EVALUATION ROADMAP			
TITLE OF THE EVALUATION	Evaluation of the European Union Agency for Network and Information Security (ENISA)		
LEAD DG – RESPONSIBLE UNIT	CONNECT – H1	**DATE OF THIS ROADMAP**	25/07/ 2016
TYPE OF EVALUATION	Evaluation Ex-post Mixed	**PLANNED START DATE** **PLANNED COMPLETION DATE**	Q3 / 2016 Q2/ 2017
		PLANNING CALENDAR	http://ec.europa.eu/smart-regulation/evaluation/index_en.htm
This indicative roadmap is provided for information purposes only and is subject to change.			

A. Purpose

(A.1) Purpose

The purpose of the evaluation of the European Union Agency for Network and Information Security is to assess the performance of the Agency in achieving its objectives, mandate and tasks, as laid down in the Regulation No 526/2013 (retrospective analysis) and to provide the basis for a possible revision of the current mandate (forward looking analysis).

With respect to the retrospective analysis, the evaluation will assess the relevance, impact, effectiveness efficiency, coherence and EU added value of the Agency having regard to its performance, governance, internal organisational structure and working practices.

With respect to the forward looking analysis, and in order to support the Impact Assessment for the review of ENISA's Basic Regulation (No 526/2013), the evaluation will assess the possible need to modify the mandate of the Agency and the financial implications of any such modification. In doing so, the assessment will take into account the evolved context where the Agency now operates, with regard in particular to: the new EU regulatory and policy framework (e.g. the Network and Information Security Directive); the evolving needs of the Agency's stakeholders' community; and the complementarity and possible synergies with the work conducted by other EU and national institutions, agencies and bodies, like CERT-EU, the European Cybercrime Centre at Europol, European Defence Agency and EU-LISA.

The results of the evaluation will form the basis for any decision regarding the possible extension of the Agency's mandate and any changes to it. The findings of the evaluation will be made public and the related report and evaluation Staff Working Document, accompanied by Commission's conclusions, will be forwarded to the European Parliament, the Council and the Management Board.

An external contractor will support the evaluation with a dedicated study.

(A.2) Justification

The legal basis for this evaluation lays in ENISA's Regulation. Article 32 (1) of Regulation EU n. 526/2013 requires the Commission to "commission an evaluation to assess, in particular, the impact, effectiveness and efficiency of the Agency and its working practices. The evaluation shall also address the possible need to modify the mandate of the Agency and the financial implications of any such modification". Article 32 (4) also indicates that "as part of the evaluation, there shall also be an assessment of the results achieved by the Agency, having regard to its objectives, mandate and tasks. If the Commission considers that the continuation of the Agency is justified with regard to its assigned objectives, mandate and tasks, it may propose that the duration of the mandate of the Agency set out in

Article 36 be extended". In view of the changes in the cybersecurity regulatory and policy landscape, with particular reference to the adoption of the Network and Information Security Directive that foresees new tasks for ENISA, the Commission is launching this evaluation earlier than required by the Regulation (Article 32(1)), indicating June 2018 as deadline for this activity.

Finally, the Commission's Better Regulation package foresees regular evaluation of EU interventions of over €5 million.

B. Content and subject of the evaluation

(B.1) Subject area

ENISA was established in 2004 (Regulation (EC) No 460/2004) as the European Union Agency for Network and Information Security with the objective to contribute to overall goal of ensuring a high level of network and information security within the EU. The initial foreseen duration for the Agency's mandate was 5 years but it was extended twice (in 2009 and 2011).

The current mandate of the Agency is set out in Article 1 of Regulation EU n. 526/ 2013 (which repealed the 2004 Regulation and represents the new basic Act for ENISA): "to undertake the tasks assigned to it for the purpose of contributing to a high level of network and information security within the Union and in order to raise awareness of network and information security and to develop and promote a culture, of network and information security in society for the benefit of citizens, consumers, enterprises and public sector organisations in the Union, thus contributing to the establishment and proper functioning of the internal market".

It should be noted that in this context ‘network and information security’ means the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via those networks and systems.

The objectives and the tasks of the Agency are without prejudice to the competences of the Member States regarding network and information security and in any case to activities concerning public security, defence, national security (including the economic well-being of the state when the issues relate to national security matters) and the activities of the state in areas of criminal law.

(B.2) Original objectives of the intervention

ENISA's objectives are defined by article 2 of its Regulation as it follows:

1. The Agency shall develop and maintain a high level of expertise.
2. The Agency shall assist the Union institutions, bodies, offices and agencies in developing policies in network and information security.
3. The Agency shall assist the Union institutions, bodies, offices and agencies and the Member States in implementing the policies necessary to meet the legal and regulatory requirements of network and information security under existing and future legal acts of the Union, thus contributing to the proper functioning of the internal market.
4. The Agency shall assist the Union and the Member States in enhancing and strengthening their capability and preparedness to prevent, detect and respond to network and information security problems and incidents.
5. The Agency shall use its expertise to stimulate broad cooperation between actors from the public and private sectors.

