EUROPEAN
COMMISSION

Brussels, 22.3.2022
SWD(2022) 66 final

COMMISSION STAFF WORKING DOCUMENT

IMPACT ANALYSIS REPORT

Accompanying the document

Proposal for a Regulation of the European Parliament and of the Council

on information security in the institutions, bodies, offices and agencies of the Union

{COM(2022) 119 final} - {SWD(2022) 65 final}

Table of Contents

Glossary

Term	*Acronym*
Artificial intelligence	AI
Commission national security expert group	ComSEG
Computer Emergency Response Team – EU	CERT-EU
Communication and Information System	CIS
CONFIDENTIEL UE/EU CONFIDENTIAL	C-UE/EU-C
Directorate-General for Human Resources and Security	DG HR
European Union	EU
European External Action Service	EEAS
European Union Agency for Cybersecurity	ENISA
EU classified information	EUCI
EU NORMAL	EU-N
Hypertext Transfer Protocol Secure	HTTPS
Information technology	IT
Information and communication technology	ICT
The Inter-service Steering Group	ISSG
International Standards Organisation	ISO
Joint Research Centre	JRC
Network and Information System	NIS
Public Key Infrastructure	PKI
Public Use	PU
Regulatory Scrutiny Board	RSB
RESTREINT UE/EU RESTRICTED	R-UE/EU-R
SECRET UE/EU SECRET	S-UE/EU-S
Sensitive non-classified	SNC
Secure/Multipurpose Internet Mail Extensions	S/MIME
Service Level Agreement	SLA
Treaty on the European Union	TEU
Treaty on the Functioning of the European Union	TFEU
TRES SECRET UE/EU TOP SECRET	TS-UE/EU-TS
Union institutions and bodies	UIBs
Virtual Private Network	VPN

1. INTRODUCTION: POLITICAL AND LEGAL CONTEXT

1.1. Political context

In recent times the Union institutions and bodies (UIBs) have been exposed to attack in all their domains due to the ever-increasing amounts of sensitive and classified information they need to handle in the context of addressing the EU challenges (e.g. economic recovery, public health, security, defence or research). The information handled by the European administration is a very attractive target and needs to be appropriately protected. This requires swift action aiming at enhancing the protection of sensitive and classified information within the Union institutions and bodies.

Member States have already called on our institutions to move into this direction. A key feature of the Strategic Agenda for 2019-2024 adopted by the European Council in June 2019 is to protect our societies from these threats. In its conclusions[1], the European Council called in particular on 'the EU institutions, together with the Member States, to work on measures to enhance the resilience and improve the security culture of the EU against cyber and hybrid threats from outside the EU, and to better protect the EU's information and communication networks, and its decision-making processes, from malicious activities of all kinds'.

In the same line, the General Affairs Council of December 2019[2] concluded that the EU institutions and bodies, supported by Member States, should develop and implement a comprehensive set of measures to ensure their security. This echoes a long-standing request from the Council Security Committee to investigate a common core of security rules for the Council, the Commission and the EEAS.[3]

In July 2020, the Commission adopted its EU Security Union Strategy[4], by which it committed to complement the national efforts in the area of security. As part of this strategy, the Commission proposed to create a minimum set of rules on information security and cybersecurity across all Union institutions and bodies.

On 16 December 2020, the Commission adopted a new EU cybersecurity package[5] with significantly increased measures to ensure cybersecurity, including an extension of the scope of the Network and Information Security Directive to cover central governments and major economic regions. This package reinforced the commitment to improve the overall level of cybersecurity across Union institutions and bodies through consistent and homogeneous rules.

---

1 EUCO 9/19

2 14972/19

3 WK 10563/2018 INIT section 9

4 Communication on the EU Security Union Strategy, COM(2020) 605, 24 July 2020 (Strategic priority 'A future-proof security environment).

5 The EU's Cybersecurity Strategy for the Digital Decade | Shaping Europe's digital future (europa.eu) including a Joint Communication with the High Representative of the Union for Foreign Affairs and Security Policy (JOIN(2020)18) and also a revised Network and Information Security (NIS) Directive (COM(2020)823)

ENISA, the European Union Agency for Cybersecurity, published its key observations in the ENISA Threat Landscape 2020[6]:

- The most targeted sectors were digital services, government administration, and the technology industry.
- Two of the main identified trends in malicious activity pertain to phishing and ransomware.
- Top 5 motivations: financial, espionage, disruption, political, and retaliation.
- Top 5 wanted assets in order of desire: Industrial property and trade secrets, state/military classified information, server infrastructure, authentication data, and financial data.
- 84% of cyberattacks rely on social engineering.
- 67% of malware was delivered via encrypted HTTPS connections.
- 230K new strains of malware appear every day.
- 71% of organisations experienced malware activity that spread from one employee to another.

These observations underline the need for a harmonised and efficient approach to information security, highlighting in particular the need for training and awareness of all personnel.

Good security of information is a basic element of an open and efficient administration. It is also an area where harmonised practices across institutions and bodies are necessary to ensure secure and interoperable electronic communications.

1.2. Legal context

Currently, the Union institutions and bodies either have their own information security legal rules in place or have not adopted such rules at all.

Depending on the nature of their tasks, only a limited number of UIBs handle EU classified information (EUCI).

Currently, in the UIBs where they do exist, information security rules address some or all of the following topics:

1. security needs for security of information and scheme to categorize information, and minimum protection rules for sensitive and/or classified information;

2. procedures to govern access to the relevant information by staff, including clearance procedures, access to facilities, and online meetings;

3. information security requirements for systems handling UIBs information, mechanisms for the certification of cryptographic products within the EU;

[6] ENISA, Threat Landscape 2020, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-main-incidents

4. governance structures and mechanisms in charge of governing a secured information exchange within UIBs and to ensure mutual trust in handling of information between parties;

5. procedures to ensure proper encryption of information inside UIBs, depending on its level of sensitivity;

6. security investigation in the context of an EUCI breach;

7. awareness raising and training on information security;

8. counterintelligence and counterterrorism activities, in relation to risks of eavesdropping, spying and interception of information; and

9. access control to information and identity management related issues across institutions, including registration, authentication, and so on.

1.3. Categories and types of information handled by Union institutions and bodies

The UIBs handle too many different types of information to compile an exhaustive list. However, it is useful to give some examples of these categories and types in order to provide the context to the problem definition in the next section.

Firstly, information is often categorised according to its level of confidentiality, based on the potential impacts of unauthorised disclosure. Generally, there are four main levels although different entities currently use different nomenclature and definitions for some of the non-classified levels:

- Public information
- Normal, non-sensitive information
- Sensitive / limited, but non-classified information
- Classified information

Classified information that is created by the UIBs is called EUCI, and is further subdivided into four levels, from the lowest to highest impacts. These levels are established by an agreement of 2011[7] with the Member States and are common to all UIBs handling EUCI.

