European Union Agency
for Cybersecurity
Vasilissis Sofias Str 1
151 24 Maroussi | Attiki | Greece
Tel: +30 28 14 40 9711
E-mail: info@enisa.europa.eu
www.enisa.europa.eu

DECISION No MB/2020/20 of the Management Board of the European Union Agency for Cybersecurity (ENISA) adopting the Programming Document 2021-2023, the Statement of estimates 2021 and the Establishment plan 2021

THE MANAGEMENT BOARD OF ENISA,

Having regard to the 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)[1], in particular Article 15.1.(c), Article 24.3., Article 24.4., and Article 29.7.

Having regard to the Decision No MB/2019/8 on the Financial Rules applicable to ENISA in conformity with the Commission Delegated Regulation (EU) No 2019/715 of 18 December 2018 of the European Parliament and of the Council

Having regard to the Communication from the Commission C(2020) 2297 final of 20 April 2020 on the strengthening of the governance of Union Bodies under Article 70 of the Financial Regulation 2018/1046 and on the guidelines for the Single Programming Document and the Consolidated Annual Activity Report.

Whereas:

(1) The Single Programming Document 2021-2023 should be adopted by the Management Board by 30 November 2020.

(2) The Statement of Estimates for the financial year 2021 and the Establishment plan 2021 were scrutinised by the Executive Board;

(3) The Single Programming Document of the Agency should be forwarded to the Member States, the European Parliament, the Council and the Commission following adoption;

HAS DECIDED TO ADOPT THE FOLLOWING DECISION:

Article 1

The Single Programming Document 2021-2023 is adopted as set out in the Annex 1 of this decision.

[1] *OJ L 151, 7.6.2019, p. 15–69*

Article 2

The Statement of estimates of revenue and expenditure for the financial year 2021 and the Establishment plan 2021 is adopted as set-out in Annex 2 and Annex 3 of this decision. It shall become final following the definitive adoption of the general budget of the Union for the financial year 2021.

Article 3

Where necessary, the Management Board shall adjust ENISAs single programming document 2021-2023 and ENISA's statement of estimates in accordance with the general budget of the Union for the financial year 2021.

Article 4

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 by written procedure on 30 November 2020.

On behalf of the Management Board,

[Signed]

Chairperson

Jean Baptiste Demaison

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ENISA SINGLE PROGRAMMING DOCUMENT 2021-2023

Including Multiannual planning,
Work programme 2021 and
Multiannual staff planning

VERSION: FINAL FOR ADOPTION

DOCUMENT HISTORY

//DRAFT ONLY - DELETE THIS SECTION AND PAGE UPON FINAL PUBLICATION

Date	Version	Modification	Author
January 2020	V1	First draft sent for MB consultation.	ENISA
January 2020	V2	Draft for MB consultation/adoption.	ENISA
February 2020	V3	Draft for MB endorsement	ENISA
May 2020	V4	Draft reviewed to reflect ENISA Strategy and apply new template adopted by COM C(2020) 2297 final	ENISA
June 2020	V5	Draft for MB consultation	ENISA
July 2020	V6	Draft for consultation	ENISA
September 2020	V6.1	Consolidated comments from MS (CZ, DE, ES, LV, SE) and COM	ENISA
October 2020	V7	Draft for EB consultation	ENISA
November 2020	V8	Final for MB	ENISA

TABLE OF CONTENTS

LIST OF ACRONYMS

[to be completed at a later stage]

CSA – Cybersecurity Act

EECC – European Electronic Communication Code

GDPR – General Data Protection Regulation

NISD – NIS Directive

NISCG – NIS directive Cooperation Group

NCSS – National Cybersecurity Strategies

INTRODUCTION

FOREWORD

This new Single Programming Document (SPD) for 2021-2023 marks a new step in the planning of the operations and activities, as well as the planning and use of resources by the Agency.

Firstly, it has been developed to enable the Agency to fully exploit its permanent mandate and be able to fulfil all the tasks given to it by the Cybersecurity Act (CSA), whilst taking into account all other changes in the Union's regulatory framework. All the activities and outputs in this work program stem and are clearly derived from the statutory obligations of the Agency, none of the statutory tasks are forgotten or neglected.

Moreover, the planning document is also making full use of the different statutory bodies set up by the CSA (such as the National Liaison Officers network and others) and Union law, to guide and help the Agency to design and validate the specific deliverables which the Agency will undertake and produce across the activities foreseen in this SPD. This ensures that the activities undertaken according to this SPD will be done in cooperation and in synergy with all relevant actors at the Union and national level.

The SPD is fully aligned and incorporates the changes introduced to the design and set-up of the Single Programming Documents of Union bodies, as adopted by the European Commission in April 2020.[1]

Secondly, the new SPD is in line with the new strategy of ENISA, which was adopted by the Management Board in June 2020, and has been used as a baseline to set the strategic objectives and priorities for programming the Agency's work in a multiannual frame.

Thirdly, the programming document has been drawn up in parallel with the reorganisation of the Agency and its new structure, which was decided by the Management Board in June and will become effective 1 January 2021, the same day when this SPD will become operational. As the new organisation aligns the tasks and functions of the Agency's structural setup with the CSA, it will not only allow a more efficient delivery of the activities foreseen in the SPD, but also ensures that there are adequate and sufficient capabilities within the Agency to fulfil its obligations and undertakings in an effective manner.

Finally, this SPD acknowledges and takes into account the ever-shifting cyber landscape and evolving wider socio-economic context. The COVID-19 crises demonstrated the ability of the Agency to rapidly shift its priorities, as well as to rise to the challenge of catering for the cybersecurity needs of a society, which has undertaken a massive digital transition of its functions, posing new risks as well as opportunities. This SPD, whilst being clear on the scope of different activities and outputs, allows for sufficient flexibility in designing individual deliverables in order to ensure that the Agency's activities and contributions will be able to take account the most recent developments, thus giving high added value to the European Union at large and the best value for money for the European taxpayer.

Juhan Lepassaar
Executive Director

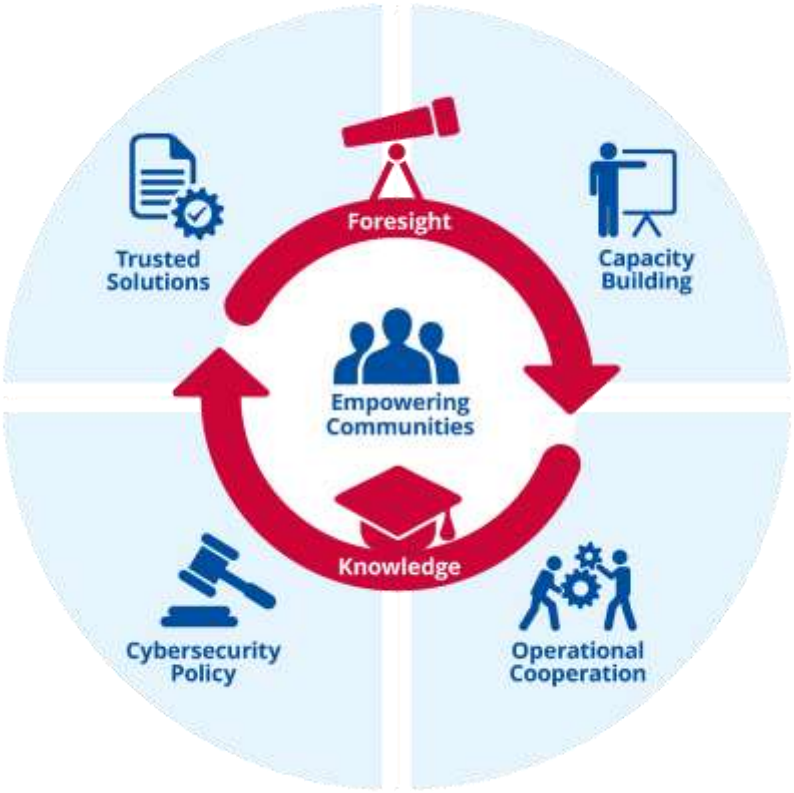
MISSION STATEMENT

[1] Communication from the Commission on the strengthening of the governance /…/ C(2020)2297 final, 20.04.2020.

The mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the Union in cooperation with the wider community. It does this through acting as a centre of expertise on cybersecurity, collecting and providing independent, high quality technical advice and assistance to Member States and EU bodies on cybersecurity. It contributes to developing and implementing the Union's cyber policies.

Our aim is to strengthen trust in the connected economy, boost resilience and trust of the Union's infrastructure and services and keep our society and citizens digitally secure. We aspire to be an agile, environmentally and socially responsible organisation focused on people.

STRATEGY



EMPOWERING COMMUNITIES

Cybersecurity is a shared responsibility. Europe strives for a cross sectoral, all-inclusive cooperation framework. ENISA plays a key role in stimulating active cooperation between the cybersecurity stakeholders in Member States and the EU institutions and agencies. It strives to ensure complementarity of common efforts, by adding value to the stakeholders, exploring synergies and effectively using limited cybersecurity expertise and resources. Communities should be empowered to scale up the cybersecurity model.

CYBERSECURITY POLICY

Cybersecurity is the cornerstone of digital transformation and the need for it permeates all sectors, therefore it needs to be considered across a broad range of policy fields and initiatives. Cybersecurity must not be restricted to a specialist community of technical cyber experts. Cybersecurity must therefore be embedded across all domains of EU policy. Avoiding fragmentation and the need for a coherent approach while taking into account the specificities of each sector is essential.

