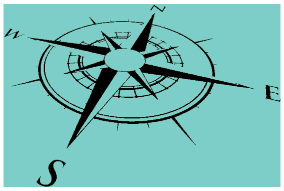
ENISA PROGRAMMING DOCUMENT 2020–2022: Including Multiannual planning, Work programme 2020 and Multiannual staff planning

Contents



European Union Agency for Cybersecurity (ENISA)

Description:

The mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the Union, by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity. We contribute to policy development and implementation, support capacity building and preparedness, facilitate operational cooperation at Union level, enhance the trustworthiness of ICT products, services and processes by rolling out cybersecurity certification schemes, enable knowledge sharing, research, innovation and awareness building, whilst developing cross-border communities... More information about ENISA and its work can be found at www.enisa.europa.eu

Stakeholder(s):

Juhan Lepassaar :
Executive Director

European Union

EU Member States

European Union Institutions

European Union Bodies

European Union Offices

European Union Agencies

Mission

To achieve a high common level of cybersecurity across the Union

Values

Trust: Our goal is to strengthen trust in the connected economy, boost resilience of the Union’s infrastructure and services and keep our society cyber secure.

Connection

Resiliency

Security

1. EXPERTISE

ANTICIPATE AND SUPPORT EUROPE'S KNOWLEDGE IN FACING EMERGING CYBERSECURITY CHALLENGES

1.1. Digital Developments

Improve knowledge on the security of digital developments

Priorities:

- Carry out regular stocktaking of EU expertise on the challenges of NIS related to existing or future services and technologies and making this information available to the EU NIS community;
- Among these challenges, focus on key issues to offer analyses and general recommendations;
- In particular, seek to explore issues related to software (e.g. mobile), ICS/SCADA, smart infrastructures and IoT, AI security and relevant technologies in sectors covered by the NIS Directive.

1.2. Cybersecurity

Cybersecurity threat landscape and analysis

Priorities:

- Conducting an annual EU threat landscape analysis providing a general technical assessment of existing and expected threats and their causes;
- Prepare annual analyses of national incident reports in the context of the implementation of the telecommunications package, eIDAS Regulation and the NIS Directive;
- Disseminate relevant threat related information through relevant channels and networks, taking into account the sensitivity of the information;
- Regularly provide a concise overview on cyber threats as they have evolved in incidents. This information should provide a neutral overview of the results of the available open source evidence

1.3. R&D

Research & Development, Innovation

Priorities:

- Assist Member States and the European Commission in defining EU priorities for R&D and deployment in the field of cybersecurity;
- Participation in relevant activities promoted by the Panel established by the proposed regulation5 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the network of National Coordination Centres;
- Built on ENISA's support to the Member States and economic operators for cybersecurity preparedness and resilience as well as on certification and standardisation; contribute to research and deployment priorities and formulate technical requirements.

2. NETWORKS & INFORMATION

PROMOTE NETWORK AND INFORMATION SECURITY AS AN EU POLICY PRIORITY

2.1. Policy Development

Support EU Policy Development

Priorities:

- Carry out a regularly updated stocktaking of current and future EU policy initiatives with NIS implications and make it available to the European Commission and national competent NIS authorities;
- Support the activities of the Cooperation Group in the field ofnew policy developments;
- Focus in particular on policies related to the sectoral dimension of NIS and on policies dedicated to cybersecurity to ensure coherence with the framework and principles agreed on in the NIS Directive;
- Seek to identify, as far aspossible, all NIS challenges that may require policy developments at EU level;
- Build on this stocktaking and take into account the previously identified NIS challenges and offer advice to the European Commission and other relevant institutions of the Union on these policy developments.