(1) RESTREINT UE/EU RESTRICTED
(2) CONFIDENTIEL UE/EU CONFIDENTIAL
(3) SECRET UE/EU SECRET
(4) TRES SECRET UE/EU TOP SECRET

The following list gives examples of some types of information that are handled by the UIBs:

[7] AGREEMENT between the Member States of the European Union, meeting within the Council, regarding the protection of classified information exchanged in the interests of the European Union (2011/C 202/05)

- Personal information (on staff members and in many other areas)
- VIP information (e.g. travel plans and protection plans)
- Security-related information (security arrangements, counterintelligence and counterterrorism information etc.)
- Defence information
- Draft legislation and policies
- Trade negotiations
- Competition cases
- Health-related information
- Budgetary and financial information
- Border control information
- Information on international crime
- Investigations (security, fraud, competition, trade, pharmaceutical)
- Legal documents and evidence in court proceedings
- Scientific research
- Information on nuclear material and other hazardous chemicals
- Media, education and culture
- Official publications such as the Official Journal
- Historical archives of the Institutions

While incomplete, these examples give an idea of the breadth and variable nature of the types of information handled by the Union institutions and bodies. It is important to note that in recent years, the amount of sensitive and classified information has increased significantly as UIBs have been tasked with financing or supervisory roles in areas where information is either very sensitive or classified. This is, for instance, the case with the European Defence Fund, the Foreign Direct Investment fund, greenhouse gases emissions allowances or border control operations. These new activities often entail exchanges of large amounts of sensitive and classified information between UIBs.

In terms of communication and information systems, there is a huge variety of IT systems handling UIBs information. All Union institutions and bodies manage online portals and websites and corporate applications for daily work. Many of them have also secure applications to handle sensitive non-classified information. A few of them operate classified systems, at the RESTREINT UE/EU RESTRICTED, CONFIDENTIAL UE/EU CONFIDENTIAL and SECRET UE/EU SECRET levels.

Most UIBs use local, hybrid and cloud-based services to host their applications and make extensive use of external staff to develop, manage and operate them.

1.4. Other relevant EU initiatives

The need to act on the security of information is regularly identified as a high priority for the EU. The European Parliament and the Council adopted a Directive in 2016 concerning measures for a high common level of security of network and information

systems across the Union[8], and the High Representative of the Union for Foreign Affairs and Security Policy issued a joint communication on the subject in 2017[9].

The NIS2 Directive[10] was adopted by the COM in December 2020 with a view to increasing the level of cybersecurity across the EU. While the Directive targets commercial organisations, it clearly demonstrates the growing need for high levels of security over information, and it is applicable to the European Cloud Service Providers that are used by many Union institutions and bodies for the provision of communication and information systems.

The current iteration of the Security Union Strategy[11] runs from 2020 to 2025, outlining four main pillars of action[12] where the EU can help Member States in fostering security for all those living in Europe. Several of the topics addressed under these pillars focus on security of information, cybersecurity, cooperation and information exchange, and critical infrastructure. This document covers the proposed legislative actions for information security. A similar document covers the proposed legislative initiative laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union.

2. PROBLEM DEFINITION

2.1. What is the problem?

Despite the progress that has been made towards more consistent rules for the protection of information, there is a significant lack of coordination on information security issues between the Union institutions and bodies.

Firstly, for non-classified information which is by far the majority of the information handled by the UIBs, there are different categories of information, different markings and different handling instructions. All of these differences may lead to confusion when information is shared and to a significant likelihood of under-protection of information. The existing schemes for categorisation of information do not adequately cover exchanges of information between UIBs.

Secondly, there is a significant difference between the level of security of UIBs depending on the applicable information security rules and the resources allocated to this task. Some small entities have no formal security rules. This leads to risks of attackers taking advantage of different levels of security to create a security breach in the weakest link and use that as a starting point for further attacks on other UIBs.

---

8 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194/1)

9 Resilience, Deterrence and Defence: Building strong cybersecurity for the EU (JOIN(2017) 450 final)

10 COM(2020) 823 final

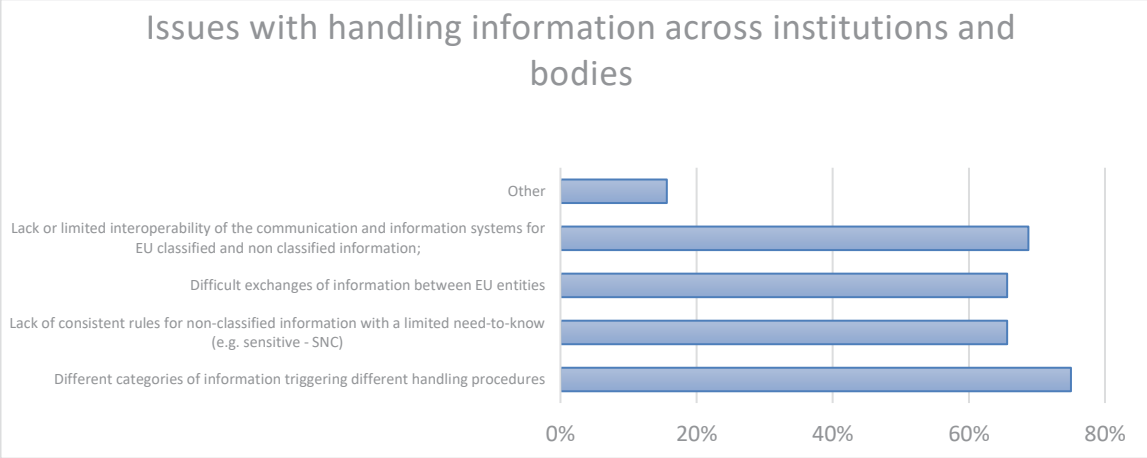
11 COM/2020/605 final

12 The four pillars are: a future-proof security environment, tackling evolving threats, protecting Europeans from terrorism and organised crime, and a strong European security ecosystem.

Third, multiple UIBs perform the same security tasks, often in different ways, which could be done more consistently and efficiently in a coordinated manner or delegated to one Union institution or body in charge of handling the matter.

Fourth, the rules on teleworking and new working methods such as remote meetings are mostly either absent or out of date following the COVID-19 situation. Consistency in this area is increasingly important for sharing information and platforms, which should permit substantial cost savings.

In conclusion, failing to update and harmonise the information security rules would cause or perpetuate weaknesses in many key areas where the threat landscape is changing rapidly. This would represent a major risk for the security of the Union institutions and bodies and would lead to increased risks of disruptions of the European administration. These risks do not only affect UIBs but they also have potential consequences for EU businesses, Member States authorities and society at large. In the survey on this proposal, respondents in the UIBs reported the lack of rules and coordination on information security as key issues leading to difficulties with the secure exchange of information.



2.2. What are the problem drivers?

The analysis that follows seeks to illustrate the various drivers that contribute to the problem presented in the preceding section.