OPERATIONAL COOPERATION

The benefits of the European digital economy and society can only be fully attained under the premise of cybersecurity. Cyber-attacks know no borders. All layers of society can be impacted and the Union needs to be ready

to respond to massive (large scale and cross-border) cyber-attacks and cyber crisis. Cross-border interdependencies have highlighted the need for effective cooperation between Member States and the EU institutions for faster response and proper coordination of efforts at all levels (strategic, operational, technical and communications).

CAPACITY BUILDING

The frequency and sophistication of cyberattacks is rising speedily, while at the same time the use of ICT infrastructures and technologies by individuals, organisations, and industries is increasing rapidly. The needs for cybersecurity knowledge and competences exceeds the supply. The EU has to invest in building competences and talents in cybersecurity at all levels, from the non-expert to the highly skilled professional. The investments should focus not only on increasing the cybersecurity skillset in the Member States but also on making sure that the different operational communities possess the appropriate capacity to deal with the cyber threat landscape.

TRUSTED SOLUTION

Digital products and services bring about benefits that need to be leveraged as well as risks, that need to be mitigated. While evaluating the security of digital solutions and ensuring their trustfulness, it is essential to adopt a common approach, with the goal to strike a balance across societal, market, economic and cybersecurity needs. Innovative solutions are explored, much as repurposing standardised ones is. A dedicated entity acting in a cohesive manner is likely to increase stakeholders' trust on digital solutions and the broader digital environment in the internal market.

FORESIGHT

Numerous new technologies, still in their infancy or close to mainstream adoption, would benefit from the use of foresight methods. Through a structured process enabling dialogue among stakeholders, decision- and policy-makers would be able to define early mitigation strategies that improve the EU resilience to cybersecurity threats and find solutions to address emerging challenges.

KNOWLEDGE

The energy that fuels the mill of cybersecurity is information and knowledge. For cybersecurity professionals to be efficient at tackling our objectives, to work in a constantly moving environment – in terms of digital developments as well as with regard to actors – to face the challenges of our time, we need a continuous process of collecting, organising, summarising, analysing, communicating, and maintaining cybersecurity information and knowledge. All phases are essential to ensure that information and knowledge is shared and expanded within the EU cybersecurity ecosystem.

SECTION I. GENERAL CONTEXT

On 27 November 2019, during the plenary session in Strasbourg, President von der Leyen presented the views and objectives of the European Commission for the entirety of its mandate 2019-2024, noting that[2]:

"/…/ cyber security and digitalisation are two sides of the same coin. This is why cyber security is a top priority. For the competitiveness of European companies we have to have stringent security requirements and a unified European approach. We have to share our knowledge of the dangers. We need a common platform, we need an enhanced European Cybersecurity Agency. That is the only way we can strengthen trust in the connected economy and boost resilience to dangers of all kinds. We can do all this if we act together, if we build on our European values. And by doing so I am confident that Europe will play a leading role in the digital age. Europe can do it!"

With the Cybersecurity Act (CSA), which was enacted in June 2019, the Agency became a key instrument for realising the EU's ambition of significantly reinforcing cybersecurity across Europe. The strengthened and expanded tasks of the Agency in the field of operational cooperation were put into test in 2020, as the need to ensure adequate cybersecurity throughout the COVID-19 crises presented the Agency with a challenge. Acting in the context of Article 7 of the CSA, ENISA undertook a number of activities,[3] which played an important role in helping EU bodies to coordinate their activities throughout the initial phases of the pandemic and raise the resilience of the Union. These practical steps and actions are not foreseen to remain one-off, but will continue to be pursued through the evolving Blueprint and could be merged, if and when necessary, with the Joint Cyber Unit framework as this concept, announced by President von der Leyen in 2019, will be further developed. 2021 will also mark the year when structured cooperation between ENISA and CERT-EU in the field of operational cooperation, [pending endorsement by the Management Board in October 2020,] will become fully operational, influencing the activities foreseen in the 2021 Work Programme of this SPD and beyond.

The CSA also set up a framework for European cybersecurity certification schemes with a view to creating a digital single market for ICT products, services and processes. The Agency started to execute this function fully in 2020, in particular on candidate schemes for common criteria and cloud services. In 2021 this work will continue, taking into account the demands of the emerging Union Rolling Work Programme for European cybersecurity certification, but also the increasing calls to take practical steps in order to ensure the Union's digital sovereignty and autonomy. The need to contribute to raising the competitiveness of the European cybersecurity market and industry, also by advising and assisting the Union bodies [including the Cybersecurity Competences Centre and Network[4]] in setting the cybersecurity research and innovation priorities, as well as providing regular insight on how both the supply and demand sides of the market function, will kick-start in 2021 and continue to grow in the years to come.

The Agency will continue to support the Union decision making institutions in relation to the announced review of the NIS Directive. This renewal and strengthening of the key pillar of Union's regulatory framework which underpins the cybersecurity of critical sectors across our society could further make use of the expanded and permanent mandate given to the Agency and thus also influence the development of the ENISA Work Programme in the years to come. The Agency will need to anticipate and stand ready to contribute to the development and implementation of Union law and policies in different sectors, including in relation to the European Electronic Communication Code (EECC) etc., by providing expertise and

[2] Ursula von der Leyen President-elect of the European Commission, Speech in the European Parliament Plenary Session, as delivered, available at: https://ec.europa.eu/info/sites/info/files/comm-2019-00612-00-00-en-tra-00_0.pdf , pages 9-10.
[3] including initiating contacts with the Commission, Europol EC3 and CERT-EU to establish an information exchange network that subsequently attracted the participation of the EEAS and the Council; contributing to the technical annex of the Commission's recommendation on contact tracing apps…
[4] In September 2018, the European Commission proposed a Regulation setting up a European Cybersecurity Competence Centre and Network. The [draft] Regulation ensures cooperation and complementarity with ENISA. In particular, ENISA will have an important role in contributing to the Competence Centre's strategic role in coordinating Cybersecurity technology - related investments by the Union, Member States, and industry. The council agreed to a negotiation position in June 2020 and the trilogies with the European Parliament started in Summer 2020.

technical input in cybersecurity aspects across different policy fields and standing ready to step into and help to fulfil new tasks, should it be called to do so by Union's institutions and Member States.

Beyond the context of political and legislative developments, the COVID-19 pandemic has dramatically altered the Union's economic outlook and posed new challenges to the functioning of the European society. The almost overnight global transition to digital solutions, in order to keep the essential functions of societies going across different fields, is unprecedented. Never before have people been forced to prefer the digital world over the physical world in in such scale and this poses new risks as well as challenges in terms of ensuring the high level of cybersecurity across the Union. The Agency, rising to meet this challenge, has dramatically increased its capabilities as well as channelled resources in this Work Programme, to assist and help capacity building activities in critical areas touched by the crises. It has furthermore prioritised both targeted and general actions to raise awareness and foster education in cybersecurity.

During these unprecedented times, it is more important than ever that the Agency increases its outreach activities, builds and utilises synergies amongst all the relevant actors at the Union level and beyond, to ensure a coherent and joined up approach to enhance cybersecurity across the Union, as well as contributing into efforts which ensure that global developments across the cybersecurity landscape are aligned and enlightened by Union's values and will increase its competitiveness. The development of the stakeholder and international strategies of the Agency will be important baselines which will frame actions to this end, and will also thus impact the evolvement of the Work Programme in the future.

SECTION II. MULTI-ANNUAL PROGRAMMING 2021 – 2023

Europe has for decades taken steps to improve digital security and trust through policies and initiatives. The Management Board of ENISA adopted a new strategy for the Agency in June 2020, which builds on the Cybersecurity Act (CSA), and outlines how the Agency will strive to meet the expectation of the cybersecurity ecosystem in a long term perspective, in a manner that is open, innovative, agile as well as being socially and environmentally responsible. The strategy sets out a vision of "A trusted and cyber secure Europe" in which all citizens and organisations of Europe not only benefit but are key components in the effort to secure Europe. Importantly, the new ENISA strategy outlines seven strategic objectives which are derived from the CSA and set the expected long term goals for the Agency.

The most fundamental, that weaves across all other objectives because of the nature of cybersecurity being a shared responsibility is the strategic objective of **empowered and engaged communities across the cybersecurity ecosystem**. The Agency strives to ensure complementarity of common efforts, exploring synergies and effective use of limited cybersecurity expertise and resources which can be achieved only through organised interactions between all players in the cybersecurity ecosystem.

The following two strategic objectives both have an integral role vis-à-vis the other strategic objectives because they are the lenses with which the other objectives operate. Strategic objective **foresight on emerging and future cybersecurity challenges** provides understanding of emerging trends and patterns in order to define early mitigation strategies that improve the EU's resilience to cybersecurity threats.

The energy that fuels the mill of cybersecurity is information and knowledge, which brings us on to the strategic objective **efficient and effective cybersecurity information and knowledge management for Europe**. To address the challenges of our time, we therefore need a continuous process of collecting, organising, summarising, analysing, communicating, and maintaining cybersecurity information and knowledge. All phases are essential to ensure that information and knowledge is shared and expanded within the EU cybersecurity ecosystem.

