Council of the European Union
General Secretariat

PUBLIC

Interinstitutional files:
2026/0011 (COD)

Brussels, 11 September 2026

WK 13875/2026 INIT

LIMITE

CYBER
JAI
DATAPROTECT
TELECOM
MI
IND
CADREFIN
FIN
BUDGET
CSC
CODEC

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 Horizontal Working Party on Cyber Issues
N° Cion doc.:	ST 5611 2026 ADD 1 + ST 5611 2026 ADD 2 + ST 5611 2026 ADD 3 + ST 5611 2026 ADD 4 + ST 5611 2026 INIT
Subject:	Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Cybersecurity (ENISA), the European cybersecurity certification framework, and ICT supply chain security and repealing Regulation (EU) 2019/881 (The Cybersecurity Act 2) – Cyber posture - Presentation by France

Delegations will find in the annex a presentation given by France at the meeting of the Horizontal Working Party on Cyber Isssues on 10 September 2026.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

PUBLIC

NIS 2

HWPCI GROUP ON CYBERPOSTURE

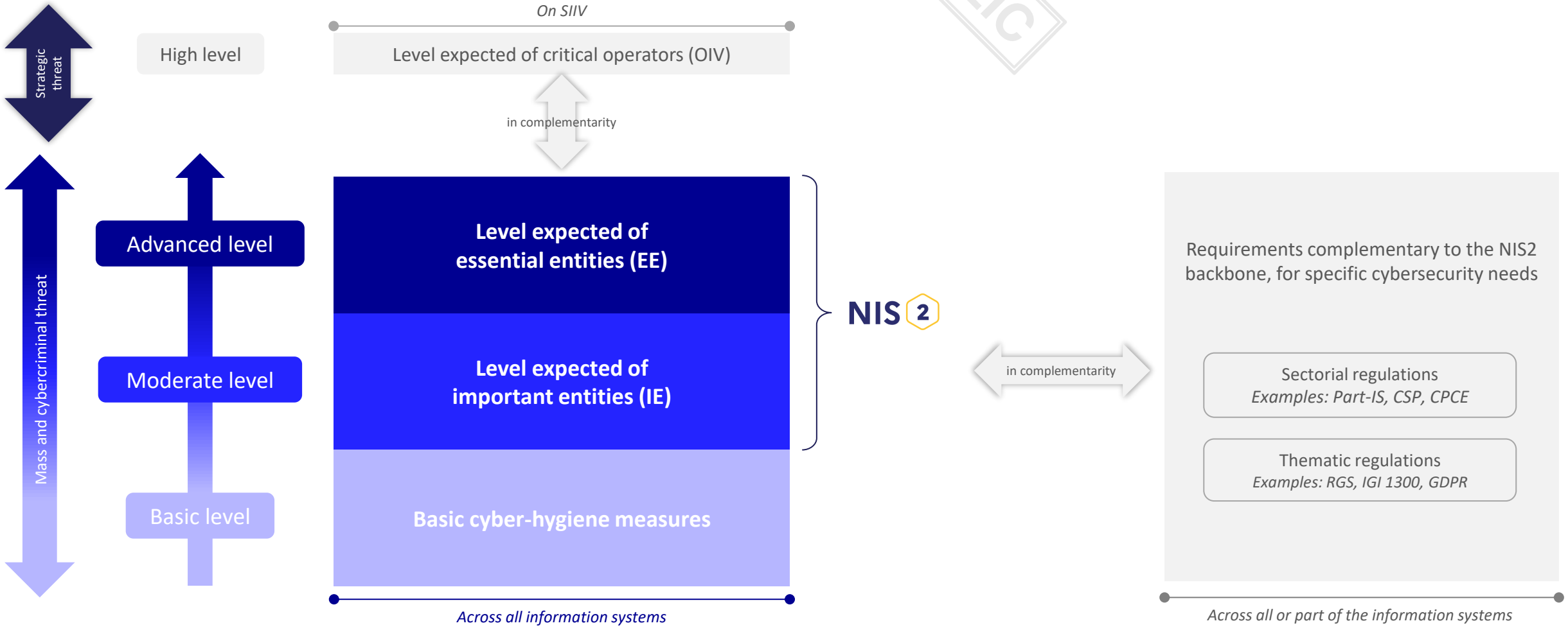
PRESENTATION OF FRANCE'S CYBERPOSTURE ENVISAGED SCHEME FOR NIS 2