Driver 1: Increasing threats to information

Threats assessments from public and private entities have highlighted the growing threats to the security of information for many years. Unfortunately, this continues to be true, with the sophistication and goals of attacks becoming more and more ambitious.

In addition to the traditional threats to the information handled by the European administration (human espionage, crime, terrorism and political activism) recent years have seen an increase in **hybrid actions** on the part of state and non-state actors, defined by the Commission and European External Action Service as the mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military,

economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare.[13]

As reported by CERT-EU[14], the number of major attacks on Union institutions and bodies was on the rise during the third quarter of 2020, while ransomware remains the most significant cybercrime threat in Europe. For example, attacks on infrastructure in the US have recently caused shortages of food and fuel, and organisations have been forced to pay millions of dollars to cyber criminals following ransomware attacks[15]. Infrastructure in the UIBs has been subjected to serious attacks from major actors in the cyber world, and the disciplines of information security and IT security must be well coordinated to effectively counter these threats.

The primary objective of the adversary is to steal sensitive information from a specific institution or body depending on its sector of activity (e.g. diplomacy, health, energy, transportation, finance, etc.). Some attackers are also challenging the current approach of an open internet and their policies aim at disrupting it. In the current COVID-19 pandemic, adversaries are looking, among other things, for sensitive information on vaccines as demonstrated by a recent cyberattack against the European Medicines Agency[16]. The UIBs' incident response teams and CERT-EU confirm that many attacks are currently focusing on identifying and exploiting weaknesses in remote access solutions.

Driver 2: Increasing collaboration between the Union institutions and bodies

The quantity and types of information that are exchanged between UIBs continue to increase as each of these collaborates with several other UIBs. New bodies or agencies are regularly established with the aim of meeting the changing needs of the EU and its Member States.

UIBs form a group of stakeholders in which substantial information flows take place under well established, mutual trust. The threat actor's typical goal is to compromise a member of the community whose security maturity is lower than others for further exploitation. Post-exploitation activity can then allow the adversary to move to other targets within the community.

The increasing collaboration is happening at all levels of information confidentiality. The Commission is currently leading the development of a SUE system for the handling and sharing of classified information up to SECRET UE/EU SECRET (or the national equivalent) between UIBs and with the Member States.

---

[13] Joint Framework on countering hybrid threats a European Union response (2016).

[14] CERT-EU, Direct threats to EU institutions, Bodies and Agencies. See TLP-WHITE-2020Q3-Threat_Landscape_Report-Executive-Summary-v1.0.pdf (europa.eu).

[15] For a recent example of a US$ 11m ransom paid, see https://threatpost.com/jbs-paid-11m/166767/

[16] See https://www.ema.europa.eu/en/news/cyberattack-ema-update-6

Driver 3: Workplace transformation

The Union institutions and bodies have integrated remote working practices for many years, with some staff already teleworking for a small part of their working time and specific tasks such as systems development outsourced to external contractors. However, the recent pandemic caused an overnight change in working practices. Remote communication tools become the rule and many procedures that were still at least partly paper-based were rapidly changed to enable electronic processing and exchanges of information. Generalised teleworking increased the importance of electronic signatures to prove the integrity of documents and of fully paperless workflows, at all levels of classification. For instance, the Commission generalised the use of secure email (S/MIME[17]) to all staff and rolled out qualified signature tokens to all senior managers.

The experience of the COVID-19 pandemic and the requirement for staff to work remotely, where possible, have shown that the UIBs can operate effectively under those circumstances. This will manifest in three main changes:

- More staff will work remotely, more of the time – typically, up to 60% remote working may be permitted in some UIBs. The pandemic has shown that most services can continue to work effectively via remote working, as long as the necessary tools are in place.
- The numbers of external personnel working on UIBs premises will be significantly reduced, with the default delivery method for many contracts changing to remote working.
- Fully electronic workflows (including signatures) will become be the norm for all business transaction across UIBs.

These aspects may bring significant cost reductions as well as improvements in the quality of life of UIBs personnel, but they will require changes in the handling of information. The proposed rules take account of the new working practices, which present significant challenges for the security of information.

Since spring 2020, several threat actors, including state-sponsored ones, have been intensively exploiting vulnerabilities in VPN products used by the UIBs to provide remote access services. A recent report titled *Enduring from Home: COVID-19's Impact on Business Security*[18] released by Malwarebytes points out that since the start of the pandemic, teleworking has been the principal reason for security breaches in 20% of organisations. Also, 24% of the survey respondents, said that their organisations had to pay unexpected costs to address security breaches or malware infections after teleworking was deemed necessary. The use of unauthorised communication tools is another concern since they may not protect information sufficiently and may be subject to non-EU government control. This is particularly relevant when personnel can use their own mobile devices for corporate purposes, and the line between corporate and personal equipment is blurred.

---

17 rfc3851 (ietf.org)

18 Malwarebytes, Enduring from home - COVID-19's impact on business security (https://resources.malwarebytes.com/files/2020/08/Malwarebytes_EnduringFromHome_Report_FINAL.pdf) [19] See Open Government – what is the value and what are the barriers and drivers? | FUTURIUM | European Commission (europa.eu)

Driver 4: Digital transformation and open government

Despite the challenging security environment, the Commission believes that open government principles are key for the success of the EU in the future. Open government is understood as open, collaborative and digital-based services characterised by a deliberate, declared and purposeful effort to increase openness and collaboration through technology in order to deliver increased public value. Open government is based on the principles of transparency, collaboration and participation functioning within an open governance framework[19].

Having transparent information security rules in place should foster the development of the UIBs digital services at a lower cost and with a high level of security. While the requirements for security are known, this allows an easier development of common systems for all UIBs.

The uptake of the EU digital services will take place in a context where the number of Information and Communication Technologies (ICT) systems, cloud services and connected devices is constantly rising. With the advent of 5G (and beyond) networks and the rise of the Internet of Everything (IoE), the number of connected devices and systems will explode in the near future, with very significant information security issues as UIBs does not generally control the 5G supply chain. In the context of any organisation and in conjunction with the proliferation of e-services, these developments lead to big data of various levels of sensitivity and all of this information must be protected.

While not all data or information is equally sensitive from a confidentiality viewpoint, it may call for protection from the perspective of integrity (correctness) and traceability, i.e. guarantees that the information is intact and verifying that it comes from legitimate sources. Moreover, all of the stored information and data should be always and readily available via the underlying services (availability).

Driver 5: Outsourcing of information

The outsourcing of information has increased greatly in recent times, due to two main factors. The first is the increased use of outsourced services, whereby external personnel process information on behalf of the UIBs. Secondly, the massive increase in outsourced systems, particularly using cloud technologies. The information security rules of UIBs need to be updated on the protection of information that is outsourced.

Information that is outsourced presents different risks, and the protective measures can be very different. In many cases, the risks must be addressed through appropriate clauses in the contracts for outsourced services, but there are also components that must be implemented within the UIBs, such as procedures for responding to security breaches that occur in outsourced services or systems.