The remaining strategic objectives tackle vertical domains of cybersecurity. Strategic Objective**:** "**Cybersecurity as an integral part of EU policies**", seeks to embed cybersecurity across all domains of EU policy. Avoiding fragmentation and the need for a coherent approach while taking into account the specificities of each sector is essential.

Strategic objective**:** "**Effective cooperation amongst operational actors within the Union in case of massive cyber incidents**" seeks to strengthen effective cooperation between Member States and the EU institutions in order to respond to large scale cross-border cyber-attacks and cyber crisis.

Strategic objective: "**Cutting-edge competences and capabilities in cybersecurity across the Union**" seeks to address the gap between supply and needs for cybersecurity knowledge and competences and makes sure that the different operational communities possess the appropriate capacity to deal with the cyber threat landscape.

Strategic objective: "**High level of trust in secure digital solutions**" seeks to provide trust to citizens ICT products, services and processes with the deployment of certification schemes.

The following table maps the strategic objectives against the CSA Articles and the activities of the Work Programme.

STRATEGIC OBJECTIVE	ACTIONS TO ACHIEVE OBJECTIVE	ARTICLE OF THE CSA	EXPECTED RESULTS	KPI	METRICS
SO1 **Empowered and engaged communities across the cybersecurity ecosystem**	Activities 1 to 9	Art.5 to Art.12	Empowered ecosystem encompassing Member States authorities, EU institutions, agencies and bodies, associations, research centres and universities, industry, private actors and citizens, who all play their role in making Europe cyber secure	Community-building across the cybersecurity ecosystem	Additional quantitative measures stemming from the stakeholder strategy that will be developed in 2021 Stakeholder satisfaction of ENISA's role as facilitator of community-building and collaboration across the cybersecurity ecosystem
SO2 **Cybersecurity as an integral part of EU policies**	Activities 1 & 2	Art.5	Where relevant, support the Commission in ensuring that EU and national policies takeaccount of cybersecurity aspects	ENISA's added value to EU institutions, bodies and Member States in providing support to policy-making (ex-ante)	1. Number of relevant contributions to EU and national policies and legislative initiatives 2. Number of references to ENISA reports, analysis and/or studies in EU and national policy documents 3. Satisfaction with ENISA added-value and weight of contributions (survey)
			• Consistent implementation of Union policy and law in the area of cybersecurity • EU cybersecurity policy implementation reflects sectorial specificities and needs • Exchange of good practice	Contribution to policy implementation and implementation monitoring at EU and national level (ex-post)	1. Number of EU policies and regulations implemented at national level supported by ENISA 2 Number of ENISA reports, analysis and/or studies referred to at the EU and national level (survey) 3 Satisfaction with ENISA added-value and weight of support (survey)
SO3 **Effective cooperation amongst operational actors within the Union in case of massive[5] cyber incidents**	Activities 4 & 5	Art.7	• All communities (EU Institutions and MS) use a rationalised set of SOP[6]s • An agreed CSIRTs Network approach for selecting, operating and decommissioning tools • Coherent SOPs for cyber crises management • Efficient framework, tools and methodologies for effective cyber crisis management	Effective use of ENISA's tools, platforms and take up of SOPs in operational cooperation	1. Number of users both new and recurring and usage per platform/ tool/ SOPs provided by ENISA 2. Uptake of the platform/ tool/ SOPs during massive cyber incidents 3. Stakeholder satisfaction on the relevance and added value of the platforms/ tools/ SOPs provided by ENISA
			• Member States and institutions cooperating effectively during large scale cross border incidents or crises • Public informed on a regular basis of important cybersecurity developments • Stakeholders aware of current cybersecurity situation	ENISA ability to support response to massive cyber incidents	1. Timeliness and relevance of information shared and expertise provided by ENISA in relation to incidents ENISA contributes to mitigate 2. Stakeholders' satisfaction of ENISA's ability to provide operational support

[5] large scale and cross-border
[6] Standard Operating Procedures.

SO4 **Cutting-edge competences and capabilities in cybersecurity across the Union**	Activities 3 & 9	Art.6 and Art.7(5)	• Enhanced capabilities across the community • increased cooperation between communities	Increased resilience against cybersecurity risks and preparedness to respond to cyber incidents	1. Increase/decrease of maturity indicators 2. Outreach, uptake and application of lessons learnt from capability-building activities. 3. Number of cybersecurity programmes (courses) and participation rates 4. Stakeholder assessment on usefulness, added value an relevance of ENISA capacity building activities
		Art.10 & Art.12	• Greater understanding of cybersecurity risks and practices • Stronger European cybersecurity through higher global resilience.	Level of awareness on cybersecurity, cyber hygiene and cyber literacy across the EU	1. Number of activities and participation to awareness raising actions organised by ENISA on cybersecurity topics 2. Level of awareness on cybersecurity across the EU/ general public (e.g. EU barometer)
SO5 **High level of trust in secure digital solutions**	Activities 6 & 7	Art.8	• Support for schemes chosen to run under the European cybersecurity certification framework Certified ICT products, services and processes are preferred by consumers and where relevant, Operators of Essential Services or Digital Service Providers	Uptake of the European cybersecurity certification framework and schemes as an enabler for secure digital solutions Effective preparation of candidate certification schemes prepared by ENISA	1. Number of stakeholders (governments or commercial solution providers) on the EU market using the cybersecurity certification framework for their digital solutions 2. Citizens' trust in digital solutions 3. Satisfaction with ENISA's support in the preparation of candidate schemes (survey)
			• Where relevant, contribution towards a more competitive European cybersecurity industry, SMEs and start-ups	Recognition of ENISAs supporting role for participants in the European cybersecurity market	1. Number of market analysis, guidelines and good practices issued by ENISA 2. Uptake of lessons learnt / recommendations from ENISA reports 3. Stakeholder satisfaction with the added value and quality of ENISA's work
SO6 **Foresight on emerging and future cybersecurity challenges** **&** **SO7** **Efficient and effective cybersecurity information and knowledge**	Activity 8	Art.9 & Art.11	• Decisions about cybersecurity are future proof and to take account the trends, developments and knowledge across the ecosystem • Stakeholders receive relevant and timely information for policy and decision making	ENISA's ability to contribute to Europe's cyber resilience through timely and effective information and knowledge	1. Number of users and frequency of usage of dedicated portal (observatory) 2 Number of recommendations, analysis, challenges identified and analysed 3 Stakeholder satisfaction on the usefulness, relevance and timeliness of ENISA's foresight and advice on cybersecurity challenges & opportunities (incl in research)

management for Europe					

The strategy of ENISA also establishes a set of values which guide the execution of its mandate and its functioning, namely:

Community Mind-Set ENISA works with communities, respecting their competencies and expertise, and fosters synergies and trust to best achieve its mission.

Excellence ENISA aims for state-of-the-art expertise in its work, upholds the highest quality standards of operation and evaluates its performance to strive for continuous improvement through innovation and foresight.

Integrity/ethics ENISA upholds ethical principles and EU relevant rules and obligations in its services and working environment ensuring fairness and inclusiveness.

Respect ENISA respects fundamental European rights and values covering all its services and working environment, as well as the expectations of its stakeholders.

Responsibility ENISA assumes responsibility thus ensuring integration of the social and environmental dimensions into practices and procedures.

Transparency ENISA adopts procedures, structures and processes that are open, factual and independent, thus limiting bias, ambiguity, fraud and obscurity.

Those values are built on the ethos of the CSA, and in particular the objectives set out in Articles 3(4) and 4(1), and have been encapsulating into two corporate objectives, which form the baseline from which the multiannual activities of the SPD will be delivered.

The corporate objective of **sound resource and risk management** is derived from requirements in Art 4(1) of the CSA that sets an objective for the Agency to: “be a centre of expertise on cybersecurity by virtue of its independence, the scientific and technical quality of the advice and assistance it delivers, the information it provides, the transparency of its operating procedures, the methods of operation, and its diligence in carrying out its tasks”. In addition, the inspiration for this corporate objective stems from the values of **Excellence** and **Transparency** derived from the ENISA strategy and the principle of **Efficiency** set out in MB decision 2020/5 on the principles to be applied for organising ENISA. This aims for ENISA to uphold the highest quality of standards, strive for continuous improvement and enhance the organisation’s performance.

The corporate objective of **building an agile organisation focused on people** is derived from requirements in Art 3(4) of the CSA which obliges the Agency to: “develop its own resources, including /…/ human capabilities and skills, necessary to perform the tasks assigned to it under this Regulation”. In addition, the inspiration for this corporate objective stems from the values of **Responsibility** and **Respect** derived from the ENISA strategy and the principle of **Competences** set out in MB decision 2020/5 on the principles to be applied for organising ENISA. This aims for ENISA to respect fundamental European rights and values in its

working environment, assume responsibility for social and environmental dimensions of its procedures and to develop its staff competences, expertise and talent.