(B.3) How the objectives were to be achieved

For ENISA to achieve its objectives, the Regulation identified a list of tasks, as well as operational, governance, organisational and financial provisions.

ENISA's tasks include the following.

(a) support the development of Union policy and law;

(b) support capability building;

(c) support voluntary cooperation among competent public bodies, and between stakeholders, including universities and research centres in the Union, and support awareness raising;;

(d) support research and development and standardisation;

(e) cooperate with Union institutions, bodies, offices and agencies, including those dealing with cybercrime and the protection of privacy and personal data, with a view to addressing issues of common concern;;

(f) contribute to the Union's efforts to cooperate with third countries and international organisations to promote international cooperation on network and information security issues;

(g) upon request from Union institutions, bodies, offices and agencies and Member State bodies, provide advice in the event of breach of security or loss of integrity with a significant impact on the operation of networks and services;

(h) carry out further tasks conferred on it by legal acts of the Union;

(i) express independently its own conclusions, guidance and advice on matters within the scope and objectives of its Regulation.

In order to perform its task, ENISA carries out its activities according to an annual and multiannual work programme and it has been granted an autonomous budget whose revenue comes primarily from a contribution from the Union and contributions from third countries participating in the Agency's work. Member States are allowed to make voluntary contributions to the revenue of the Agency.

With regard to the governance and organization, the main bodies of the Agency are:

- Executive Director, who has the responsibility of the administration of the Agency. This implies, among the others, the implementation of the decisions adopted by the Management Board and, upon consultation with the Management Board, the preparation of the annual and multiannual work programme.
- Management Board, composed of representatives of the Member States and the Commission, whose main responsibilities are, among the others, to establish the budget and verify its execution, adopt the work programme and appoint the Executive Director.
- Executive Board, composed of five members of the Management Board, prepares decisions to be adopted by the Management Board on administrative and budgetary matters.
- Permanent Stakeholders Group, advisory body composed of experts representing the relevant stakeholders.

The Agency counts approximately 80 staff members (including external staff), divided into two Departments: Administration and Support, based in Heraklion (Crete); Core Operations Department, located in Athens.

C. Scope of the evaluation

(C.1) Topics covered

In accordance to article 32 and 36 of ENISA's Regulation, the evaluation will support the Commission to both assess the impact, effectiveness, efficiency and added value of ENISA and its working practices and prepare the ground for a possible revision of the mandate of the Agency.

In particular, the main objectives of the evaluation will be:

1. to assess the relevance, impact, effectiveness and efficiency, coherence and EU value added of the work undertaken by the Agency and its working practices. The assessment should evaluate, but not be limited to, the implementation of the work programme as well as how the whole set of activities run by ENISA (including opinions, guidelines, trainings, recommendations or reports) have contributed to fulfil its role, objectives, mandate and tasks.
2. to assess how effectively the current governance as well as the internal organisational structure of ENISA (Management Board, Executive Board, Executive Director and staff and Permanent Stakeholders Group) contributes to efficiency and effectiveness in the work of ENISA. The assessment of the organisational structure should include an evaluation of the efficiency and effectiveness of the current arrangements related to the location of ENISA's offices.
3. to assess how successfully ENISA, within its mandate, meets the needs of its constituency in comparison to other EU and national bodies working on cybersecurity.
4. to assess the possible need for a revision or extension of the mandate entrusted to ENISA, also taking into account the evolution of the cybersecurity and digital privacy landscape, including the regulatory and policy framework (in particular the adoption of the Network and Information Security Directive).

The time period covered by the evaluation will be 2013 – 2016. The analysis will start with the entry into force of the Regulation No 526/2013, which set the new mandate for ENISA. .

(C.2) Questions/issues to be examined

The evaluation shall examine the following questions:

Effectiveness:

- To what extent has the Agency achieved its objectives and implemented the tasks set out in its mandate? What are the key factors influencing/restricting progress and how do they link to the agency (if at all)?
- What have been the benefits of acting at Agency level both from the operational and strategic perspective?
- To what extent has ENISA contributed to the overall EU goal of increasing network and information security in Europe?
- How appropriate is the balance of activities in relation to different cybersecurity and digital privacy topics considering the evolving needs of the main stakeholders?
- To what extent ENISA became an EU-wide centre of expertise and a reference point for EU institutions, Members States and the wider stakeholders community, in providing guidance, advice and assistance on issues related to network and information security?
- How effectively the Agency manages to set its work priorities?
- How effectively does the Agency tackle important upcoming, unplanned issues deriving by demands of its constituencies and/or EU policy priorities?
- Does the Agency consistently perform the same tasks with the same quality level over the time?
- How does ENISA compare to the other EU and national bodies offering similar services in

relation to their capability to satisfy the cybersecurity and digital privacy needs of ENISA's constituency?