---

[19] See Open Government – what is the value and what are the barriers and drivers? | FUTURIUM | European Commission (europa.eu)

In the new way of working after the COVID-19 pandemic, external staff (service providers) will increasingly be expected to work remotely instead of being on premises. They will be handling information in environments that the UIBs do not control, potentially in any of the Member States. This presents challenges at many levels, including the legal agreements, supervisory and reporting processes, and working practices.

The rise of the cloud is a key factor to improve categorisation of information. As information is not kept in-house, and as cloud providers should not directly assess the sensitivity of information by looking at the substance of it for confidentiality reasons, it is very important to properly categorize information and ensure that adequate security measures are adduced taking into account the sensitivity of information.

Outsourced systems have many advantages, particularly in terms of flexibility and the reduction of resources needed inside the UIBs and state of the art security. There is an increased reliance on the service providers and a number of new risks appear, such as the administration by external personnel, the risk of legal seizure of information and risks coming from other customers of the same service provider, to name but a few.

Driver 6: Supply chain risks

The Union institutions and bodies rely on many components that are provided by third parties, especially (but not exclusively) in relation to IT equipment. If any such components are compromised before they are delivered to the UIBs, they can present significant threats, such as exfiltration of sensitive information. Such attacks have been observed in recent times (e.g. the SolarWinds compromise[20]).

Fears of supply chain risks have caused many Western countries to delay the introduction of 5G networks, for example, due to concerns over the origins of the network equipment that is used to provide these services. Supply chain risks were one of the topics that were explicitly addressed by President Biden in an executive order in May 2021[21].

An integrated approach to supply chains in the security field will enable the UIBs to use their combined power to improve the reliability of externally supplied components.

2.3. How will the problem evolve?

The already challenging **threat picture of today** is likely to worsen.

The EU has already responded to the impact of the **evolving geopolitical context** on critical infrastructure with a mechanism to assess the desirability of critical processes being controlled by or vulnerable to influence by **third countries[22]**. This will affect

[20] See https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

[21] Executive Order on Improving the Nation's Cybersecurity, May 12, 2021 (see https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/)

[22] Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union

decision-making on the ownership of critical service operators and the relationships they have with other entities. Equally, there is growing concern about the sourcing and vulnerability of critical infrastructure components, a trend that suggests that **supply chain security** will receive additional attention in the years to come, the aim being to ensure that new components or upgrades to existing equipment within critical systems do not introduce additional threats or vulnerabilities[23].

The technologies that are available to perform attacks on information security will increase in sophistication and availability. In particular, the evolution of cloud-based attack services has greatly increased the power and reduced the cost of performing attacks and consumer grade products might not be secure enough for the needs of the UIBs[24]. In the future, the development of practical quantum computing devices could cause a revolution in security, with today's encryption methods potentially becoming obsolete at a stroke.

Finally, in response to current and future challenges, the **regulatory and legislative environment** will continue to evolve. UIBs will continue to respond to these challenges, but without a central direction, the necessary updates to their legislation may occur in an uncoordinated and uneven manner, leading to greater fragmentation and a more uneven playing field.

One question asked by the Commission to the institutions and bodies participating in the survey organised as consultation activity in preparing this legislative activity was on the usefulness of centralising the below security tasks; the table shows the numbers of positive answers out of 32 responses:

Function	Responses
Clearances	22 (69%)
Procurement of physical security material	21 (66%)
Reference security services (e.g. PKI, authentication, digital signature)	27 (84%)
Sweeping[25]	17 (53%)
Accreditation of CIS	22 (69%)
Incident response	21 (66%)
Training and awareness	22 (69%)

[23] The process put in place by the Commission's 2019 Recommendation on the Cybersecurity of 5G networks has led to Member State action on the measures set out in a 5G toolbox, as reflected in the report on the implementation of the Toolbox adopted in July 2020. The Recommendation foresees its review in the last quarter of 2020.

[24] See for example the Pegasus spyware attacks from NSO group which were sold to clients in many countries, able to breach the confidentiality of consumer grade products.

[25] Note that "Sweeping" and "Accreditation of CIS" are only relevant to entities that handle EUCI.

3. WHY SHOULD THE EU ACT?

3.1. Legal basis

Considering the objective and the content of this proposal, its most appropriate legal basis is Article 298 TFEU and Article 106a of the Treaty establishing the European Atomic Energy Community (Euratom).

Article 298 TFEU was introduced by the Lisbon Treaty and has never been used in the EU legislation. It enables the legislator to establish provisions with a view to creating an efficient and independent administration that will support the institutions, bodies, offices and agencies in carrying out their mission.

An efficient and independent administration relies on the security of its information. With a view to achieving their mission, our institutions, bodies, offices and agencies shall benefit from a secure environment for the information they handle daily. A common baseline of standards mandatory for all would enhance the administration's resilience in the face of evolving threats.

Furthermore, with an overall aim to achieve a high common level of security for the EU classified and non-classified information handled by the Union institutions and bodies, this proposal enables the European administration to better protect itself from external interferences and spying activities.

Article 298 TFEU enables the Union to establish a minimum set of information security rules for the whole of the European administration to ensure that all institutions and bodies share the same approach to the security of EU classified information and non-classified information.

According to article 298 TFEU, the European Parliament and the Council shall act by means of a regulation and in accordance with the ordinary legislative procedure.

This proposal needs an additional legal basis as it also covers the information related to some of the Euratom activities. The information involved is not Euratom Classified Information, but it is handled by Union institutions and bodies under the general regime of EU classified information.

This additional legal basis is Article 106a of the Euratom Treaty which renders article 298 TFEU applicable to Euratom activities as well.

3.2. Subsidiarity: necessity of EU action

According to the principle of subsidiarity laid down in Article 5(3) of the Treaty on European Union, action at EU level should be taken only when the aims envisaged cannot be achieved sufficiently by Member States alone and can therefore, by reason of the scale or effects of the proposed action, be better achieved by the EU.

As this proposal is exclusively addressed to the Union institutions and bodies and not to the Member States, the subsidiarity principle does not apply.

4. OBJECTIVES: WHAT IS TO BE ACHIEVED?

4.1. General objective

The general objective of the initiative is to create information security rules for all Union institutions and bodies with the aim to ensuring an enhanced and consistent protection against the evolving threats to their information.

This initiative's aim is to contribute to an efficient and an independent European administration and to prevent major security incidents and leaks.

4.2. Specific objectives

The general objective is translated into four specific objectives, each of them corresponding to one of the problem areas identified in section 2.1 above:

- SO 1: Establish harmonised and comprehensive categories of information, as well as common handling requirements for all information handled by the European administration, and facilitate secure information exchange between the UIBs, while minimising the impact on Member States.
- SO 2: Ensure that all Union institutions and bodies identify any security gaps in their processes and implement the measures required to ensure a level playing field of information security.
- SO 3: Establish a lean cooperation scheme on information security between Union institutions and bodies able to foster a coherent information security culture across UIBs.
- SO 4: Modernise the information security policies at all levels of classification/categorization, for all UIBs, taking into account the digital transformation and the development of teleworking as a structural practice.