CORPORATE OBJECTIVE	ACTIVITY TO ACHIEVE OBJECTIVE	ARTICLE OF THE CSA	EXPECTED RESULTS	KPI	METRICS
Sound resource and risk management	Activity 10	Art 4(1)	Maximize value for money provided to stakeholders and citizens Building lasting credibility and trust	Organisational performance culture	1. Proportion of KPI's reaching targets 2. Individual contribution to achieving the objectives of the agency via clear link to KPI's (CDR report) 3. Exceptions in Risk Register 4. Number of complaints filed against ENISA incl number of inquiries/ complaints of the EU Ombudsman 5. Results of annual risk assessment exercise 6. Observations from external audit bodies (e.g. ECoA) requiring follow-up actions by ENISA (i.e. number of 'critical', 'significant' or 'very important' findings
Build an agile organisation focused on people	Activity 11	Art 3(4)	ENISA as an employer of choice	Staff commitment, motivation and satisfaction	1. Staff satisfaction survey (incl attractiveness of ENISA as employer, staff empowerment, organisational culture, opportunities on internal mobility, work-space, -environment and -tools) 2. Quality of ENISA training and career development activities organised for staff 3. Reasons for staff departure (exit interviews) 4. Staff retention/turnover rates 5. Resilience and quality of ENISA IT systems and services

2. HUMAN AND FINANCIAL RESOURCE - OUTLOOK FOR YEARS 2021 – 2023

2.1 OVERVIEW OF THE PAST AND CURRENT SITUATION

This section will briefly indicate the evolution and explanatory reasons for the staff population, revenue and expenditure respectively.

With the enactment of the CSA both the staff numbers and the financial resources of the agency have grown, reflecting the expanded tasks and mandate of the Agency. The Agency has historically found it very hard to recruit and retain talent it sourly needs to fulfil its mandate, as the job-market for cybersecurity skills is highly specialised and extremely competitive. This 'deficiency' was reflected in the average occupancy rate of the Establishment Plan, which was 88.3% over the years 2017-2019. In turn, the unfulfilled posts have been a source of 'systemic surpluses' within the Agency's budget, requiring some amendments over the financial year, to absorb the funds unused for staff salaries.

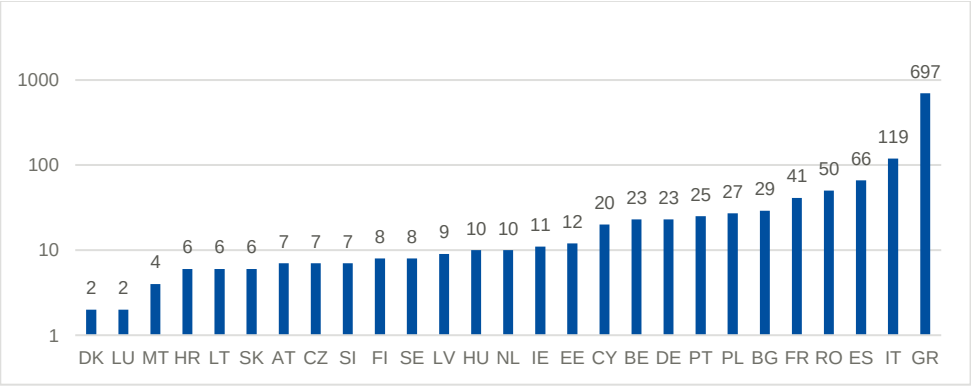
The occupancy rate of the Establishment Plan has been a cause for concern also for 2019 and 2020, owing to a number of factors including the mid-year enactment of CSA in 2019 which put a stress on recruitment, outbreak of the pandemic which has delayed the launch and conduct of recruitment operations in 2020 as well as the change of senior manager, development of new strategy for the Agency and the launch of reorganisation, all of which have complicated the process of defining the competences and talent the Agency requires to fulfil the new objectives and functions.

	2019	2020	2021	2022
Establishment plan posts	59	69		
Occupancy rate (%)	87%	75%*	n.a.	n.a.

*as of July 2020, expected to grow significantly by the end of the year

However, to overcome these challenges, the Agency in the beginning of 2020 embarked on wide scale novel recruitment exercise with an aim to create sufficiently diverse and wide single reserve list of 75 short-listed candidates with more transversal competences and skills which could be used for recruiting staff into grades AD6-AD8 and functions and thus fill the gaps in the current Establishment Plan, as well as to serve as pool of candidates for the establishment plan in 2021 and 2022 if necessary. The call, which was accompanied by a heavy promotion campaign, attracted 1235 candidates (who submitted more than 1600 applications) across all Member States (please see graph below), a result which is unprecedented in the history of the Agency and it has already yielded 69 candidates on reserve lists, recruitment from which has already been launched. This outcome needs to be added to the ongoing CA call, that attracted over 600 applications and is currently ongoing.

Graph: Origin of candidates of the 2020 TA call (AD6/AD7/AD8)



While gender balance in the Agency follows the trends in technology-dominated parts of the job market, the Agency pro-actively pursues gender balance in its general requests, with varying degrees of success. Agency staff citizenship is overbearing towards citizens of the Member State, as well as to a smaller extent citizens of neighbouring Member States. Again, the diversity of candidates in the ongoing call might bring some remedy and while geographical balance is a chronic issue; in the job market of the host Member State, ENISA represents a sound employer that has been proven to be reliable through the period of economic challenges in the Union. Overall the situation of the Agency is not that dissimilar from that of other Agencies.

Other information concerning appraisal of performance and reclassification/promotions, mobility policy, gender and geographical balance and schooling is provided in Annexes.

2.2 OUTLOOK FOR THE YEARS 2021 - 2023

In terms of evolution of tasks, the CSA sets new levels of performance and cooperation, which need to be met by the Agency's staff. Also, and as noted under Section I, the foreseen political and legislative developments place demand for the Agency to have the necessary skills and expertise to cater increasing needs in fulfilling its mandate in the field of operational cooperation, as well as international cooperation – both tasks which are relatively new to the Agency.

The overarching need to grow the Agency's capabilities, can be met either through (a) developing talent and measuring staff's performance, (b) recruiting new staff that possess the competences required to meet the requirements of the CSA.

For the purpose of competence development, the Agency has already experience in learning and development that continually produces outcomes in the areas of cybersecurity, project management, finance etc. the area of performance management currently covers annual appraisals, reclassification and the linking of appraisals with training needs. There is a need however to more concretely develop metrics for performance management and use information systems to this end, a process which has been kick-started with this SPD.

The shift in the profiles of newly recruited staff is also likely to lead to benefits for the Agency as it is expected that greater collaboration across agency verticals will be instigated. The drive towards interdisciplinary and social sciences based profiles, is likely to support the areas that the Agency expects to develop in the years to come.

Better retention rates have lowered the impact of staff turnover in the Agency and in combination with the outcome of the 2020 TA call, which has provided the agency with sufficient short-listed candidates to swiftly recruit it is thus anticipated that in the next years, payroll expenditure will become more predictable, as the Agency has historically implemented the Establishment plan as approved by the Budgetary Authority. The Agency has provided significant, albeit not balanced at all times, opportunities for reclassification to its staff.

While mobility in the Agency, has been a continual concern of management, several re-adjustments of its resources have taken effect over the course of the past few years; in a continual effort to seek the right balance between tasks and performance. It is expected that in 2020, the Agency will adapt its resources to the new environment set up by the CSA.

Breaking from the initial 3 management posts, in the past 8 years the Agency relied on a high number of management posts, which have allowed for broader distribution of tasks and possibly more targeted controls at the various stages of processing the Agency tasks. However, with the implementation of the new structure in 2021 the ratio of middle management is foreseen to decrease and stabilise from 8 to 6 middle management posts. It is hereby affirmed that the Executive Director is the senior manager of this Agency.

2.3 RESOURCE PROGRAMMING FOR THE YEARS 2021 – 2023

2.3.1 Financial Resources

The evolution of the planned total EU contribution for 2021-2023 as well as for the full period of the new Multiannual Financial Framework 2021-2027 is not yet available. As part of the CSA, the estimated impact

on expenditure was indicated for the period 2019-2022, which is presented in the table below. Average growth during 2019-2022 is expected to be at 12 %. Similar growth trend is expected for 2023.

In EUR thousand	2019	2020	2021	2022
Total appropriations for ENISA	16.550	21.683	23.433	24.227

95% of ENISA's revenue in 2019 was the EU contribution, 2% from the EFTA country contribution and 3% from other contributions (Table 1 in Annex III). A similar trend is expected for 2021-2023. The amount of EU contribution for 2021 is estimated to be EUR 22,3 million, the EFTA contribution is estimated at EUR 0,5 million and other contributions, mainly from Hellenic Authorities, is expected to be at EUR 0,6 million.

The general allocation of funds between titles is expected to remain at a similar level in 2021-2023 in comparison with 2019 (Table 2 in Annex III). Expenditure in 2020 is expected to be EUR 21,7 million, out of which EUR 11,2 million in Title 1 covering all staff related costs, EUR 3,2 million in Title 2 covering main items as building rental and ICT expenses, EUR 7,3 million in Title 3 covering all core operating expenditure.

.

2.4 STRATEGY FOR ACHIEVING EFFICIENCY GAINS

ENISA is committed to continuously implement measures to obtain efficiency gains in all activities. The new structure of the organisation, adopted and endorsed by its Management Board in June 2020, has been developed to specifically achieve and follow the principles of sound budgetary management and build efficiencies in both executing its core mandate as well as in fulfilling its corporate functions.

