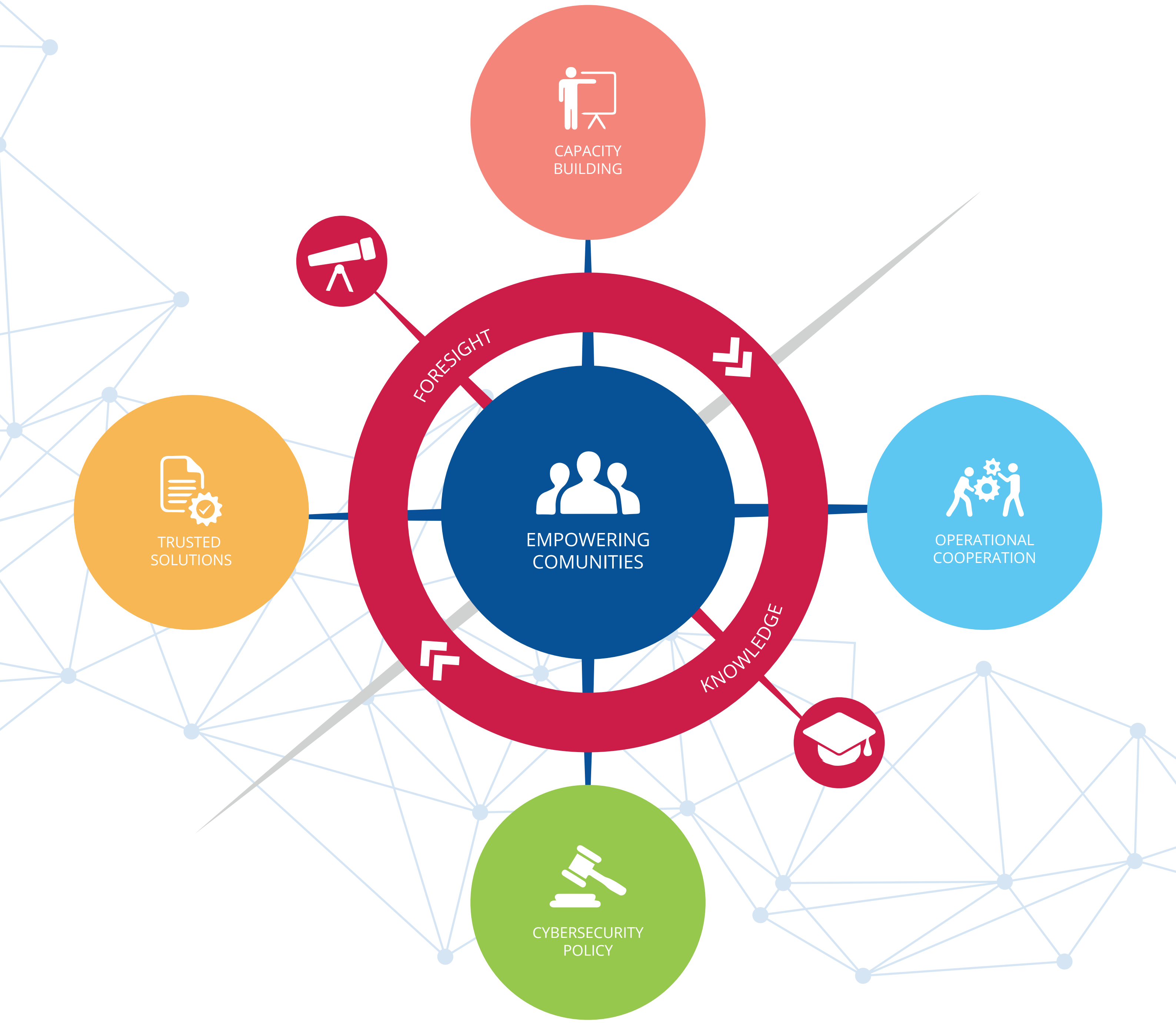
EUROPEAN UNION AGENCY
FOR CYBERSECURITY

2026–2028 ENISA Stakeholder Strategy

JANUARY 2026


CAPACITY BUILDING
FORESIGHT
TRUSTED SOLUTIONS
EMPOWERING COMUNITIES
OPERATIONAL COOPERATION
KNOWLEDGE
CYBERSECURITY POLICY

Introduction

The European Union Agency for Cybersecurity's (ENISA or 'the Agency') mandated responsibilities with regards to stakeholders are focused on gaining input and coordination from, and/or providing information, support or guidance to, stakeholders in order to ensure the effective implementation of Regulation (EU) 2019/881 (the Cybersecurity Act).