2.2. Policy Implementation

Supporting EU Policy Implementation

Priorities:

- Support the cooperation group and assist the competent national NIS authorities in cooperating in the implementation of already agreed EU policies (legislations) with a NIS dimension;
- Focus on the NIS Directive, in particular regarding the requirements related to Operators of Essential Services (OES) (e.g. identification, security requirements, incident reporting) and on the eIDAS Regulation, taking into account the NIS aspects of GDPR (and more generally data protection) and the ePrivacy Regulation draft as it reflects the ENISA regulation;
- Support cybersecurity activities in the framework of the implementation of the European Electronic Communications Code.

3. CAPACITY

SUPPORT EUROPE IN MAINTAINING STATE-OF-THE-ART NETWORK AND INFORMATION SECURITY CAPACITIES

3.1. Capacity Building

Assist Member States' capacity building

Priorities:

- Advise and assist Member States in building national cybersecurity capacities based on national experiences and best practices;
- Focus on the NIS capacities foreseen in the NIS Directive, building on ongoing activities in the CSIRTs Network and national CSIRTs on which ENISA should continue to work on to promote the strengthening of the CSIRTs of the EU Member States';
- Develop national NIS capacity indicators, building on capacities foreseen in the NIS Directive and allowing an assessment of the state of the NIS capacity development within the EU;
- Identify and derive recommendations for other national NIS capacities that would contribute to strengthening EU NIS through dissemination throughout the EU NIS community, e.g. national cybersecurity assessments, PPPs for instance in the field of CIIP, national information sharing schemes, etc.;
- Providing support and guidance for the establishment of national and European Information Sharing and Analysis Centres (ISACs) in specific sectors.

3.2. Assistance

Assist in the EU institutions' capacity building

Priorities:

- Representation of the EU decentralised agencies on the CERT-EU Steering Board;
- Cooperation with relevant EU agencies on initiatives covering NIS dimension related to their mission;
- Support (upon request and in coordination with the institutions) capacity building for trainings, awareness raising, and development of education material.

Stakeholder(s):
EU Institutions

3.3. Awareness

Awareness raising

Priorities:

- Work with the relevant national authorities to advise private sector on how to improve its own NIS through by developing key recommendations for the private sector cybersecurity ;
- Support the exchange of best practices on awareness and education between public and private sectors at European level;
- Organise the European Cybersecurity Month (ECSM) and the European Cybersecurity Challenge (ECSC) to make these events a place for EU cybersecurity awareness; pool, organise and make

information on security of network and information systems, in particular on cybersecurity (provided by the EU institutions, agencies and bodies) publicly availablethrough a dedicated portal ;

- Regularly carry out stocktaking of national awareness-raising initiatives;
- Build on this stocktaking and, in liaison with the ECSM and ECSC, analyse and provide recommendations and advice on best practices in the field of awareness-raising, in particular with regard to communication activities.

4. COOPERATION

FOSTER THE OPERATIONAL COOPERATION WITHIN THE EUROPEAN CYBERSECURITY COMMUNITY

4.1. Cyber Crises

Cyber crisis cooperation

Priorities:

- Further develop and organise Cyber Europe 2020, exploring new dimensions and formats to further prepare the Member States and EU institutions for cyber crises that may occur in the EU in the future;
- Integrate existing and future EU-wide crisis management orientations, mechanisms, procedures and tools within the framework of Cyber Europe exercises, in particular the CSIRTs network foreseen in the NIS Directive and the cooperation group;
- Actively contribute to the implementation of the blueprint by supporting MS in integrating guidelines, mechanisms, procedures and tools at EU level into the national crisis management frameworks; the Agency will contribute to developing a cooperative response at Union and Member States level to large-scale cross-border incidents or crises related to the cybersecurity through a series of tasks, from raising wide situational awareness across the Union to testing cooperation plans for incidents;
- Integrate existing and future EU-wide crisis management orientations, mechanisms, procedures and tools into the existing crisis management framework of the MS;
- Closely follow the development of the CEF Cybersecurity DSI CSP and ensure a smooth handover to ENISA and support the voluntary adoption by the CSIRT community;
- Proactively develop its expertise in the field of cyber crisis management and exercises in cooperation with other EU institutions and Member States wishing to develop exercises with a cyber dimension. In doing so, ensure consistency with the Cyber Europe framework.