4.3. Policy approach and benefits

Policy approach

The Commission proposes to establish common standards of information security for all Union institutions and bodies through a Regulation. The Regulation will enforce the best of breed policies and update the security framework to properly address the current and anticipated threats to information security.

The regulation will not automatically repeal the existing security rules adopted internally by UIBs, although it will override any conflicting rules. It is expected that the existing rules will be reviewed with a view to taking into account this regulation.

Depending on the business environment of each Union institution or body and in accordance with their security needs the impact of the Regulation on UIBs will be different. For some of the smaller bodies the regulation may be sufficient and if existent, their own relevant rules can be revoked. ,. The two sets of rules should be coordinated to minimise any divergence at the more detailed levels. For instance, UIBs with an existing

marking scheme for non-classified information might need to adapt their scheme and ensure some equivalence with the categorisation and marking scheme of this Regulation.

The Regulation is set to become applicable 2 years after its date of publication in the Official Journal of the European Union. This delay is meant to confer UIBs sufficient time for operating the changes required by the new legal framework.

In addition to the policy and regulatory alignment, each Union institution and body should perform a gap analysis to identify any non-compliance of their implemented security measures with the regulation.

To support the implementation of the Regulation by UIBs, the Commission will initiate the work on producing guidance documents within the Inter-Institutional Coordination Group.

Finally, due to the centralisation of some information security tasks UIBs will cooperate in a consistent and formal way and benefit from the knowledge and experience sharing in common bodies.

Effectiveness

While the alignment of all UIBs with the new regulation will take some time to achieve, it is expected to be effective in its main goals of harmonising security rules, improving efficiency and increasing the overall levels of security. It will reduce the current discrepancies and the lack of transparency of the current variety of information security rules of the various Union institutions and bodies.

In particular, the harmonisation of security measures to protect information in communication and information systems (CISs) should help to eliminate potential weak links, which will protect all of the other UIBs and improve the overall effectiveness of their information security programmes.

The new Regulation is drafted in a technology-neutral way due to the constant evolution of the threats against information security.

The effectiveness of the Regulation will be monitored at a high level by the Interinstitutional Information Security Coordination Group, which will be established by the Regulation. The Coordination Group will be able to issue recommendations for improvements where required and follow up their implementation.

Efficiency

The implementation of this Regulation should lead to increased efficiency, particularly regarding:

- Gains from seamless, secure exchange of classified and non-classified information between UIBs.
- Better risk management due to mandatory risk assessments for UIBs' information
- Gains from improved coordination of common tasks, particularly:

  - Clearances
  - Procurement of physical security material
  - Reference security services (e.g. PKI services, authentication, digital signature)
  - Sweeping
  - Accreditation of CISs
  - Training and awareness

- Increased use of common contracts and common outsourcing policies (leading to reduced resource costs in the procurement processes as well as reduced prices)
- Greater use of shared facilities, such as common Secured Areas for protecting classified information
- Sharing of knowledge and experience through the Interinstitutional Information Security Coordination Group and its sub-groups

Any measurable efficiency gains, such as resources saved through coordination, will be reported to the Inter-institutional Information Security Coordination Group.

Coherence

One of the main benefits of this regulation will be an improved coherence of the information security rules and protective measures between the UIBs. This will also have a positive impact on Member States and third parties, which communicate with multiple UIBs, since the rules on handling information will be unified.

The centralisation of tasks and the creation of common bodies will also improve the coherence of the security-related services as well as of the equipment used by the UIBs. This will be a significant factor in enabling, for instance, greater use of shared capabilities.

4.4. Policy Areas

In order to achieve the policy objectives, the proposed Regulation should cover the following areas.

Principles of Information Security

Clear, shared principles must be established as the basis for the common standards of information security. These set up the basic goals that need to be achieved, such as protecting the confidentiality, availability and integrity of information while respecting the general principles of the European Union (transparency, proportionality, efficiency and accountability).

Governance and cooperation

The Regulation provides for common bodies representing the Security Authorities of all Union institutions and bodies and common processes through centralisation of some security tasks. A degree of coordination between the UIBs will be required in order to achieve these benefits.

Non-classified information

Currently, the most significant difference between the UIBs lies in their definition and rules for non-classified information and so the greatest gains can be made by harmonising the rules in this area. Areas where this will bring significant benefits include:

- sharing information transparently between UIBs;
- sharing information with Member States, using equivalent markings;
- facilitating the use of shared CISs with common security requirements;
- greater use of metadata to improve and automate security protection; and

EUCI

The principles for the protection of EUCI are established at the Treaty level and all UIBs that currently handle EUCI have rules in place that are in line with these principles. The benefit of this proposal in the area of EUCI is to provide a single common set of standards for all UIBs in the fields of personnel security, physical security, management of EUCI, Industrial security and EUCI sharing and exchange of classified information.

Organisation and delivery of information security

The delivery of effective security measures in line with this proposal requires autonomous organisation within each of the UIBs. The Regulation should establish the general levels of responsibility for information security in each institution or body and lay out their main tasks.

5. IMPACTS OF THE POLICY

5.1. Economic and resource impacts

Member States

No significant economic impacts are expected at the level of the Member States. The Regulation is only addressed to UIBs and not directly addressed to Member States.

Union institutions and bodies

It is expected that the Union institutions and bodies should achieve some efficiency gains due to the setup of the proposed shared and collaborative subgroups. . Moreover, improvements in information security should help to protect the Union institutions and bodies from potential economic or reputational impacts of security incidents.

There will be effort required to implement the new legislation and organisation but in the long term gains will be obtained through a coherent approach in addressing the evolving threats to information security. It is expected that the costs of adapting to the Regulation can be covered as part of the existing information security improvement programmes in

each UIB. These programs are in any case necessary given the high level of threat that the EU is currently facing.

The Commission will need to set up a permanent secretariat for the Inter-Institutional Information Security Coordination Group. The cost of this secretariat is expected to be one AD official and one AST official. This secretariat should be formally established in the Security Directorate of the Directorate-General for Human Resources and Security.

5.2. Impact on fundamental rights

This proposal ensures full compliance with the fundamental rights as enshrined in the Charter of Fundamental Rights of the European Union, and notably the right to good administration[26].

Moreover, by creating common standards of information security the Commission expects to improve the alignment of the UIBs with the relevant legislative requirements, particularly in relation to data protection. Consequently, there should be a minor improvement in the protection of staff members' rights in those areas.

Transparency and compliance with the good administration principle should increase, as the Regulation is set to be adopted through the co-decision legislative procedure and would largely replace and harmonise a patchwork of internal rules and procedures.