- Article 3(1) of the Cybersecurity Act states that 'ENISA shall carry out the tasks assigned to it under this Regulation for the purpose of achieving a high common level of cybersecurity across the European Union (EU), including by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity. ENISA shall act as a reference point for advice and expertise on cybersecurity for **Union institutions, bodies, offices and agencies** as well as for other **relevant Union stakeholders**';
- Article 4(4) on 'Objectives' states that 'ENISA shall promote cooperation, including information sharing and coordination at Union level, among **Member States, Union institutions, bodies, offices and agencies**, and relevant **private and public stakeholders** on matters related to cybersecurity';
- Article 10(a) mandates the Agency to 'raise public awareness of cybersecurity risks, and provide guidance on good practices for individual users aimed at **citizens, organisations** and **businesses**, including cyber-hygiene and cyber-literacy';
- Article 20(l) on 'Duties of the Executive Director' states that the Executive Director shall be responsible for 'developing and maintaining contact with the **business community and consumers' organisations** to ensure regular dialogue with **relevant stakeholders**';
- Chapter 2 (Articles 5 to 12) specifies the tasks of the Cybersecurity Act and emphasises the need to support, assist and cooperate with **relevant stakeholders**.

Since the previous stakeholder strategy (adopted by the Management Board in 2021), the Agency has been entrusted with more statutory tasks via new EU legislation (notably the Network and Information Systems Directive 2, the Cyber Resilience Act, the Cyber Solidarity Act, the Digital Operational Resilience Act) and has been confronted with increased stakeholder interest. The Management Board of the Agency has also reviewed the ENISA Strategy in 2024, which gives the Agency a new focus and objectives in areas requiring a better understanding of its stakeholders and outreach, and aligns with the Agency's strategic objective of 'empowered communities in an involved and engaged cyber ecosystem'.

Objectives

The goals of the 2026–2028 ENISA stakeholder strategy (ESS) are as follows.

1. Define and specify relevant stakeholder groups for ENISA and ensure that all ENISA engagement with stakeholders is value-driven, i.e. it is aligned with and derived from specific needs as set in the Agency's strategic objectives and priorities and statutory tasks. The ESS itself does not define ENISA's objectives or deliverables.
2. Set Agency-wide principles for engagement with its stakeholders through a framework that is in line with the Agency's values and operating principles as defined here and in other ENISA documents ([1]). It also specifies under which conditions ENISA should conduct its outreach proactively and when it should refrain from doing so.
3. Set the governance framework for stakeholder management and outreach, helping the Agency, its managers and its staff to manage their stakeholder relations effectively and efficiently. The ESS aims to ensure that stakeholder management is internally coordinated and avoids overwhelming stakeholders (duplication of outreach towards certain types of stakeholders) and stakeholder fatigue.

Guiding Principles

i. In line with Union law and ENISA's values and operating principles, the Agency shall engage with its stakeholders in a transparent, coordinated, open and non-discriminatory fashion, respecting the principles as imposed by its International Strategy when engaging with non-EU stakeholders. The Agency and its staff shall engage with stakeholders with integrity and respect in line with good administrative behaviour and the ENISA code of conduct. This includes respectful communication between the Agency and its stakeholders, whereby requests are replied to by the Agency within an acceptable timeframe.

ii. In general, the Agency collaborates and engages with stakeholders through statutory stakeholder cooperation mechanisms, such as its own Advisory Group, ENISA ad hoc expert groups, formal public consultations or cooperation fora established under Union law by the Member States or Union entities – such as the competency communities established by the NCC network. Exceptions and deviations from this general principle are set out in this strategy.

iii. The Agency will seek guidance from and give regular updates to its Management Board when implementing this strategy, notably through regular updates to the Executive Board and summaries of main activities related to stakeholder engagement and outreach within its annual activity reports.