Within the domain of its operational activities, the Agency is revolutionising its approach in implementing its Work Programme in a way to ensure efficiencies and maximising its added value. Namely, it will seek to systematically use its statutory bodies (NLO Network, ENISA Advisory Group,), as well as other statutory groups ENISA is involved in (SCCG as set out in CSA Art. 22, NISD Cooperation Group and its work-streams, expert groups created under the Union law) and its own ad hoc expert groups, where appropriate to peer-review the scope and direction of actions undertaken to implement outputs, as well as validate the results. This way the Agency will fulfil its obligation is outlined in Article 3(3) of the CSA, to avoid the duplication of Member State activities and taking into consideration existing Member State expertise. Hence, all activities enlisted under section 3.1. and 3.2. in this SPD contain an indication of how specific deliverables and other actions undertaken to fulfil the outputs will be validated and peer-reviewed or consulted as per legal framework in the area of certification.

The Agency is also setting up a framework for structured cooperation with CERT-EU to utilise synergies and avoid duplication of activities in executing its task in the field of operational cooperation (Art 7 of the CSA). In addition, the establishment of local office in Brussels should enable the Agency to further create synergies with other EU Institutions, agencies and bodies within and beyond these activities. The Agency is also pursuing cooperation with relevant Union bodies (JRC) and will embark to create synergies with the Cybersecurity Competence Centre and Network once it is established to pursue synergies in fulfilling its tasks in the field of research and innovation (Article 11 of the CSA).

In its corporate functions, ENISA further seeks to rationalise its internal processes to improve its overall efficiency and to benchmark its activities with the best practices implemented by other EU Institutions and Agencies. The Agency is continuing and further expanding the sharing of services among other EU agencies. A number of collaborations and agreements are currently in place (EU-LISA; EUIPO) and the Agency in 2020 signed a service level agreement with CEDEFOP, which is also located in Greece, to enable further collaboration. This will include a pursuit to set up a joint compliance function and share procurement procedures.

Prompted by the COVID-19 crisis, the Agency is reviewing its digital and tele-working framework and will embark on actively seeking efficiency gains through digitalisation of its functions throughout all endeavours, including. It is already using the EU Tools such as ABAC; ABAC assets; Procurement; E-invoicing. Furthermore in 2020, the Agency deployed Sysper and is examining the migration of its services to other tools, such as MIPS, eRecrutiment etc. The Agency is using a basic workflow application called Paperless that made redundant

handwritten signatures for internal approvals. Most of the administrative tasks are already supported by the application Paperless and others that are significant steps for the aimed 100% e-administration.

E-trainings are also internally encouraged with the aim, among others, to reduce the associated costs from “class-room” training (traveling costs, etc…). However, with the COVID-19 the Agency will also review its trainings, conferences and seminars provided to external parties and will upgrade its capabilities to use secure digital conferencing across the field, providing further opportunities in efficiency gains as well as expanding the scale and scope of its activities.

SECTION III. WORK PROGRAMME YEAR 2021

This is the main body of the Work Programme describing, per operational and corporate activity, what the agency aims to deliver in the respective year towards achieving its strategy and the expected results. In total 9 operational activities and 2 corporate activities have been identified to support the implementation of ENISA's mandate in 2021.

3.1 OPERATIONAL ACTIVITIES

Activity 1 Providing assistance on policy development

OVERVIEW OF ACTIVITY

The activity delivers assistance and advice to the EU and Member States in developing cybersecurity policy and sector-specific policy and law initiatives where matters related to cybersecurity are involved.

The activity seeks to bolster policy initiatives on novel/emerging technology areas by providing technical, fact-driven and tailor-made cybersecurity advice and recommendations. In addition to support in emerging policy areas (such as AI, 5G and response to current and future crises), ENISA – in coordination with the EC and MSs - will also conduct policy scouting to support them in identifying potential areas in policy development, as well as develop monitoring capabilities and tools to regularly and consistently be able to give advice on the effectiveness of the existing Union policy and law works .

The added value of this activity is to support the decision makers in a timely manner on developments at the technological, societal or economic market level which affect the cybersecurity policy framework (see also Activity 8). Given the cross-cutting nature of cybersecurity across the policy landscape, the activity will provide an up-to-date risked based analysis of cybersecurity not only in the areas of critical infrastructure and sectors, but will provide advice across the field in an integrated and holistic manner.

The legal basis for this activity is Article 5 of the CSA.

OBJECTIVES

- Foster cybersecurity as an integral part of EU policy (existing and new)
- EU policy makers are regularly informed about the effectiveness of the existing framework EU policy makers and stakeholders are provided with timely and tailor-made policy recommendations on future cybersecurity challenges and opportunities

RESULTS	LINK TO STRATEGIC OBJECTIVE (ENISA STRATEGY)
Where relevant, support the Commission in ensuring that EU and national policies take into account cybersecurity aspects	Cybersecurity as an integral part of EU policies
OUTPUTS	**KPI**
1.1 Issue reports, studies and analysis on the effectiveness of the current cybersecurity policy framework in a requested area and the relevant best practices 1.2 Support the EC and MS with tailor-made advice and recommendations on new policy initiatives which tackle emerging technological, societal and economic trends 1.3 Assist the Commission in reviewing the NIS Directive	**Indicator:** ENISA's added value to EU institutions, bodies and Member States in providing support to policy-making (ex-ante) **Metric:** 1.1 . Number of relevant contributions to EU and national policies and legislative initiatives 1.2 Number of references to ENISA reports, analysis and/or in EU and national policy documents 1.3 Satisfaction with ENISA added-value and weight of contributions (survey) **Frequency:** Annual (1.1 and 1.2), bi-annual (1.3)
VALIDATION	**TARGET GROUPS AND BENEFICIARIES**
• Cooperation Group (NIS CG) (outputs 1.1. 1.2.) • ENISA ad hoc working groups[7] (output 1.2)	EU and national policy making institutions; EU and national experts (NIS CG, relevant/competent EU or MS-organisations/bodies)

[7] created under Art 20(4) of CSA

• NLO Network and ENISA Advisory Group (when necessary)	

RESOURCES PLANNED

Human Resources (FTE)			Financial Resources	EUR
Total	6		Total	280.000

Activity 2 Supporting implementation of Union policy and law

OVERVIEW OF ACTIVITY

The activity provides support to MS and EU Institutions in the implementation of European cybersecurity policy and legal framework and advice on specific cybersecurity aspects related to the NIS directive, telecom security and security of electronic communications, data protection, privacy, eID and trust services, incident notification and the general availability or integrity of the public core of the open internet. It further supports initiatives related to implementation of policy frameworks on novel digital technologies such as artificial intelligence, machine learning, internet of things etc. and networking technologies such as 5G (e.g. 5G security toolbox) and assisting the work of the Cooperation Group and its sectorial work streams. An ENISA contribution towards the Commission's regular monitoring of the implementation of specific EU policies is envisaged, which considers relevant indicators and could contribute to possible index which could capture the maturity of relevant cybersecurity policies

This activity helps to avoid fragmentation and supports a coherent implementation of Digital Single Market across Member States.

The legal basis for this activity is Article 5 and Article 6(1)b of CSA.

OBJECTIVES

- Align horizontal cyber security policies with sectorial polices to avoid implementation inconsistencies
- Contribute to the efficient and effective monitoring of EU cybersecurity policy implementation in MS
- Effective implementation of cybersecurity policy across the Union and approximation of MS laws, regulations and administrative provisions related to cybersecurity
- Improved cybersecurity practices taking on board lesson learned from incident reports

RESULTS	Link to strategic objective (ENISA STRATEGY)
• Consistent implementation of Union policy and law in the area of cybersecurity • EU cybersecurity policy implementation reflects sectorial specificities and needs • Exchange of good practice	• Cybersecurity as an integral part of EU policies • Empowered and engaged communities across the cybersecurity ecosystem

OUTPUTS	KPI
2.1 Support the NIS Cooperation Group and sectorial Work Streams as per NIS CG work programme 2.2 Support MS and Commission in the implementation of the 5G toolbox and its individual actions 2.3 Recommendations, technical guidelines and other activities to assist and support the implementation of the policies within NISD sectors, in the area of trust services and electronic identity, under the EECC and its implementing acts, in the field of privacy and data protection and artificial intelligence 2.4 Assisting in establishing and implementing vulnerability disclosure policies. 2.5 Analyse and report on incidents as required by Art 5(6) of CSA	**Indicator:** Contribution to policy implementation and implementation monitoring at EU and national level (ex-post) **Metric:** 2.1 Number of EU policies and regulations implemented at national level supported by ENISA 2.2 Number of ENISA reports, analysis and/or studies referred to at the EU and national level (survey) 2.3 Satisfaction with ENISA added-value and weight of support (survey) **Frequency:** Annual (1), bi-annual (2 and 3)

VALIDATION	TARGET GROUPS AND BENEFICIARIES
• Art 13a expert group (for related activities under output 2.3.) • Art19 expert group (for related activities under output 2.3.) • NIS CG or established sectorial work streams (output 2.1. and 2.2.) • NLO Network (as necessary)	• Art. 13a EG, Art. 19 EG • Citizens • Conformity Assessment Bodies • Data Protection Authorities • EC, EU Institutions/ bodies (e.g.. BEREC) • MS cybersecurity authorities (NISD CG members) • Supervisory Authorities • Trust Service Providers • European ISACs

RESOURCES PLANNED

Human Resources (FTE)			Financial Resources	EUR
Total	14		**Total**	985.000

Activity 3 Building capacity

OVERVIEW OF ACTIVITY

This activity seeks to improve and develop the capabilities of Member States, Union Institutions, bodies, and agencies, as well as various sectors, to respond to cyber threats and incidents, raise resilience and increase preparedness across the Union. Actions to support this activity include organising large scale exercises, sectorial exercises and trainings, including CSIRT trainings. In addition the activity seeks to develop and raise CSIRT capabilities, support information sharing within the cybersecurity ecosystem and assist in reviewing and developing national and Union level cybersecurity strategies, including cross-border.

