include cybersecurity training and awareness in their baseline, the InfoSec proposal prescribes the obligation of UIBAs to provide such activities limited to

Comparative table – Proposals for Regulation on Cybersecurity and Information Security

	Proposal for a Regulation on Cybersecurity 2022/0085 (COD) (Cyber proposal)	Objectives	Proposal for a Regulation on Information Security 2022/0084 (COD) (Infosec proposal)	Objectives	Interaction between 2 proposals
					information security. The broad scope of the **cybersecurity** training is evident from the list of examples below: Basics of Cybersecurity *- Part 1: mobile security, creation of strong passwords, data privacy and phishing* *- Part 2: ransomware and DDoS attacks, phishing, teleworking and browsing safe* *- Part 3: the context of cybersecurity, types of malware and social media* *- Part 4: cryptocurrency, the internet of things, malicious documents and attachments, how to store and transfer data safely;* *On **Information security**, the trainings are focused on:* *- information assessment and categorisation.* *- marking and handling of each confidentiality level of information processed.* Training scope is quite complementary.

Comparative table – Proposals for Regulation on Cybersecurity and Information Security

	Proposal for a Regulation on Cybersecurity 2022/0085 (COD) (Cyber proposal)	Objectives	Proposal for a Regulation on Information Security 2022/0084 (COD) (Infosec proposal)	Objectives	Interaction between 2 proposals
4	**Annex II - Measures to be addressed by each UIBA in the implementation of their cybersecurity baseline**	Concrete steps for moving towards Zero Trust Architecture	**Art.17(1)h - minimum requirements for CISs handling SNC**	Each UIBA shall implement security measures based on the zero-trust architecture to minimise access to SNC in CISs by service providers and contractors	Specific obligation in the Infosec proposal, limited to the access to information handled by a CIS, complementing the provision in Cyber proposal.
		Adoption of multifactor authentication as a norm across network and information systems	**Art.17(1)a - minimum requirements for CISs handling SNC**	Each UIBA shall implement strong authentication to access SNC in CISs.	As above, a specific obligation provided by the Infosec proposal as limited to information handled by a CIS, complementing the provision in Cyber proposal, laying down the obligation to adopt a multifactor authentication.
		Establishment of software supply chain security through criteria for secure software development and evaluation.	**No corresponding provision**		
		Enhancement of procurement rules to facilitate a high common level of cybersecurity through: • the removal of contractual barriers that limit information sharing from IT service providers about incidents, vulnerabilities and cyber threats with CERT-EU • the contractual obligation	**No corresponding provision**		

Comparative table – Proposals for Regulation on Cybersecurity and Information Security

	Proposal for a Regulation on Cybersecurity 2022/0085 (COD) (Cyber proposal)	Objectives	Proposal for a Regulation on Information Security 2022/0084 (COD) (Infosec proposal)	Objectives	Interaction between 2 proposals
		to report incidents, vulnerabilities and cyber threats as well as to have appropriate incidents response and monitoring in place.			
5	**Governance** **Art. 9 - IICB** **Art.12 - CERT-EU**	IICB is responsible for monitoring the implementation of the Cybersecurity regulation, for supervising and providing strategic direction to CERT-EU. CERT-EU will contribute to the cybersecurity of the unclassified IT environment of all Union institutions, bodies and agencies by advising them on cybersecurity.	**Art.10 Subgroup on information assurance**	The sub-group shall provide guidance on processing the information in the CISs, in coordination with the ICCB, and sets a metadata scheme to help the exchange of information between UIBAs, when CISs are interconnected.	Provisions are complementary as the Cyber proposal looks to the support to the overall IT environment and operations of UIBAs, while the Infosec proposal addresses individual specific systems. Still the Infosec proposal provides as one of the responsibilities of the IA sub-group to contribute to the coherence between both proposals.