(1) Such as ENISA's International Strategy and the ENISA code of conduct.

Stakeholder Management and Outreach Framework

In order to implement its strategy and accomplish its statutory tasks, the Agency needs to engage with six main stakeholder groups, as already identified in the first ENISA stakeholder strategy:

1. Member States' national authorities entrusted to implement EU cybersecurity policies and legislation;
2. EU institutions, bodies or agencies (EUIBAs) dealing with cybersecurity policy development and implementation at the EU level;
3. Cybersecurity industry and private sector actors (including non-EU actors) who need to fulfil the requirements stemming from EU law and who sustain and develop the EU cybersecurity ecosystem;
4. Third country cybersecurity authorities (or international organisations)
5. Cybersecurity-related academic institutions and research and education organisations;
6. Civil society and the general public.

The Agency's level of engagement with those stakeholders varies depending on the Agency's needs. The ENISA stakeholder strategy outlines four levels of ENISA's interactions with stakeholders, depending on the degree of interest and influence: (1) partner(ship), (2) engage(ment), (3) consult(ation) and (4) inform(ation). The Table below maps and gives an indicative overview of the Agency's engagement level across the six stakeholder groups in relation to ENISA's seven strategic objectives.

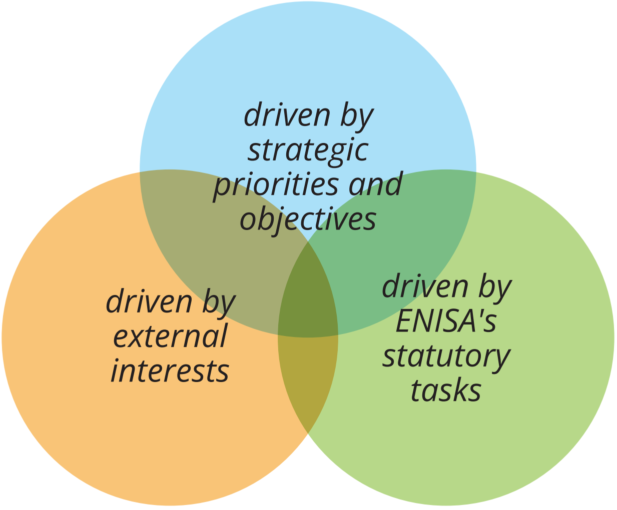
Strategic objective (ENISA Strategy)	Six main stakeholder groups					
	1	2	3	4	5	6
Effective and consistent implementation of EU cybersecurity policies	partner engage	partner engage	consult	inform	inform	inform
Effective Union preparedness and response to cyber incidents, cyber threats, and cyber crises	partner engage	partner engage	consult partner	inform	inform	inform
Strong cybersecurity capacity within EU	partner engage	partner engage	consult partner	inform	consult inform	inform
Building trust in secure digital solutions	partner engage	partner engage	consult	consult inform	inform	inform
Empowered communities in an involved and engaged cyber ecosystem	partner engage	partner engage	consult	consult inform	inform	inform
Foresight on emerging and future cybersecurity opportunities and challenges	partner engage	partner engage	consult	consult inform	consult inform	inform
Consolidated and shared cybersecurity information and knowledge support for Europe	partner engage	partner engage	consult partner	consult inform	inform	inform

The level of engagement with Member States and EU institutions, bodies or agencies – indeed the partnership – that the Agency needs to effectively fulfil its statutory tasks and strategic objectives is ingrained into ENISA's mandate, governance and operations. As such, there is not much need for the ESS to specify or direct the Agency's interactions with the first two stakeholder groups beyond the reiteration that the general principles of ESS apply and that the Agency shall interact closely, systematically and regularly with those two stakeholder groups across all of its operations.

The Agency's interactions with non-EU countries and international organisations are governed under its international cooperation strategy, to which the ESS shall adhere. The required interaction with the fifth stakeholder group is less close, and in the case of the sixth stakeholder group the Agency takes a secondary and supportive role to the Member States' authorities and the European Commission.