The legal basis for this activity is Articles 6 and 7(5) of the CSA.

OBJECTIVES

- Increase the level of preparedness and cooperation within and between Member States and sectors and EU institutions, bodies and agencies
- Prepared and tested capabilities to respond to cybersecurity incidents
- Foster interoperable European risk management, consistent methodology and risk assessment practices
- Increase skill sets and align cybersecurity competencies
- Increase the supply of skilled professionals to meet market demand, incl supporting the necessary educational structures

RESULTS	Link to strategic objectives (ENISA STRATEGY)
• Enhanced capabilities across the community • increased cooperation between communities	• Cutting-edge competences and capabilities in cybersecurity across the Union • Empowered and engaged communities across the cybersecurity ecosystem

OUTPUTS	KPI
3.1 Assist MS to develop National Cybersecurity Strategies 3.2 Organise large scale bi-annual exercises and sectorial exercises (incl Cyber Europe, BlueOLEx, CyberSOPEx etc) 3.3 Organise trainings and other activities to support and develop maturity and skills of CSIRT (incl. NISD sectorial CSIRT) and other communities 3.4 Develop coordinated and interoperable risk management frameworks 3.5 Support the capacity building activities of Cooperation Group and sectorial Work Streams as per NIS CG work programme 3.6 Support the establishment, development and cooperation of European Information Sharing schemes based on ISACs, PPPs, and other existing mechanisms. 3.7 Organise European cybersecurity challenge (ECSC) 3.8 Report on cybersecurity skills needs and gaps, and support skills development, maintenance and implementation (incl. Digital Education Action Plan and a report on higher-education programmes)	**Indicator:** increased resilience against cybersecurity risks and preparedness to respond to cyber incidents **Metric:** 3.1 Increase/decrease of maturity indicators 3.2 Outreach, uptake and application of lessons learned from capability-building activities. 3.3 Number of cybersecurity programmes (courses) and participation rates 3.4 Stakeholder assessment on usefulness, added value and relevance of ENISA capacity building activities. (Survey) **Frequency:** 1, 2 & 3 Annual, 4 Bi-annual

VALIDATION	TARGET GROUPS AND BENEFICIARIES
• NLO Network (as necessary) • CSIRTs Network, (output 3.3.) • Cooperation Group (output 3.6)	• Cybersecurity professionals • EU Institutions • Operational communities • Private industry sectors (health, transport etc.) CSIRTs Network • European ISAC

RESOURCES PLANNED

Human Resources (FTE)			Financial Resources	EUR
Total	15		**Total**	1.400.000

Activity 4 Enabling operational cooperation

OVERVIEW OF ACTIVITY

The activity supports operational cooperation among Member States, Union institutions, bodies, offices and agencies and between operational activities. Actions include establshing synergies with national and EU actors including CERT-EU with the view to exchange know how, best practices, provide advice and issue guidance.

In addition the activity supports Member States with respect to operational cooperation within the CSIRTs network by advising on how to improve capabilities and providing support to ex-post technical inquiries regarding incidents.

Under this activity ENISA is supporting operational communities through helping to develop and maintain networks / IT platforms and communication channels

The legal basis for this activity is Article 7 of the CSA.

OBJECTIVES

- Enhance and improve incident response capabilities across the Union
- Enable effective incident response and cooperation amongst Member States and EU institutions (incl via Blueprint)
- Improve maturity and capacities of operational communities (incl CSIRTs network, CyCLONe group)

RESULTS	Link to strategic objectives (ENISA STRATEGY)
• All communities (EU Institutions and MS) use a rationalised set of SOPs • An agreed CSIRTs Network approach for selecting, operating and decommissioning tools • Coherent SOPs for cyber crises management • Efficient framework, tools and methodologies for effective cyber crisis management	• Effective cooperation amongst operational actors within the Union in case of massive cyber incidents • Empowered and engaged communities across the cybersecurity ecosystem

OUTPUTS	KPI
4.1. Support the functioning and operations of the CSIRTs Network (also through MeliCERTes), CyCLONe group and Cyber Crisis Management in the EU 4.2. Activities to support the development, implementation and evolution of MoU between ENISA, Europol, CERT-EU and EDA 4.3. Develop standard operating policies, procedures, methodologies and tools for cyber crisis management	**Indicator:** Effective use of ENISA's tools, platforms and take up of SOPs in operational cooperation **Metric:** 4.1Number of users both new and recurring and usage per platform/ tool/ SOPs provided by ENISA 4.2 Uptake of the platform/ tool/ SOPs during massive cyber incidents 4.3 Stakeholder satisfaction on the relevance and added value of the platforms/ tools/ SOPs provided by ENISA. (Survey) 4.4 **Frequency:** 1 & 2 annual and 3 bi-annual

VALIDATION	TARGET GROUPS AND BENEFICIARIES
• Management Board (output 4.2.) • NLO Network (as necessary) • CSIRTs Network and CyCLONe group (output 4.1.)	• Blueprint stakeholders • EU decision makers, institutions, agencies and bodies • MS CSIRTs Network Members • NISD Cooperation Group • OESs and DSPs

RESOURCES PLANNED

Human Resources (FTE)			Financial Resources	EUR
Total	8		**Total**	1.110.000

Activity 5 Contribute to cooperative response at Union and Member States level

OVERVIEW OF ACTIVITY

The activity contributes to developing a cooperative response at Union and Member States level to large scale cross border incidents or crises related to cybersecurity by aggregating and analyzing reports to establish a common situational awareness, ensuring information flow and escalation measures between CISRTs network and technical, operational and political decision makers at Union level .

In addition, at the request of Member states facilitate handling of incident or crises, public communication related to such incidents or crisis and testing cooperation plans for such incidents or crisis. Supporting Union institutions, bodies, offices and agencies in public communication to incidents and crises. The activity also supports Member States with respect to operational cooperation within the CSIRTs network by providing advice to a specfic cyber threat, assisting in the assessment of incidents, faciliting technical handling of incidents, supporting cross-border information sharing and analyzing vulnerabilities.

Moreover the activity seeks to engage with CERT-EU in structured cooperation.

The legal basis for this activity is Article 7 of the CSA

OBJECTIVES

- Effective incident response and cooperation amongst Member States and EU institutions, incl cooperation of technical and political actors during incidents or crisis
- Common awareness on cyber incidents and crisis across the Union
- Information exchange and cooperation, cross layer and cross border between Member States and as well as with EU institutions
-

RESULTS	Link to strategic objectives (ENISA STRATEGY)
• Member States and institutions cooperating effectively during large scale cross border incidents or crises • Public informed on a regular basis of important cybersecurity developments • Stakeholders aware of current cybersecurity situation	• Effective operational cooperation within the Union in case of massive cyber incidents • Empowered and engaged communities across the cybersecurity ecosystem
OUTPUTS	**KPI**
5.1. Generate and consolidate information (incl to the general public) on cyber situation awareness, technical situational reports, incident reports, threats and support consolidation and exchange of information on strategic, tactical and technical levels 5.2. Support technical and operational cooperation, incident response coordination during crisis and activities with the CSIRT Network and CERT-EU, EC3, EEAS and EDA EU wide crisis communication planning 5.3. Providing assistance and support on the basis of Art 7(4) and (7) of CSA	**Indicator:** ENISA ability to support response to massive cyber incidents **Metric:** 5.1 Timeliness and relevance of information shared and expertise provided by ENISA in relation to incidents ENISA contributes to mitigate (Survey) 5.2 Stakeholders' satisfaction of ENISA's ability to provide operational support (Survey) **Frequency:** 1 & 2 bi-annual
VALIDATION	**TARGET GROUPS AND BENEFICIARIES**
• Blueprint actors	• EU Member States (incl CSIRTs Network members) • EU Institutions, bodies and agencies • Other type of CSIRTs and PSIRTs

RESOURCES PLANNED

Human Resources (FTE)			Financial Resources	EUR
Total	8		**Total**	1.200.000

Activity 6 Development and maintenance of EU cybersecurity certification framework

OVERVIEW OF ACTIVITY

This activity emcompasses actions to developdraft candidate cybersecurity certification schemes to impement the EU cybersecurity certification framework. The Agency takes action in line with Article 49 of the CSA, at the request of the Commission or on the basis of the Union Rolling Work Program. Actions also include evaluating adopted certification schemes (such as schemes for common criteria and cloud services once adopted) and participating in peer reviews. In addition the activity assists the Commission in the ECCG, co-chairing and supporting the secretariat of the SCCG and maintaining a dedicated European cybersecurity certification website.

The legal basis for this activity is Article 8 and Title III Cybersecurity certification framework of the CSA.