6. MONITORING AND EVALUATION OF IMPACTS

The Commission should monitor the implementation of this proposed Regulation with regard to the achievement of policy objectives identified in this Impact Analysis. A commitment to report to the European Parliament and to the Council every five years on the implementation of this Regulation is included in the draft text.

In addition to this formal report, the Commission should evaluate this Regulation with a view to assessing its actual effects and the need for further action.

SPECIFIC OBJECTIVES	OPERATIONAL OBJECTIVES	INDICATORS
SO 1: Establish harmonised and comprehensive categories of information, as well as common handling requirements for all information handled by the European administration, and facilitate secure information exchange between the UIBs, while minimising the impact on Member States.	Implement the changes in confidentiality levels and markings in all UIBs Providing requirements for the implementation of appropriate communication and information systems to support the secure exchange of information between UIBs	Adoption of suitable guidelines Implementation of new markings Publication of updated handling instructions Implementation of common systems

[26] Article 41 of the Charter of Fundamental Rights of the European Union

SPECIFIC OBJECTIVES	OPERATIONAL OBJECTIVES	INDICATORS
SO 2: Ensure that all UIBs identify any security gaps in their processes and implement the measures required to ensure a level playing field of information security.	Perform gap analysis Produce a Security Improvement Plan Report progress	Number of recommendations made / implemented Number of information leaks across UIBs
SO 3: Establish a lean cooperation scheme on information security between UIBs able to foster a coherent information security culture across UIBs.	Establish coordinated security processes where relevant Establish common training and awareness schemes Review and optimise the use of common security processes	Statistics on centralised versus local procurement Inspection reports Number of queries dealt with by the Secretariat of the Information security coordination group.
SO 4: Modernise the information security policies at all levels of classification/categorization, for all UIBs, taking into account the digital transformation and the development of teleworking as a structural practice	Ensure that UIBs adopt suitable implementing rules, standards and guidelines as necessary Establish guidance on working practices for secure teleworking Establish a user awareness programme	Status updates on the adoption of ancillary implementing rules etc. Statistics on teleworking versus office working Numbers of users undergoing training Level of awareness of staff of each UIB regarding the relevant information security rules Percentage of staff members equipped with secure teleworking equipment, able to handle information up to RESTREINT UE/EU RESTRICTED.

All data collected on the specific indicators will be reported to the Inter-Institutional Information Security Coordination Group.

7. ANNEX 1: PROCEDURAL INFORMATION

Lead DG, DEcide Planning/CWP references

The lead DG is the Directorate-General for Human Resources and Security (DG HR). The agenda planning reference is PLAN/2020/9689.

Organisation and timing

A legislative initiative for a proposal for a Regulation of the European Parliament and of the Council laying down information security rules for all Union institutions and bodies was politically validated by the Presidency on the 3 December 2020.

The Inception Impact Assessment was published on 9 December 2020.

The Inter-service Steering Group (ISSG) was set up by DG HR in agreement with the Secretariat-General to assist in the preparation of the initiative. Representatives of all Directorates General were invited to participate in the ISSG work.

The last meeting of the Inter-Service Steering Group took place on the 15th September 2021.

Consultation of the RSB

This initiative does not follow the strict requirements of the better regulation framework due to its limited impact to the Union institutions and bodies. Therefore DG HR will conduct a limited impact analysis as presented in this document on information security threats to the UIBs and on relevant impacts of the initiative to these entities. It is not necessary to submit this impact analysis to the RSB.

Evidence, sources and quality

As detailed in Annex 2, the impact analysis is based on a number of consultation activities that have taken place in 2021 and that have been carried out by the Commission independently. These consultations have targeted the Union institutions and bodies, the national security authorities in the Member States and research experts (via a study carried out by the Joint Research Centre).

More examples of consultation include the collection of feedback on the Inception Impact Assessment, which sought views from all interested parties via the Commission's 'Have your say' portal, targeted stakeholder consultations with Union institutions and bodies and competent Member State authorities, using a combination of online questionnaires, workshops and bilateral exchanges as appropriate.

Taken together, the consultations activities carried out by the Commission independently have generated a sufficient amount of data for supporting the proposed initiative.

8. ANNEX 2: STAKEHOLDER CONSULTATION

This annex provides a synopsis report of all stakeholder consultation activities undertaken in the context of this Impact Analysis.

Consultation strategy

The Commission has consulted broadly on various aspects related to information security rules of the Union institutions and bodies. The overall aim of the consultation activities was to collect relevant input from different categories of stakeholders to enable the preparation of a legislative initiative on information security in the Union institutions and bodies. The consultations sought to collect inputs on:

- Problems related to the existing framework of information security within the Union institutions and bodies that stakeholders consider should be addressed in the initiative.
- The relevance, effectiveness, efficiency and added value of the initiative.
- The risk assessment of the core information security assets
- The anticipated impacts of the initiative and possible other consequences for the stakeholders.

In preparing the initiative, including the Impact Analysis and draft proposal, Commission services have carried out a mapping of key **stakeholders** with a particular interest in the initiative and /or expertise in the field of information security, which include: (i) Union institutions and bodies; (ii) Member States national security authorities, (iii) research experts.

Over the course of the consultation process, Commission services used the following **methods and forms of consultation**:

- An opportunity for all interested parties to provide feedback on the Inception Impact Assessment via the Commission's 'Have your say' platform;
- A targeted questionnaire addressed to the information security experts within the Union institutions and bodies via online EU survey;
- A targeted questionnaire addressed to the Member States national security authorities via online EU survey;
- A request for a tailored risk assessment of the core information security assets and,
- Numerous meetings and exchanges with counterparts from institutions and bodies, as well as from the Member States national security authorities.

These consultation activities and brief summary of the outcomes are summarised in the next section. It should be noted that due to circumstances related to the COVID-19 pandemic, e.g. travel restrictions, limits on physical meetings, the **format of some of all consultation activities had to be carried out using alternative means to the in-person encounters**, e.g. online surveys, video teleconferencing, phone conversations, written inputs.

All feedback received through the consultation activities organised in the framework of this initiative was processed manually. The assessment of replies involved reading each consultation response in full and documenting viewpoints, including any issues and

concerns that were raised. This feedback was then used as appropriate in conducting the impact analysis.

Given the particularly of this initiative which is exclusively applicable to the Union institutions and bodies, Commission services chose to prioritise the collection of viewpoints from the relevant stakeholder groups. As such, **no public consultation was conducted** specifically for this impact analysis.

Consultation activities and results

Questionnaire to the Union institutions and bodies via online survey

The Commission prepared and conducted a survey addressed to the Union institutions and bodies during a five-week period in February-March 2021. Fifty-six (56) UIBs were invited to participate to the survey, representing most of the institutions[27], agencies[28], other bodies[29] and joint undertakings[30].

The goal of the survey was to generate an overview of the internal policies of UIBs on information security and to identify the gaps in the current processes and the potential tasks that could be centralised.