That leaves the third stakeholder group – cybersecurity industry and other private sector actors. The 'standard' engagement level with this stakeholder group is 'consult'. This means that stakeholders in this category may be impacted by ENISA's activities but have little influence over them. They may want more of ENISA's time than can be given, and interaction with them should always be done in a manner that avoids potential conflicts of interests.

However, with new tasks and objectives, there are areas of ENISA's work that now demands setting up different partnerships with private sector actors – such as within the operationalisation of the EU Cybersecurity Reserve (contractual relationships) or uptake and implementation of the skills framework – European Cybersecurity Skills Framework (alliances and advocacy). The ESS should thus establish efficient ways to engage with private sector actors.


driven by strategic priorities and objectives
driven by external interests
driven by ENISA's statutory tasks

ENISA's interaction with this stakeholder group can be placed under three categories. Engagement might be proactive (initiated by ENISA) due to the needs stemming from: (1) ENISA's strategic objectives and priorities and/or (2) its statutory tasks; it might also be a reactive response to (3) external initiative, when this aligns with (1) and/or (2), as engaging only on the basis of external interest would not be aligned with the objectives of the ESS (value-driven) or with its principles (non-discrimination).

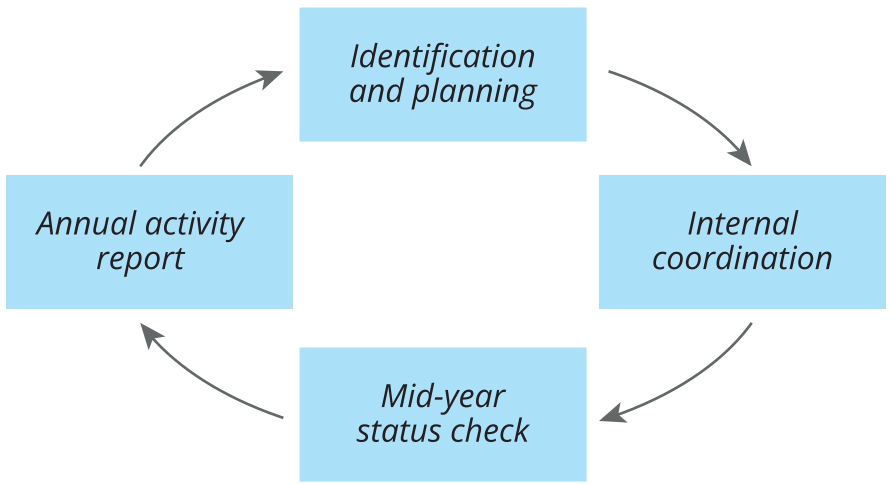
Thus, the following sections shall set out and explain ENISA's engagement with private sector actors (in addition to its (lower) engagement with the fifth stakeholder group: academia and research and education).

PRIORITY-DRIVEN (STRATEGIC-OBJECTIVE-DRIVEN)

Priority-driven stakeholder engagement is **forward-looking and proactive**: the Agency initiates cooperation or engagement that supports delivering the ENISA Strategy objectives, including as defined in the annual programming document priorities and as tracked and measured by the relevant strategic KPIs.

When ENISA's strategic objectives or its priorities as defined in its Single Programming Document require the Agency to engage with a specific stakeholder or community but there is no statutory mechanism in place to do so, the Agency can **proactively establish a stakeholder** relationship as required.

In order to manage the Agency's priority-driven stakeholder engagement, the Agency maintains a **strategic stakeholder mapping**, which shall be reviewed annually and used to coordinate the Agency's engagements with its strategic stakeholders and support reporting to the Management Board (and subsequently inform the National Liaison Officers, upon request of the Management Board). This is an internal exercise to map the Agency's engagement with cybersecurity industry and other private sector actors and with academia, research and education. ENISA's strategic stakeholder mapping supports prioritisation, alignment and coordination. It also enables the Agency to report to the Management Board and involve the National Liaison Officers. This helps avoid duplication and supports coherence within the Agency and with our key partners: EU Member States and EU institutions, bodies and agencies.