OBJECTIVES

- Trusted ICT products, services and processes
- Increase use and uptake of European cybersecurity certification

RESULTS	Link to strategic objectives (ENISA STRATEGY)
• Support for schemes chosen to run under the European cybersecurity certification framework • Certified ICT products, services and processes are preferred by consumers and where relevant, Operators of Essential Services or Digital Service Providers	• High level of trust in secure digital solutions • Empowered and engaged communities across the cybersecurity ecosystem

OUTPUTS	KPI
6.1. Draft candidate cybersecurity certification schemes and contribute to the establishment of the schemes. 6.2. Implementation and maintenance of the established schemes including evaluation of adopted schemes, participation in peer review etc 6.3. Support the statutory bodies in discharging their duties with respect to governance roles and tasks 6.4. Development and maintenance of necessary tools for efficient and effective Union cybersecurity certification framework (incl certification website and collaboration platform)	**Indicator:** 1. Uptake of the European cybersecurity certification framework and schemes as an enabler for secure digital solutions. 2. Effective preparation of candidate certification schemes prepared by ENISA **Metric:** 6.2 Number of stakeholders (governments or commercial solution providers) on the EU market using the cybersecurity certification framework for their digital solutions 6.3 Citizens' trust in digital solutions. (Survey) 6.4 Satisfaction with ENISA's support in the preparation of candidate schemes (survey) **Frequency:** 1 annual, 2 and 3 bi-annual

VALIDATION	TARGET GROUPS AND BENEFICIARIES
• Ad hoc certification expert groups (output 6.1.) • ECCG (6.1.-6.2.) • European Commission (outputs 6.1.-6.3) • SCCG (output 6.3. and 6.4.)	• Accreditation Bodies at Member States & EU level, Certification Supervisory Authorities, Conformity Assessment Bodies, • Product manufacturers and service providers who have an interest in EU schemes for the certification of ICT products and services (industry) • The European Commission, other Institutions, Agencies and competent authorities (e.g. EDPB), public authorities in the Member States, the members of the ECCG and the SCCG

RESOURCES PLANNED

Human Resources (FTE)			Financial Resources	EUR
Total	12		**Total**	870.000

Activity 7 Supporting European cybersecurity market and industry

OVERVIEW OF ACTIVITY

The activity seeks to foster cybersecurity market in the Union and the development of the cybersecurity industry, in particular SMEs and start-ups, to reduce dependence from outside the Union and to reinforce supply chains inside the Union. It involves actions to promote and implement 'security by design' and 'security by default' measures in ICT products, services and processes, including through standardisation. Actions to support this activity include compiling guidelines and good practices on cybersecurity requirements, facilitating the establishment and take up of European and international standards for risk management and perform regular analysis of cybersecurity market trends on both the demand and supply sides and monitoring, collecting and identifying dependencies or vulnerabilities used or integrated into ICT products or services.

In addition this activity supports cybersecurity certification by monitoring developments in standards to be applied in the evaluation of certification schemes and recommending appropriate technical specifications for the use in the development of certification schemes where standards are not available.

The legal basis for this activity is Article 8 and Title III Cybersecurity certification framework of the CSA.

OBJECTIVES

- Improve the conditions for the functioning of the internal market
- Foster a robust European cybersecurity industry and market

RESULTS	Link to strategic objectives (ENISA STRATEGY)
• Where relevant, contribution towards a more competitive European cybersecurity industry, SMEs and start-ups	• High level of trust in secure digital solutions • Empowered and engaged communities across the cybersecurity ecosystem

OUTPUTS	KPI
7.1. Market analysis on the main trends in the cybersecurity market on both the demand and supply side 7.2. Monitoring developments in related areas of standardisation, analysis on standardisation gaps and establishment and take-up of European and international standards for risk management. 7.3. Guidelines and good practices on cybersecurity certification requirements for ICT products, services and processes 7.4. Monitoring and documenting the dependencies and vulnerabilities of ICT products and services.	**Indicator:** Recognition of ENISAs supporting role for participants in the European cybersecurity market **Metric:** 7.1 Number of market analysis, guidelines and good practices issued by ENISA 7.2 Uptake of lessons learnt / recommendations from ENISA reports 7.3 Stakeholder satisfaction with the added value and quality of ENISA's wo (Survey) **Frequency:** 1,2 annual and 3 bi-annual

VALIDATION	TARGET GROUPS AND BENEFICIARIES
• SCCG (outputs 7.2. & 7.3.) • ENISA Advisory Group (output 7.1.) • NLO (as necessary)	• European ICT industry, SME's, start-ups, product manufacturers and service providers • European standardisation organisations (CEN, CENELEC and ETSI) as well as international and industry standardisation organisations

RESOURCES PLANNED

Human Resources (FTE)			Financial Resources	EUR
Total	9		**Total**	490.000

Activity 8 Knowledge on emerging cybersecurity challenges and opportunities

OVERVIEW OF ACTIVITY

This activity shall provide strategic long-term analysis, guidance and advice on emerging technologies (such as in the area of artifitial intelligence, quantum, distributed ledgers, cloud computing, edge computing, software development, etc), cyber threats and threat landscapes, vulnerabilities and risks, and provides topic-specific as well as general assessments on the expected societal, legal, economic and regulatory impact, as well as targeted recommendations to Member States and Union institutions, bodies, offices and agencies. The activity also seeks to identify and give advice on research and innovation needs and priorities in the field of cybersecurity, and contribute to strategic agenda setting for cybersecurity research and innovation. To this end, as part of this activity relevant EU programmes will be assessed (e.g. Horizon Europe Programme).

These activities leverage on expertise of relevant legal, regulatory, economic and society trends and data by aggregating and analysing information.

The legal basis for this activity is Article 9 and Article 11 of the CSA.

OBJECTIVES

- Identify and understand future cybersecurity challenges and opportunities and assess the interlinks between cybersecurity and relevant disrupting technologies in current and future digital transformation
- Increase Member States' and Union's resilience and preparedness in handling future cybersecurity challenges and opportunities
- Increase knowledge and information for specialised cybersecurity communities

RESULTS	Link to strategic objectives (ENISA STRATEGY)
• Decisions about cybersecurity are future proof and take account of the trends, developments and knowledge across the ecosystem • Stakeholders receive relevant and timely information for policy and decision-making	• Foresight on emerging and future cybersecurity challenges • Efficient and effective cybersecurity information and knowledge management for Europe • Empowered and engaged communities across the cybersecurity ecosystem

OUTPUTS	KPI
8.1 Identification, collection and analysis of present and emerging challenges (ex: technological, economic or societal) in cybersecurity (incl developing and maintaining a European Cybersecurity Index) 8.2 Provide targeted as well as general reports, recommendations, analysis and other actions on future cybersecurity scenarios and threat landscapes (incident response landscape mapping for NISD sectors). 8.3 Develop and maintain a portal (information hub), a one stop shop to organise and make available to the public information on cybersecurity, and establishment of procedural framework to support knowledge management activities 8.4 Support EU research & development programmes and activities of European competences centres, including the 4 EU pilot projects for the European Cybersecurity Competence Network.	**Indicator:** ENISA's ability to contribute to Europe's cyber resilience through timely and effective information and knowledge **Metric:** 8.1 Number of users and frequency of usage of dedicated portal (observatory) 8.2 Number of recommendations, analysis, challenges identified and analysed 8.3 Stakeholder satisfaction on the usefulness, relevance and timeliness of ENISA's foresight and advice on cybersecurity challenges & opportunities incl in research (Survey) **Frequency:** 1 & 2 annual, 3 b-annual

VALIDATION	TARGET GROUPS AND BENEFICIARIES
• NLO Network • ENISA Advisory Group (as necessary) • ENISA ad hoc working group (as necessary) • The forthcoming European Cybersecurity Competence Center and Network of National Coordination Centers	• General public • Industry, research and academic institutions and bodies • EU and national decision making bodies and authorities • European Cybersecurity Competence Centre & Network

RESOURCES PLANNED

Human Resources (FTE)			Financial Resources	EUR
Total	9		**Total**	1.155.000

Activity 9 Outreach and education

OVERVIEW OF ACTIVITY

The activity seeks to raise the overall awareness of cybersecurity risks and practices. in cooperation with Member States, Union institutions, bodies, offices and agencies and EU's international partners, it aims to build an empowered global community which can counter those risk in line with the values of the Union. Under this activity the Agency will be organising regular outreach campaigns, providing guidance on best practices and support coordination across MS on awareness and education.

The added value of this activity comes from building global communities of stakeholders which improve and enhance current practices in cybersecurity by harmonizing and amplifying stakeholder actions.

The activity will also seek to contribute to the Unions efforts to cooperate with third countries and international organisations on cybersecurity.

The legal basis for this activity are Articles 10 and 12 and Article 42 of the CSA.