4.2. Operations & Communities

Community building and operational cooperation

Priorities:

- Provide the secretariat and active support for the CSIRT Network foreseen in the NIS Directive;
- Ensure, among other things, a well-functioning and resilient CSIRT Network IT infrastructure and communication channels. Ensure structured cooperation with CERT-EU, EC3 and other relevant EU bodies;
- Use the development of the CSIRT core platform under the the “Connecting European Facility” (CEF) mechanism to support the functioning of the CSIRT Network and, upon request, advise Member States’ CSIRTs on projects to be proposed on future CEF calls for projects;
- Leverage the role of the Single Point of Contact (NISD), taking into account that is performs a liaison function to ensure cross-border cooperation of MS.

5. CERTIFICATION

DEVELOP CYBERSECURITY CERTIFICATION SCHEMES FOR DIGITAL PRODUCTS, SERVICES AND PROCESSES

5.1. Activities

Support activities related to cybersecurity certification

Priorities:

- Support the work undertaken within the EU Cybersecurity Certification Framework;
- making available to designated stakeholders and the general public, information on cybersecurity certification schemes through a dedicated portal;
- Support the European Commission in its role as Chair of the EU Cybersecurity Certification Group;
- Support the Stakeholder Cybersecurity Certification Group.

5.2. Certification Schemes

Develop candidate cybersecurity certification schemes

Priorities*

- Support the work carried out under the EU Cybersecurity Certification Framework, including the provision of technical expertise to prepare candidate European cybersecurity certification schemes in functional application areas in accordance to the Union’s rolling work programme for certification;
- Support the development and implementation of the Union’s policy on standardisation, certification and market surveillance;
- Facilitate the adoption of risk-management standards for electronic products, networks and services and advise relevant stakeholders on cybersecurity certification framework technical security requirements;
- Focus on cybersecurity certification policies to ensure coherence with the framework and principles agreed onin the Cybersecurity Act.

6. ENABLING

REINFORCE ENISA'S IMPACT

6.1. Management & Compliance

Management and compliance

Priorities:

- Optimise talent acquisition and retention to fulfill ENISA's mandate; establish an appropriate development management programme; ensure a safe and healthy working environment, supported by proportional and adequate social measures;
- Maximise the leaning and rationalisation of processes and tools in compliance with the EU regulatory framework and the use of best practices;
- Provide a learning environment for employees by offering a wide range of learning and development opportunities to achieve the organisation's objectives;
- 100% compliance with our financial and legal framework;
- Assess and implement the Agency's business requirements and internal strategy;
- Develop an appropriate internal control system for internal delivery optimisation, compliance, fraud prevention and management of potential conflict of interests;
- Maintain and improve the goal of preventing harassment and applying best practices for healthy work environments.

6.2. Engagement

Engagement with stakeholders and international relations

Priorities:

- Involve the experts of the competent national NIS authorities of the Member States in the preparation of the results;
- Proactively engage with other competent Union institutions (e.g. the European Commission), other agencies or CERT-EU to identify possible synergies, avoid redundancy and offer advice based on ENISA's NIS expertise;
- Seek to increase and evaluate the added value and impact of its activities with the European NIS community;
- Communicate transparently with stakeholders, in particular with Member States, on activities to be carried out and inform them of their implementation;
- Contribute, when relevant and on an ad hoc basis, to the Union's efforts to cooperate with third countries and international organisations to promote international cooperation on NIS.

Administrative Information

Start Date: 2020-01-01
End Date: 2022-12-31

Publication Date: **2020-04-24**
Source: https://www.enisa.europa.eu/publications/corporate-documents/enisa-programming-document-202020132022

Submitter:

Given Name: Owen
Surname: Ambur
Email: Owen.Ambur@verizon.net
Phone: