European Union Agency
for Cybersecurity

Agamemnonos 14
Chalandri 15231 | Attiki | Greece
Tel: +30 28 14 40 9711
E-mail: info@enisa.europa.eu
www.enisa.europa.eu

MANAGEMENT BOARD DECISION

DECISION No MB/2025/19

OF THE ENISA MANAGEMENT BOARD

of date, 20 November 2025

on adopting the ENISA Stakeholder Strategy 2026-2028

THE MANAGEMENT BOARD OF THE EUROPEAN UNION AGENCY FOR CYBERSECURITY

Having regard to

- Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), in particular Articles 5-12,
- ENISA Management Board Decision No MB/2024/14 of 14 November 2024 on the general direction of the operation of ENISA (ENISA Strategy)

Whereas

(1) The tasks of ENISA are laid down in Articles 5-12 of the Cybersecurity Act;

(2) The Management Board has adopted the ENISA Strategy, including strategic objectives of the Agency.

HAS DECIDED TO ADOPT THE FOLLOWING DECISION:

Article 1

The ENISA Stakeholder Strategy 2026-2028 is adopted as set out in annex of this decision.

Article 2

The present decision shall enter into force on the day following that of its adoption. It will be published on the Agency's website.

Done in Athens, 20 November 2025

On behalf of the Management Board,

[signed]

Ms Fabienne Tegeler
Chair of the Management Board of ENISA

European Union Agency for Cybersecurity
Agamemnonos 14 | Chalandri 15231 | Attiki | Greece
Tel: +30 28 14 40 9711 | e-mail: info@enisa.europa.eu
www.enisa.europa.eu

ENISA STAKEHOLDER STRATEGY 2026-2028

INTRODUCTION

ENISA's 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 the Cybersecurity Act (CSA[1]). For example:

- Article 3(1) of CSA 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 **"**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 CSA and emphasise the need to support, assist, cooperate with **relevant stakeholders**.

Since the previous stakeholder strategy (adopted by the Management Board in 2021), the Agency's has been entrusted with more statutory tasks via new EU legislation (notably NIS2, CRA, CSOA, DORA) and confronted with increased stakeholder interest. Also, the Management Board of the Agency has reviewed ENISA Strategy in 2024, which gives the Agency a new focus and objectives in areas requiring stronger grip of its stakeholder and outreach, and aligns with ENISA's strategic objective "empowered communities in an involved and engaged cyber ecosystem".

[1] L_2019151EN.01001501.xml

OBJECTIVES

The goals of the ENISA stakeholder strategy 2026-2028 (ESS) are to:

(1) define and specify relevant stakeholder groups for ENISA and ensure that all ENISA engagement with stakeholders is value driven – it is aligned with and derived from specific needs as set in the Agency's strategic objectives and priorities and ENISA's statutory tasks. 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[2]. 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 staff to manage their stakeholder relations effectively and efficiently. ESS aims to ensure that stakeholder management is internally coordinated, avoids over-whelming stakeholders (duplication of outreach towards certain types of stakeholders) and stakeholder-fatigue;

GUIDING PRINCIPLES

(i) In line with Union law, ENISA 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 Cooperation 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 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 (MB) 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.

[2] Such as ENISA's International Cooperation Strategy, ENISA Code of Conduct etc

STAKEHOLDER MANAGEMENT & OUTREACH FRAMEWORK

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

1. MS national authorities entrusted to implement EU cybersecurity policies and legislation;
2. EU Institutions, bodies or agencies (EUIBAs) which deal with cybersecurity policy development and/or implementation at EU level;
3. Cybersecurity industry and private sector actors (incl non-EU actors), who need to fulfill the requirements stemming from EU law and who sustain and develop the EU cybersecurity ecosystem;
4. Third country cybersecurity authorities (or international organizations);
5. Cybersecurity related academic institutions, research & education organizations:
6. Civil society and general public.

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

Strategic Objective (ENISA Strategy)	6 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, threats, and cyber crises	**partner engage**	**partner engage**	**consult partner**	inform	inform	inform
Strong cyber security capacity within EU	**partner engage**	**partner engage**	**consult partner**	inform	inform **consult**	inform
Building trust in secure digital solutions	**partner engage**	**partner engage**	**consult**	inform **consult**	inform	inform
Empowered communities in an involved and engaged cyber ecosystem	**partner engage**	**partner engage**	**consult**	inform **consult**	inform	inform
Foresight on emerging and future cybersecurity opportunities and challenges	**partner engage**	**partner engage**	**consult**	inform **consult**	inform **consult**	inform
Consolidated and shared cybersecurity information & knowledge support for Europe	**partner engage**	**partner engage**	**consult partner**	inform **consult**	inform	inform

The level of engagement with the MS and EUIBAs – indeed the partnership – which the Agency needs to effectively fulfill its statutory tasks and strategic objectives is ingrained into ENISA's mandate, governance

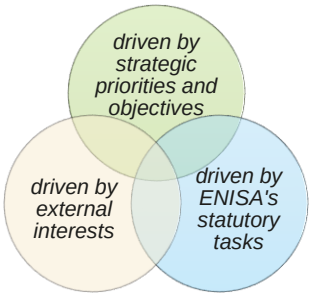
and operations. As such, there is not much need for the ESS to specify nor direct the Agency's interactions with the first two stakeholder groups, beyond the reiteration that the general principles of ESS apply, and that the Agency shall interact intensely, systematically and regularly with those two stakeholder groups across all of its operations.