The questions were organised in two major blocks on non-classified and EU classified information and targeted the following topics:

- Protection of classified information, including in the communication and information systems
- Categories of non-classified information, markings and handling conditions
- Protection of information in outsourced systems
- Exchange of information between UIBs and with third countries and international organisations
- Centralisation of tasks across UIBs

[27] Council of the EU, European Parliament, Court of Justice, Court of Auditors, European Central Bank

[28] ACER, Berec, CdT, Cedefop, Cepol, EACEA, EASA, EASO, EBA, ECDC, ECHA, EDA, EEA, EFCA, EFSA, EIOPA, EMA, EMCDDA, EMSA, Eurofund, EUIPO, EMEA, ENISA, EIGE, ERA, ERCEA, ESA, ETF, Eurojust, Europol, EUSPA, EU-LISA, FRA, Frontex, INEA, REA, OSHA, SRB

[29] EEAS, EDPS, EIB + EIF, COR, CESE

[30] BBI, FCH, ITER/F4E, IMI2

Feedback received

A total of thirty-two (32) UIBs responded to the survey[31] and the main conclusions were as follows:

(i) The fragmentation of the relevant legal frameworks between Union institutions and bodies creates significant duplication of efforts for creating and maintaining internal rules as well as non-interoperable practices in handling classified and non-classified information;

(ii) A better use of resources, capabilities and knowledge is required in the field, through the centralisation of some tasks and the creation of forums for sharing best practices;

(iii) While common standards of information security for all Union institutions and bodies would enhance the resilience of the European administration with respect to the evolving threats, the diversity and the different business environment of each UIB shall be taken into account and local solutions shall be allowed;

(iv) Information security rules need to balance usability and a sound risk assessment; they have to allow Union institutions and bodies achieve their operational objectives while ensuring a high level of security for their information;

(v) All UIBs need to be part of an ecosystem with standardised security rules or implemented best practices, where they can demonstrate compliance and provide trustworthiness between stakeholders.

Questionnaire to Member States via online survey

In parallel with the questionnaire addressed to the Union institutions and bodies, the Commission organised an online survey for the Member States' National Security Authorities. It was conducted over the course of five weeks in February - March 2021. The objective of the survey was to get the views of the national competent authorities on the challenges/deficiencies of the current system of information security at the level of Union institutions and bodies and on the need for common standards.

More specifically, the questions contained in the survey focused on:

- the impacts for the national security authorities of the current situation where each Union institution or body has different information security rules;
- the shortcomings of the current systems used for exchanging EUCI and non-classified information with UIBs; and

[31] ACER, Berec, BBI, Cedefop, Cepol, Council of EU, Court of Justice, Court of Auditors, EASA, EBA, ECB, ECHA, ECDC, EDA, EDPS, EEAS, CESE+COR, EFCA, EFSA, EIB+EIF, EIOPA, EMCDDA, EMSA, ERA, European Parliament, Eurofund, EUIPO, Europol, EUSPA, EU-LISA, F4E, SRB

- the advantages and/or the disadvantages for the national security authorities of creating a common set of rules on Information security, applicable to all Union institutions and bodies.

Feedback received

A total of 9 Member States[32] responded to the questionnaire. The consultation revealed a number of key challenges, namely that:

(i) when sharing EUCI with UIBs, a MS has to comply with different requirements, as provided by each legal framework of the respective institution or body;

(ii) the diversity of the rules of UIBs increase the risks of misunderstanding and misinterpreting as the terminology is not consistent;

(iii) there is no common information system of exchange of EUCI between Member States and UIBs, and

(iv) no secured voice and videoconference tools are available.

Study on a tailored risk assessment of the core information security assets

With a view to use evidence-based scientific data when describing the context of this initiative, the Commission has carried out, through the Joint Research Centre[33] a risk assessment of the main assets of information security. The report of this study is attached in Annex 5.

Consultative meetings with the Union institutions and bodies

The Commission organised several meetings[34] with its counterparts from other UIBs with the aim to discuss the substance of the proposal and its provisions.

The input received during the meetings with UIBs revealed the following important points:

- there is strong support for keeping the four classification levels for EUCI, due to the significant consequences that a suggested change to three levels would involve;

- the majority of UIBs are ready to cooperate with their counterparts in common bodies for information security purposes but not willing to delegate their relevant decision-making powers;

32 CY, CZ, ES, FR, GR, HR, HU, NL, SK

33 The Joint Research Centre is the European Commission's science and knowledge service

34 3 meetings with all participants on 15 April, 2 June and 23rd June, 2 dedicated meetings to the EUCI and 1 dedicated meeting to the non-classified information

- the drafting of the proposal needs to consider the different security maturity levels of UIBs and leave the possibility of adjusting the rules to their specific situation and in line with their own risk assessment;

- the draft shall allow UIBs to keep the categories of non-classified information that they have created for their specific needs;

- the security organisation of each institution and body shall remain under their full responsibility; the denominations of the competent information security departments and relevant functions shall be drafted broadly to permit variations in line with the individual UIBs' needs;

- provisions on handling sensitive non-classified information while teleworking need to consider the EU Delegations and other missions in third countries;

- the provisions on Security of Information Agreements cannot go beyond the scope of article 218 TFEU which regulates the competence and the roles of the relevant institutions and bodies in this matter.

Consultative meetings with Member States

The National Security Authorities of Member States were consulted by the Commission during two ComSEG[35] meetings[36] dedicated to this legislative initiative. During these discussions, the Member States provided several inputs which are summarised below:

- although exclusively applicable to the Union institutions and bodies, the Regulation proposal shall be drafted in respect of the Intergovernmental agreement of the Member States[37] on the protection of classified information in the EU;

- considering the ongoing review of the Council Security Rules, the Regulation proposal shall take into account the provisions already agreed upon during this process;

- several MSs opposed the intention to eliminate the level of CONFIDENTIEL UE/EU CONFIDENTIAL due to the huge impact that such change would entail to the twenty-six (26) relevant national systems having this level as well as to the agreements on the exchange of classified information and the industrial security;

- at the governance level, some Member States proposed to have in the draft an involvement of the national security authorities;

---

35 C(2015)628 Commission Decision on setting up the Commission Security Expert group on the Commission's internal security policy and regulations regarding the protection of EU classified information

36 15 May and 13 July 2021

37 Agreement between the Member States of the European Union, meeting within the Council, regarding the protection of classified information exchanged in the interests of the European Union, 2011/C 202/05

- the categories of non-classified information have no legal status and no legislative protection in the Member States, which entails no directly applicable legal guarantees for its protection outside UIBs.

Inception impact assessment

The Inception Impact Assessment was published for feedback by all interested parties on the Commission's 'Have your say' portal. Respondents were invited to provide online comments and views on the initiative for a period of four weeks, starting on 9 December 2020.