STATUTORY-TASK-DRIVEN

In order to maintain the ability and capacity to implement the more than 240 statutory tasks across EU legislation [2] beyond those tasks related to implementing ENISA's strategic objectives and its SPD, ENISA shall develop and sustain the engagement with the stakeholders relevant to the tasks in question, in line with the principles enshrined above.

[2] Cybersecurity Act; Regulation (EU) 2024/2847 (Cyber Resilience Act); Directive (EU) 2022/2555 (Network and Information Systems Directive 2); Critical Entities Resilience Directive (Directive (EU) 2022/2557); Regulation (EU) 2024/1689 (Artificial Intelligence Act); Regulation (EU) 2025/38 (Cyber Solidarity Act); Regulation (EU) 2022/2554 (Digital Europe Programme Regulation); Regulation (EU) 2022/868 (Data Governance Act); Regulation (EU) 2022/2554 (Digital Operational Resilience Act); Regulation (EU) 2021/887 (European Cybersecurity Competence Centre Regulation); Regulation (EU) 2025/327 (European Health Data Space Regulation); Regulation (EU) 2024/1183 (Electronic Identification, Authentication, and Trust Services Regulation);

To ensure coordinated stakeholder engagement for the Agency's statutory tasks, the Agency maintains **a mapping of key private and non-profit sector stakeholders** – beyond those already covered in its strategic stakeholder mapping and those belonging to the first two stakeholder groups (EU Member States and EU institutions, bodies and agencies). This includes press contacts. These stakeholders must align with ENISA's values, objectives and principles as outlined in this strategy. This list shall be reviewed annually and used to coordinate internally and, upon request of the Management Board, be used to inform the Management Board (and subsequently the NLOs).

The Agency shall not regularly engage with stakeholders (entities, associations, etc.) who have not been enlisted in the map.

EXTERNAL-INTEREST-DRIVEN

Due to resource constraints and other factors, the Agency cannot always respond promptly and accept requests from external stakeholders to engage. Thus, it shall take **a restrictive approach towards engagements driven by external interest groups** ([3]), prioritising and accepting only requests from stakeholders that:

- belong to similar stakeholder category as defined in its priority-driven and/or statutory-task-driven stakeholder mappings;
- are necessary for the implementation of its priorities or for ensuring that it is able to undertake statutory tasks in the short-to-medium term;
- do not contradict or undermine ENISA's values and engagement principles as defined in this strategy or in ENISA's International Strategy.

ENISA's public events shall pre-register participants, and ENISA reserves the right to refuse participation of representatives from entities whose engagement would not align with the abovementioned requirements.

In exceptional circumstances, the Agency engages to ensure compliance with mandatory obligations, legal frameworks, or upon direct request from the ENISA Management Board or from the European Commission in relation to Union interests and/or EU policy goals.

In maintaining its operational autonomy and independence within its cybersecurity stakeholder communities, the Agency will not engage stakeholders in order to endorse, co-sign or in any other way sanction and attach its name to any documents or publications that have been prepared by an external party, unless the co-creation of such documents with ENISA is foreseen in the Agency's mandate, its annual work programme or in a specific cooperation plan with an external entity ([4]).

GOVERNANCE

The Executive Director imposes measures and nominates the roles and responsibilities necessary for the implementation of this strategy. The Executive Director also prepares a review of the strategy whenever the Management Board reviews ENISA's Strategy or, at the latest, by the end of 2028.

(3) These types of requests might include, but are not necessarily limited to, requests for bilateral meetings, visits, missions, conferences, seminars and unprompted approaches towards Agency staff during or surrounding any public events.

(4) The Agency will operate in line with the principles set out in the ENISA International strategy.

ABOUT ENISA

The European Union Agency for Cybersecurity (ENISA) has been working to make Europe cyber secure since 2004. ENISA works with the EU, its member states, the private sector and Europe's citizens to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. Since 2019, it has been drawing up cybersecurity certification schemes. More information about ENISA and its work can be found at www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14
Chalandri 15231, Attiki, Greece

Brussels Office
Rue de la Loi 107
1049 Brussels, Belgium

enisa.europa.eu

Publications Office
of the European Union