1783 INSIGHTS

Long View

**INFORMAL STRATEGIC NOTE**
**January 2026**

**ENISA - CISA : Two architectures stemming from two different political organizations**
***Distinct methods, common objective, shared values*** *(Analysis based on Commission text IP/26/105)*

*For decision-makers and 1783 strategic community - non-paper*

## Purpose of this note

This note aims to clarify the differences between ENISA and CISA, not as competing models or a power struggle, but as the logical expression of different political and institutional frameworks organizing public action in distinct ways.

The observed divergences in methods, standards, and tools do not stem from conflicting values or fundamental strategic disagreement.

They are the product of different political structures, nevertheless pursuing a strictly common objective: strengthening the resilience of open societies, securing critical infrastructure, and preserving trust in the digital space.

### 1. Methodological clarification (essential)

The ENISA/CISA comparison is frequently biased by a flawed assumption: that CISA is a central cyber authority with enforcement powers, whereas the European Union has chosen a regulatory approach.
This reading is inaccurate.

CISA has no direct regulatory or enforcement authority in cybersecurity matters. In the United States, cyber competence falls under:

- State governments
- Sectoral regulators
- Contractual, insurance, and liability mechanisms
- Primarily incentive-based federal frameworks.

### 2. What the IP/26/105 text seeks to achieve with ENISA

The IP/26/105 text responds to a structural constraint specific to the European Union: making ***27 sovereign national security strategies*** work together, without centralizing or erasing them. In this regard, the text:

- Strengthens ENISA as a central building block of European coherence,
- Explicitly embeds it in the implementation of existing binding frameworks (NIS2, Cybersecurity Act, certification schemes),
- Confirms its role as a methodological, analytical, and preparatory hub designed to facilitate collective action.

The text does not seek to create a European operational authority. It aims to reduce friction, increase clarity, and enable more consistent implementation of already-decided policies.

### 3. Comparative table – ENISA vs CISA (institutional reality)

| Dimension | ENISA (European Union) | CISA (United States) |
|---|---|---|
| Political order | Composite supranational union of sovereign states | Federal nation-state |
| Institutional nature | EU agency with coordination and advisory mandate | Federal operational agency under DHS |
| Primary function | Harmonisation, coordination, capacity-building | Operational orchestration and execution |
| Source of authority | EU regulations and mandates agreed by Member States | Presidential authority and federal law |
| Operational command | No direct command authority over Member States | Direct federal-level operational coordination |
| Relation to national authorities | Facilitator between national cybersecurity authorities | Integrator of federal agencies |
| Role of private sector | Stakeholder to align and coordinate | Operational partner and capacity multiplier |
| Normative vs operational bias | Primarily normative and framework-oriented | Primarily operational and action-oriented |
| Crisis management role | Support, coordination, information sharing | Lead coordination and incident response |
| Strategic logic | Trust through harmonisation and common standards | Trust through execution and demonstrated capability |
| Structural constraint | Subsidiarity and political heterogeneity | Centralised executive authority |

### 4. Two methods stemming from two political organizations

*4.1. The American approach*

The American model is structured by strong constitutional federalism. Cybersecurity is organized through operational capability, coordination, legal liability, and market discipline. CISA acts as a horizontal orchestrator, facilitating alignment of public and private actors without direct legal constraint. System coherence relies primarily on technical capability, operational credibility, and the cost of failure.

*4.2. The European approach*

The European Union rests on a specific political reality: a plurality of sovereign states, each with its own national security strategy. Historically and politically, the method for organizing this diversity is well-established the internal market, law, and standards. Through these instruments, the Union achieves:

- Convergence without centralization,
- Cooperation without denying sovereignty,
- Reduced friction between heterogeneous systems,
- Enabling collective action.

In this framework, ENISA is designed as a facilitation tool, serving coherence and collective preparedness. By structuring common standards, methodologies, and shared reference frameworks, it creates conditions of interoperability and trust that make collective capability both possible and durable.

Standards are not an alternative to capability. They constitute its prerequisite.

**5. Effectiveness and acknowledged limitations of the European method**

The European method is functional and consistent with the Union's political architecture. It enables convergence, clarity, and collective legitimacy. However, it is not sufficient on its own. Without credible operational capabilities, regular cross-border exercises, clearly established decision chains in crisis situations, normative convergence risks not fully translating into collective action capacity.

**The IP/26/105 text creates the conditions of possibility for capability building.** It does not prejudge the political choices necessary to make it effective.

**6. A shared values framework**

Despite different methods, the European and American approaches rest on a common values foundation:

- · Protection of open societies and the rule of law,
- · Central role of the private sector in resilience,
- · Importance of international cooperation,
- · Trust conceived as strategic infrastructure.

Observed divergences concern instruments and modes of action, not objectives.

**7. Conclusion**

The IP/26/105 text constitutes institutional engineering work, aimed at streamlining European action based on the Union's political reality. By strengthening ENISA as a methodological and preparatory hub, it seeks to enable better articulation of national strategies, without artificial centralization and without challenging state sovereignty.

The methodological differences observed between Europe and the United States are not power conflicts, but the direct consequence of distinct political frameworks nevertheless pursuing the same strategic objective. The European method is functional. It has enabled normative convergence. The transition to enhanced collective capability now depends on political choices to be made while respecting national sovereignty.

***Open question (to inform discussion)***
What concrete mechanisms could strengthen European collective capability through coordination, interoperability, and shared preparedness, while respecting the institutional and political balance of the Union? In particular, how can voluntary cooperation frameworks, joint exercises, operational interoperability, and public-private articulation enhance collective effectiveness without creating artificial centralization?

*Note on terminology and context. This analysis uses "ENISA" & "CISA" as institutional shorthand for broader systems. In practice:*

- *ENISA operates within a multi-layered European cybersecurity ecosystem including national CERTs/CSIRTs, sectoral regulators, the NIS Cooperation Group.*
- *CISA coordinates with state-level agencies, sector-specific ISACs, and federal partners including NSA, FBI, and others.*
- *Both agencies function as coordination nodes rather than command authorities, though the legal and political frameworks structuring their coordination differ fundamentally.*