10/09/2026

NIS2: backbone of our French cyber regulatory framework

PUBLIC

▶ Three levels of security measures acting as the bedrock of all cybersecurity regulations



Implementing risk-management measures

PUBLIC

European level

Member states responsible for ensuring that appropriate and proportionate measures are being implemented by entities to manage the risks threatening the security of their networks and information systems

Legislative level

Operational and organisational technical measures provided for by the NIS2 directive

- Governance
- Protection
- Defence
- Resilience

Adapted in accordance with the principle of proportionality between essential and important entities

Regulatory level

Proportionality

To defend against the mass cybercriminal threat:

- 20 security objectives for essential entities
- 15 security objectives for important entities, corresponding to cyber-hygiene measures

Sustainability

- For important entities, security objectives are defined by ANSSI based on its expertise and knowledge of cyber threats; requiring therefore a compliance approach by these entities

Detailed in the NIS 2 rule framework

Recommendations level

- Framework of measures which entities **may implement** in order to **achieve their security objectives**
- Framework which provides entities with flexibility with regards to all or part of their requirements, depending on their specificities
- Should these measures be implemented, possibility of **invoking them in the event of a control**

Toward streamlined pathways to meet NIS2 security objectives

PUBLIC

ANSSI's framework of suggested measures

Essential and important entities

- Development of a framework of measures which entities **may implement** in order to **achieve their security objectives**:
  - **Objective:** Through a non-binding framework, provide entities with flexibility with regards to all or part of their requirement
  - **Effect:** Should these measures be implemented, possibility of **invoking them in the event of a control**
- Option to implement any other standard recognized as equivalent by ANSSI and to cite it in the event of a control

Cyber-posture certification

Designed for important entities

- An incentive-based, non-mandatory certification, aligned with the compliance approach:
  - Give regulated entities the opportunity to benefit from a presumption of conformity with NIS2
  - Foster the development of a NIS2-compliant offering for smaller regulated entities
- Beyond NIS2:
  - **Ability to demonstrate to its ecosystem (insurer, bank, customers, etc.) the security measures an entity has implemented and the level of cybersecurity it has achieved**
  - Incentive scheme for improving cybersecurity maturity

Trusted security services

Designed for essentiel entities

- **Trusted security services** : high-value, trusted cybersecurity and cyberdefense services qualified by ANSSI. Examples :
  - Qualified support and consulting services for information system security (PACS)
  - Qualified information system security audit services (PASSI)
  - Qualified incident detection services (PDIS)
- **The use of a trusted security service qualified by ANSSI allows regulated entities to demonstrate their compliance with one or more requirements of ANSSI's cybersecurity framework**, as specified by that framework

A need to deepen our discussions around key principles

PUBLIC

The need to agree on common general objectives

- Provide legal certainty to organizations by giving them the ability to benefit from a presumption of conformity
- Use certification as a proof for organizations to demonstrate the level of security they have achieved (supply chain security)
- Start a virtuous cycle to boost cybersecurity by turning certification into a competitive advantage

Learn from established national cyberposture certification frameworks

- Strengthen the Member States' role in the establishment of cyberposture certification scheme
- Build on mutual recognition initiatives launched by Member States in relation to their national qualifications frameworks and to relevant international or sectoral standards

Build a future-proof cyberposture certification framework

- In principle, keep cyber posture certification voluntary and non-mandatory to take better into account the specific characteristics of the respective economic contexts of each Member State;
- Keep the framework flexible enough to address the specific characteristics of each organization, its maturity, its level of risk, etc.

➢ **Alignment with these structural principles as an opportunity to initiate technical discussions on the practical implementation of this mechanism at EU level**