- To what extent has ENISA been more effective in achieving its results compared to other past, existing or alternative national or EU level arrangements?
- How do the current governance, the internal organisational structure and the human resources policies and practices of ENISA contribute to efficiencies and effectiveness in the work of the agency?
- How effective has ENISA been in building a strong and trustful relationship with its stakeholders when executing its mandate?
- What is the impact of the current arrangements related to the location of ENISA's offices on the overall capability of the Agency of meeting its objectives?

Efficiency:

- To what extent has ENISA been efficient in implementing the tasks set out in its mandate as laid down in its Regulation? To assess this question, elements relating to internal structure, operation, programming of activities and resources, accountability and controls, etc. will be analysed.
- Were the annual budgets of the Agency implemented in an efficient way with a view on achieved results?
- Have the resources allocated to the agency been sufficient for the pursuing of its tasks (input/output analysis)?
- To what extent are the organisational solutions and procedures of ENISA adequate to the work entrusted to it and to the actual workload? Is the planning cycle of the agency (work programme and budget) in line with the objective of achieving efficient results?
- To what extent have ENISA's governance, organisational structure, locations and operations as set in its Regulation and the arrangements related to the location of its offices been conducive to efficiency and to achieving economies of scale?
- To what extent are the internal mechanisms for programming, monitoring, reporting and evaluating ENISA adequate for ensuring accountability and appropriate assessment of the overall performance of the Agency while minimising the administrative burden of the Agency and its stakeholders (established procedures, layers of hierarchy, division of work between teams or units, IT systems, etc)?
- To what extent has ENISA succeeded in building up the in-house capacities for handling various tasks entrusted to it? Are the "make or buy" choices made according to efficiency criteria?
- To what extent and how have external factors influenced the efficiency of ENISA?

Coherence:

- To what extent is ENISA acting in cooperation with the European Commission and other EU bodies, to ensure complementarity and avoid duplication of efforts?
- To what extent is ENISA acting in cooperation with the Member States to ensure complementarity and avoid duplication of efforts?
- To what extent are ENISA activities coherent with the strategy documents adopted in this policy field?
- Are the procedures put in place effective to ensure that ENISA's cooperation activities are coherent with the policies and activities of its stakeholders?
- What are the risks/sources of overlaps/conflict of interests?

Relevance and EU added value:

- What would be the most likely consequences at the EU level of stopping ENISA?
- How could ENISA increase its added value and its contribution towards the EU, the Member States and the private sector in the future, using the capabilities and competences already in place?
- How far are the Agency's tasks and resources aligned with key EU political priorities?
- Which Agency tasks are absolutely essential to deliver on these priorities?
- Which Agency tasks are necessary to continue implementing existing and evolving obligations

under the Treaties and EU legislative framework?

- Are there some Agency tasks that have become redundant / negative priorities? If so, which are they?
- Are the objectives set out in the mandate of ENISA still appropriate given the current cybersecurity and digital privacy needs, regulatory and policy framework and needs?
- Have some of the initially non-core activities of the Agency become part of its core-business? What was the rationale in such cases?
- What would be the most likely consequences at the EU level of stopping ENISA's activities?

Other questions:

The final report shall also address the following evaluation questions:

- Does the new scenario with increased frequency, sophistication and potential impact of cyber-threat trigger new needs from ENISA's constituency? To what extent could ENISA's current mandate, tasks and/or capabilities address these needs?
- How does the new policy and regulatory landscape, having regard to the recently adopted Network and Information Security Directive and the priorities set by the Digital Single Market Strategy, impact on ENISA's activities?
- What are the main strengths and weaknesses of ENISA, within its current mandate and organisational set-up and capacity, in taking up the new challenges?
- Is a fixed-term mandate coherent with the new challenges and tasks ENISA will have to take on?
- Which are the concrete needs and opportunities for further increased practical cooperation with Member States and EU bodies?
- Which are the concrete needs and opportunities for cooperation and synergies with international bodies working in adjacent fields, like the NATO Cooperative Cyber Defence Centre of Excellence?
- How could ENISA's mission, tasks, working practices or activities be further developed in order to better respond to the new cybersecurity landscape?
- What would be the financial implications associated to each of the possible options for modifying the mandate as they emerge from the evaluation?

(C.3) Other tasks

The evaluation will support the preparatory work for an impact assessment that will feed a Commission proposal for a possible review of ENISA's mandate.