The Agency's interactions with non-EU countries and international organizations are governed under it's international cooperation strategy, which the ESS shall adhere to. The required interaction with the fifth stakeholder group is of less intensity, 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 although have little influence over them. They may want more of ENISA time than can be given, and interaction with them should always be done in a manner which avoids potential conflicts of interests.

However, with new tasks and objectives, there are areas of ENISA work which now demand also setting up different partnerships with private sector actors – such as within the operationalization of Cybersecurity Reserve (contractual relationships) or uptake and implementation of the skills framework – ECSF (alliances and advocacy). ESS should thus set in place efficient ways to engage with private sector actors.

ENISA 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) it's statutory tasks. Or it might 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) nor with its principles (non-discrimination).



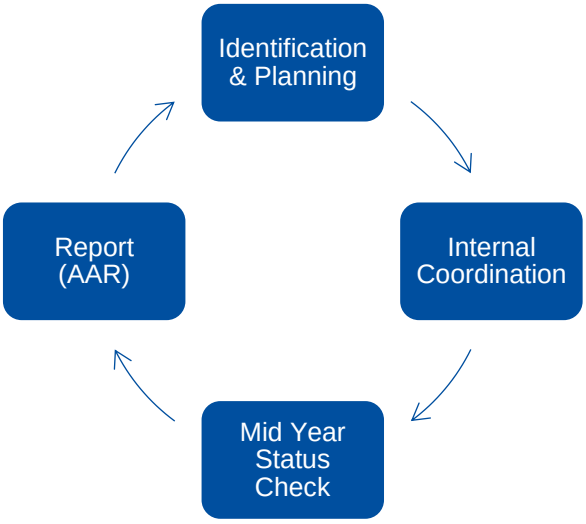
Thus, the following sections shall set and explain ENISA's engagement with private sector actors (and though less, then also with the fifth stakeholder group: academia and research and education).

'PRIORITY'-DRIVEN (STRATEGIC OBJECTIVE-DRIVEN)

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

When ENISA's strategic objectives and/or its priorities as defined in its SPD 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 Agency's engagements with its strategic stakeholders and support reporting towards the Management Board (and subsequently inform the National Liaison Officers, per request of the Management Board). This is an internal exercise to map primarily the Agency's engagement with cybersecurity industry and other private sector actors and also 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 NLOs. This helps avoid duplication, and supports coherence within the Agency and with our key partners: EU MS and EUIBAs.



'STATUTORY TASK'-DRIVEN

In order to maintain the ability and capacity to implement the more than 240 statutory tasks across EU legislation[3], beyond those tasks related to implementing ENISA strategy objectives and its SPD, ENISA shall develop and sustain the engagement with stakeholders relevant to the tasks, in line with the principles enshrined above

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 stakeholders belonging to the first two stakeholder groups (EU MS, EUIBAs). This includes press contacts. These stakeholders must align with ENISA values, objectives, and principles as outlined in this strategy. This list shall be reviewed annually and used to coordinate internally, and per 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 and other constraints, the Agency cannot always respond and accept requests from external stakeholders to engage. Thus, it shall take **a restrictive approach towards engagements driven by external interest groups**[4], prioritising and accepting only requests from stakeholders which:

- belong to similar stakeholder category as defined in its priority driven and/or statutory task driven stakeholder mappings; and

- are necessary to implement its priorities or sustain capacities to undertake statutory tasks in the short-mid term; and

[3] CSA, CRA, NIS2, CER, AIA, CSOA, DEP, DGA, DORA, ECCC, EHDS, eIDAS2, IEA, NCSS,
[4] Those types of requests might include but are not necessarily limited to: requests for bilateral meetings, visits, missions, conferences, seminars, non-prompted approaches towards Agency's staff during or in the margins of any public events etc

- do not contradict or undermine ENISA values and engagement principles as defined in this strategy or in ENISA international cooperation strategy.

ENISA's public events shall have pre-registration of participants and ENISA reserves the right to decline participation of representatives from entities, whos' engagement would not align with the above mentioned requirements

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

In maintaining its operational autonomy and independence amidst 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 which have been prepared by an external party, unless the co-creation of such documents with ENISA is foreseen in the Agency's mandate, it's annual work program or in a specific cooperation plan with an external entity.[5]

GOVERNANCE

The Executive Director impose measures and nominate roles and responsibilities which are necessary to implement this strategy. The executive director shall furthermore prepare a review of the strategy whenever the MB reviews ENISA strategy or at latest by end 2028.

[5] The Agency will operate in line with the principles set out in the ENISA International strategy