Feedback received

A total of seven contributions were submitted over the feedback period out of which two were not relevant to the subject. Of the remaining five replies, there were three provided by Union institutions and bodies, one by a National Authority of a Member State and one anonymous.

Overall, these contributions welcomed the initiative for a common legal framework for all institutions and bodies with a view to ensuring the same level of protection for the information handled by UIBs. At the same time, the contributions underlined the need to consider the diversity of UIBs, their specific business environment and security needs.

One representative from an agency expressed specific suggestions in the area of communication and information systems, related to the need to set out in the Regulation clear technical rules for the interconnection between UIBs. Other ideas referred to the possible financial implications triggered by the implementation of this Regulation.

Stakeholder participation

Stakeholders consulted included:

- Union institutions and bodies;
- National security authorities in the Member States;
- Research experts from JRC.

9. ANNEX 3: WHO IS AFFECTED AND HOW?

Practical implications of the initiative

The initiative will have a direct impact on the Union institutions and bodies and the way they govern information. It also has an impact on Member States administrations, private sector and third states as far as sharing and exchange of information is concerned and in the framework of industrial security.

The initiative ensures that our institutions and bodies progress towards more secure open and efficient administration procedures.

The main impact is that UIBs will have to categorise information according to the scheme defined in the Regulation and protect it accordingly.

Union institutions and bodies

- Categorise information in line with the scheme promoted in the Regulation, when the information is exchanged between UIBs or when it is classified. Handle information in compliance with the Regulation.

- Participate in the Inter-institutional information security Coordination Group.

- Update their internal rules of procedures to comply with the Regulation. In particular, establish equivalence tables in case they already have an internal categorisation scheme for their information.

- Adjust their outsourcing policies to ensure that they meet the requirements of the Regulation.

- Ensure that their CISs are compliant with the Regulation, formally categorize their CIS taking into account the maximum level of information that can be handled into it.

- Monitor and report to their respective security authority any information leak.

Member States

- The Commission proposal is not directly adressed to the Member States, which are exclusively competent for their national security policies.

- As far as classified information is concerned, the Regulation is fully compliant with the intergovernmental agreement[38] of 2011 on the protection of classified information in the EU.

- The protection afforded by the Member States to the classified information subject of the Agreement remains equivalent to the standards provided by the Council Security rules. As far as non-classified information is concerned, the Regulation does not create new obligations on the Member States. When information will be exchanged between the Member States and UIBs, they will be informed about the handling rules for such information (either through metadata or visual markings). This is already a common practice, and the Regulation will clarify the markings and metadata tagging of information, which are now very diverse as each UIB has its own scheme.

- The proposal should increase the use of nationally approved crypto products for the handling of classified information,

[38] Idem 35

Private Sector

- The Commission proposal has no practical impact on the private sector. The Regulation maintains the current rules for classified grants and contract, and thus will have no or minimal impact on private sector.

- The Regulation introduces some information localisation rules that should benefit EU-based outsourcing providers, as it makes it mandatory to host sensitive and classified information on the EU territory.

European Commission

- The European Commission will set up a permanent secretariat for the Inter-institutional Information Security Coordination Group.

- The European Commission will provide security services to UIBs under SLAs. Some services are already provided to other UIBs but their scope will increase under the proposed Regulation.

10. ANNEX 4: ASSESSMENT 'SENSITIVE NON-CLASSIFIED' INFORMATION CATEGORY / SCOPE OF THE REGULATION

This section includes a summary of the most relevant rules and obligations related to each category of information covered by the proposed Regulation.

Summary table, handling instructions for each category of information

	PU	EU-N	SNC	R-UE/ EU-R	C-UE /EU-C	S-UE/ EU-S	TS-UE/ EU-TS
Staff obligations							
Can be handled in public spaces	Y	N	N	N	N	N	N
Can be handled outside the office in a private location	Y	Y	Y	Y*	N	N	N
Needs to be handled in a registry	N	N	N	N	Y	Y	Y*
Can be handled on a private computer	Y	Y	N	N	N	N	N
Can be handled on a standard corporate computer	Y	Y	Y*	N	N	N	N
Requires a security clearance	N	N	N	N	Y	Y	Y*

Specific rules on printing and destruction	N	N	Y	Y	Y	Y	Y
Access granted on an individual basis	N	N	N	Y*	Y*	Y*	Y*
Formal registration of documents and copies	N	N	N	N	Y	Y	Y*
Need to know	N	N	Y	Y	Y	Y	Y
Marking of documents	N	N	Y	Y	Y	Y	Y
System owner obligations							
Cyber security plan [39]	Y	Y	Y	Y	Y	Y	Y
Measures to protect secrecy	N	Y	Y	Y	Y	Y	Y
Control over encryption	N	N	Y	Y	Y	Y	Y
Zero trust	N	N	Y	Y	Y	Y	Y
Formal Accreditation	N	N	N	Y	Y	Y	Y
Air gapped	N	N	N	Y/N	Y	Y	Y
Outsourcing (cloud/operations)	Y	Y	Y*	N	N	N	N
Cleared operations staff	N	N	N	Y	Y	Y	Y

Y: yes, Y*: yes with restriction, N: no

11. ANNEX 5: A LANDSCAPE ANALYSIS ON THE INFORMATION SECURITY IN THE AGE OF EU INSTITUTIONS DIGITALISATION (ATTACHED)

A quick contemplation on the emergence of new tasks for the Union institutions and bodies, the many-to-many fashioned synergies developed among these entities, alongside the ever-changing and complex digital landscape, is more than enough to demonstrate the necessity for creating and ratifying a contemporary common baseline for information security across UIBs. For instance, new missions assigned to the Union institutions and bodies will eventually create greater demands for handling and exchanging large volumes of information and data for which it is possible that no classification has been set and no rules on how to exchange and store them exist. Altogether, these developments affect all the involved parties, and immensely render the need for the establishment of a unified and harmonised information security framework more imperative than ever.

[39] Article 7 of the proposal for a Regulation […] of the European Parliament and of the Council laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union.

Moreover, at least in the mid-term, the fruits of this endeavour are expected to also diminish the overall attack surface, as everyone will follow the same rules, and personnel training can be coordinated and harmonised, let alone the reduced associated resources and management costs.

The report offers a fresh and detailed perspective on the aforementioned challenges, but interestingly from an information risk assessment viewpoint. Specifically, the focus is on any piece of information, both classified and non-classified, including that stored or managed by third-party providers on behalf of UIBs and it is extended to digital archives and across the whole information lifecycle.

The report aspires to not only serve as a means to stimulate and facilitate the needy process towards a new UIBs policy addressing common rules on Information security, but also as a reference to anyone interested in better understanding the diverse facets of this fast evolving and thought-provoking ecosystem[40].

[40] KAMBOURAKIS, NEISSE, NAI-FOVINO, *Information security in the age of EU-Institutions digitalisation, a landscape analysis*, European Commission, Joint Research Centre, 2021, JRC125214.