The external contractor will also help the Commission's services in the preparation and the reporting of a public consultation that the Commission will launch as part of both the evaluation and the impact assessment process.

D. Evidence base

(D.1) Evidence from monitoring

According to ENISA's Regulation and ENISA's Financial Regulation, several planning and monitoring provisions are in place, such as :

- The Executive Director should prepare and implement the annual work programme and the multiannual work programme and reporting to the Management Board thereon;
- The Executive Director should prepare an annual report to be submitted for adoption to the Management Board. The annual report shall include the accounts and describe how the Agency has met its performance indicators.
- The Executive Director should also prepare an action plan following-up on the conclusions of the retrospective evaluations and reporting on progress every two years to the Commission;
- By 1 March following each financial year (1 March of year N + 1), the Agency's accounting

officer shall send the provisional accounts to the Commission's accounting officer together with a report on the budgetary and financial management for that financial year.

- The European Court of Auditors provides observations on the Agency's provisional accounts, pursuant to Article 148 of the Financial Regulation and it audits the Agency's accounts to ensure transparency and accountability.
- The European Court of Auditors has the power of audit, on the basis of documents and on the spot, over all grant beneficiaries, contractors and subcontractors who have received Union funds from the Agency (art. 108 ENISA's financial regulation).
- The European Parliament, upon a recommendation from the Council, before 15 May of year N+2 save where otherwise provided in the constituent act, gives a discharge to the Executive Director in respect of the implementation of the budget for year N.
- The Management Board has to adopt an anti-fraud strategy that is proportionate to the fraud risks having regard to a cost-benefit analysis of the measures to be implemented.
- The Management Board has to ensure adequate follow-up to the findings and recommendations resulting from investigations of the European Anti-fraud Office (OLAF) and the various internal or external audit reports and evaluations.
- The Management Board has to adopt rules for the prevention and management of conflicts of interest.

Any other internal or external audit reports and evaluations should also be taken into account.

(D.2) Previous evaluations and other reports

With regard to the evidence deriving from existing planning and monitoring provisions, the evaluation will take into account (but not be limited to) the following documents:

- Annual work programmes of the Agency for 2014, 2015, 2016, 2017 (forthcoming)
- ENISA Annual activity reports for the years 2013, 2014 and 2015 (forthcoming).
- ENISA's External Evaluation for the years 2014 and 2015.
- Commission Opinions on work programmes 2014 – 2017.
- European Parliament decisions and resolutions in the context of the budget discharge procedure for ENISA for the years 2013 and 2014
- Court of Auditors' reports on the annual accounts for the years 2013 and 2014
- Multi-Annual Work Programme of the Agency 2014-2018 (included in the work programme 2016)
- The Joint Statement of the European Parliament, the Council of the EU and the European Commission on a Common Approach on decentralised agencies.

The evaluation may also take into account the Impact Assessment Report (2010) that supported the "proposal from the Commission for a Regulation concerning the European Network and Information Security Agency (ENISA)" which paved the ground for the current ENISA's Regulation.

(D.3) Evidence from assessing the implementation and application of legislation (complaints, infringement procedures)

No complaints have been received by the Commission on the functioning of the Agency or the application of the establishing Regulation. There have been no infringement procedures.

(D.4) Consultation

The evaluation will follow a consultation strategy aiming at the involving the broad set of stakeholders that form ENISA's constituency and the wider public. The management and the staff of the Agency will also be consulted during the evaluation process.

The consultation will include evidence gathering activities and discussions targeting in particular the inner circle of ENISA's stakeholders - the EU institutions and other bodies, the Member States, the private sector (in particular via the Permanent Stakeholders Group).

Bridging the retrospective evaluation with the forward looking analysis for the review of ENISA, a 12

week online public consultation will also be launched to seek views from the wider public.
In the context of the commissioned study, the external contractor will also support the evidence gathering and consultation phases.

A non-exhaustive list of stakeholders that will be consulted includes the following bodies:

- The EU Member States, in particular the Host Member State and the representatives in the Management Board and Advisory Groups, as well as EFTA Countries.
- Industry and consumers representatives
- CSIRTs
- European Commission's services
- The European External Action Service, the European Parliament, the Council of the European Union, the European Data Protection Supervisor; the European Court of Auditors;
- Other EU Agencies and bodies, in particular CERT-EU, Europol and its EC3, European Defence Agency, BEREC, Eu-LISA, CEPOL.
- ENISA's contractors
- Citizens

The consultation activities will be carried out from October 2016 to April 2017.
In particular, the public consultation will be carried about from January 2017 to April 2017 (tentative dates).

(D.5) Further evidence to be gathered

A contractor will be used to support the evaluation process, with their work to be summarised in an external report.

E. Other relevant information/ remarks

N/A