OBJECTIVES

- Elevate the understanding of cybersecurity risks and practices across the EU and globally
- Foster EU cybersecurity values and priorities

RESULTS	Link to strategic objectives (ENISA STRATEGY)
• Greater understanding of cybersecurity risks and practices • Stronger European cybersecurity through higher global resilience	• Empowered and engaged communities across the cybersecurity ecosystem

OUTPUTS	KPI
9.1 Develop ENISA stakeholder strategy and undertake actions for its implementation 9.2 Develop ENISA international strategy and outreach 9.3 Organise European cybersecurity month (ECSM) 9.4 Organise International Cybersecurity Challenge 9.5 Activities to promote and ensure uptake of information on good cybersecurity practices (incl on Union strategies, security by design and privacy by design at Union level, cybersecurity certification schemes) throughout different target groups.	**Indicator:** Level of awareness on cybersecurity, cyber hygiene and cyber literacy across the EU **Metric:** 9.1 Number of activities and participation in awareness raising actions organised by ENISA on cybersecurity topics 9.2 Level of awareness on cybersecurity across the EU/ general public (e.g. EU barometer) **Frequency:** 1 annual, 2 bi-annual

VALIDATION	TARGET GROUPS AND BENEFICIARIES
• Management Board (for output 9.1. and 9.2.) • SCCG (for certification related issues under output 9.5) • NLO Network • ENISA Advisory Group (outputs 9.1. and 9.5.)	• Public, businesses and organisations • Member States, EU institutions, bodies and agencies • International partners

RESOURCES PLANNED

Human Resources (FTEs)			Financial Resources	EUR
Total	6		Total	1.010.000

1.2 CORPORATE ACTIVITIES

Activities 10 to 11 encompass enabling actions that support the operational activities of the agency.

Activity 10: Performance and risk management

OVERVIEW OF ACTIVITY

The activity seeks to achieve requirements set out in Art 4(1) of the CSA that sets an objective for the Agency to: "be a centre of expertise on cybersecurity by virtue of its **independence**, the scientific and technical **quality of the advice and assistance it delivers**, the information it provides, the **transparency of its operating procedures**, the **methods of operation**, and its **diligence in carrying out its tasks**". This objective requires an efficient performance and risk management framework, which should be developed and implemented hand in hand with the imposition of the new organisational setup.

Under this activity ENISA will continue to enhance key objectives of the reorganisation, as described in the MB decision No MB/2020/5, including the need to adress the gaps in the Agency's quality assessment framework, install proper and functioning internal controls and compliance checks, make best use of the internal resources of the Agency, impose of sound financial and budgetary management, and utilise internal and external synergies within ENISA. These aspects are addressed in the new organisational architecture, but should also be built into the daily operations of the Agency as guided by the Work Programme. Actions undertaken will ensure that Agency's outputs add real value, through making performance and ex-post and ex-ante evaluation integral to the Work Programme througout its lifecycle, including by rigorous quality assurance through proper project management, internal peer-reviews and independent audits and validations.

The legal basis for this activity is Art 4(1) and Art 32 of the CSA, the latter of which strongly focuses on the sound financial management principle with a view to maximise value for money.

OBJECTIVES

- Increased effectiveness and efficiency in achieving Agency objectives
- To be fully compliant with legal and financial frameworks in our performance (build a culture of compliance)
- Protect the Agencies assets and reputation, while reducing risks

RESULTS	Link to corporate objective:
Maximize value for money provided to stakeholders and citizens Building lasting credibility and trust	Sound resource and risk management

OUTPUTS	KPI
10.1. Roll out of agency wide performance management framework and systems across its functions 10.2. Develop, establish and implement risk management plan and systems, incl Anti-Fraud Strategy, conflict of interest policy, whistleblowing policy, Information Security policy, anti-harassment policy, IPR policy etc. 10.3. Developing and implementing Agency wide IT strategy 10.4. Carry out relevant trainings and develop guidelines to staff	**Indicator**: Organisational performance culture **Metrics:** 10.1 Proportion of KPI's reaching targets 10.2 Individual contribution to achieving the objectives of the agency via clear link to KPI's (CDR report) 3. Exceptions in Risk Register 4. Number of complaints filed against ENISA incl number of inquiries/ complaints of the EU Ombudsman 5. Results of annual risk assessment exercise 6. Observations from external audit bodies (e.g. ECoA) requiring follow-up actions by ENISA (i.e. number of 'critical', 'significant' or 'very important' findings **Frequency:** Annual

VALIDATION	TARGET GROUPS AND BENEFICIARIES
• Management Team • Budget Management Committee • IT Management Committee • IPR Management Committee • Staff Committee • ENISA Ethics Committee	• Citizens • All stakeholders of the Agency

Activity 11 Staff development and working environment

OVERVIEW OF ACTIVITY

This activity seeks to support ENISA aspirations as stipulated in Art 3(4) which obliges the Agency to: "*develop its own resources, including /…/ human capabilities and skills, necessary to perform the tasks assigned to it under this Regulation*".

Moreover, with the COVID-19 pandemic, the number of organisations who have announced permanent teleworking options, has grown globally. This must accelerate a review of the employer-employee relationships in the Agency, with a view of introducing a more flexible (50/50) framework while maintaining and enhancing employee motivation, efficiency and development, an option which was supported by 87% of respondents of the staff survey conducted in June 2020.

The actions which will be pursued under this activity will focus on attracting retaining and developing talent and building ENISA's reputation as employer of choice and as an agile and knowledge based organisation where staff can evolve personally and professionaly, keeping staff engaged, motivated and with sense of beloging. The activity will seek to build an attractive workspace by establishing and maintain excellent working conditions (premises, layout of office space) and developing user-centric (tele)working and conferencing tools (incl IT systems and platfoms) delivering state of the art services and supporting ENISA's business owners and stakeholders in line with the Agency's objectives.

OBJECTIVES

- Engaged staff, committed and motivated to deliver, empowered to use fully their talent, skills and competences
- Digitally enabled work-place and environment (incl home work-space) which cultivates and nourishes performance and enhances social and environmental responsibility

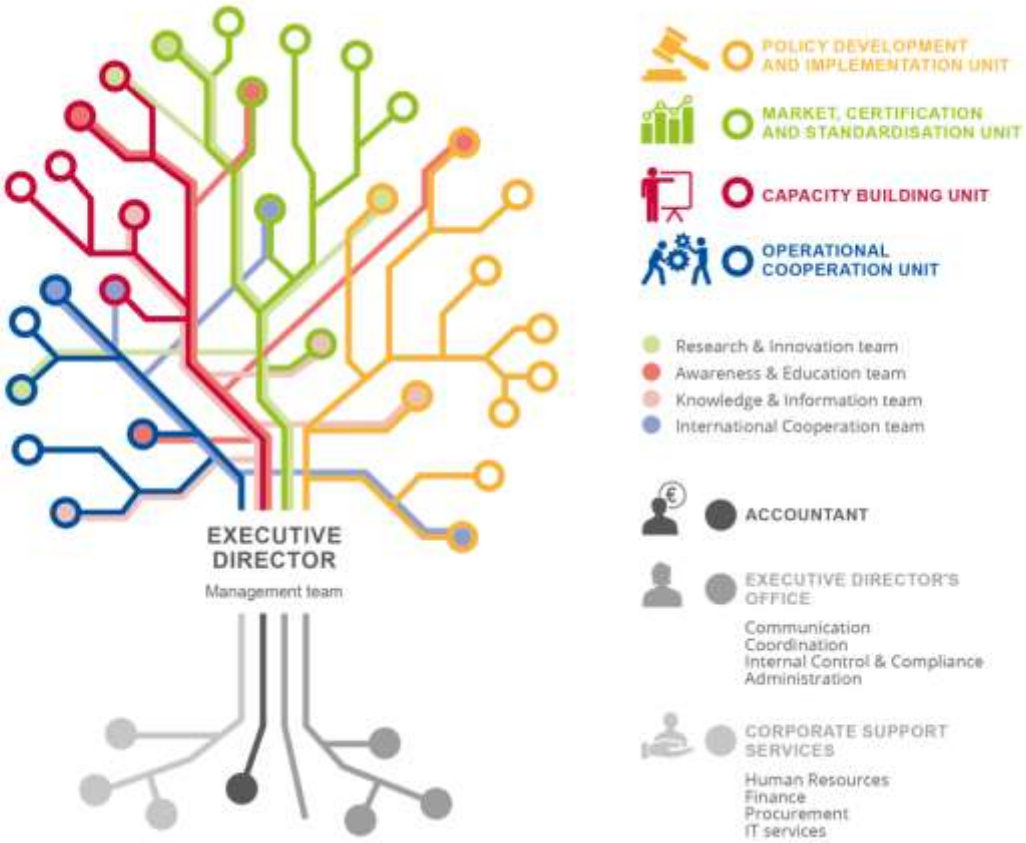
RESULTS	Link to corporate objective:
ENISA as an employer of choice	Build an agile organisation focused on people

OUTPUTS	KPI
11.1. Implement the competence framework (incl into training strategy, CDR, internal competitions, exit-interviews etc) 11.2. Actions to develop and nourish talent (in line with output 11.1) 11.3. Undertake actions to support digital working environment and develop necessary tools and services in line with objective 10.3 11.4. Planning, preparing and executing the establishment of the Agency's HQ to its new premises in line with the objectives of the activity	**Indicator** Staff commitment, motivation and satisfaction **Metric**: 11.1 Staff satisfaction survey (incl attractiveness of ENISA as employer, staff empowerment, organisational culture, opportunities on internal mobility, work-space, -environment and -tools) 11.2 Quality of ENISA training and career development activities organised for staff 11.3 Reasons for staff departure (exit interviews) 11.3Staff retention/turnover rates 11.5 Resilience and quality of ENISA IT systems and services **Frequency**: Annual (or ad hoc for metric no 3)

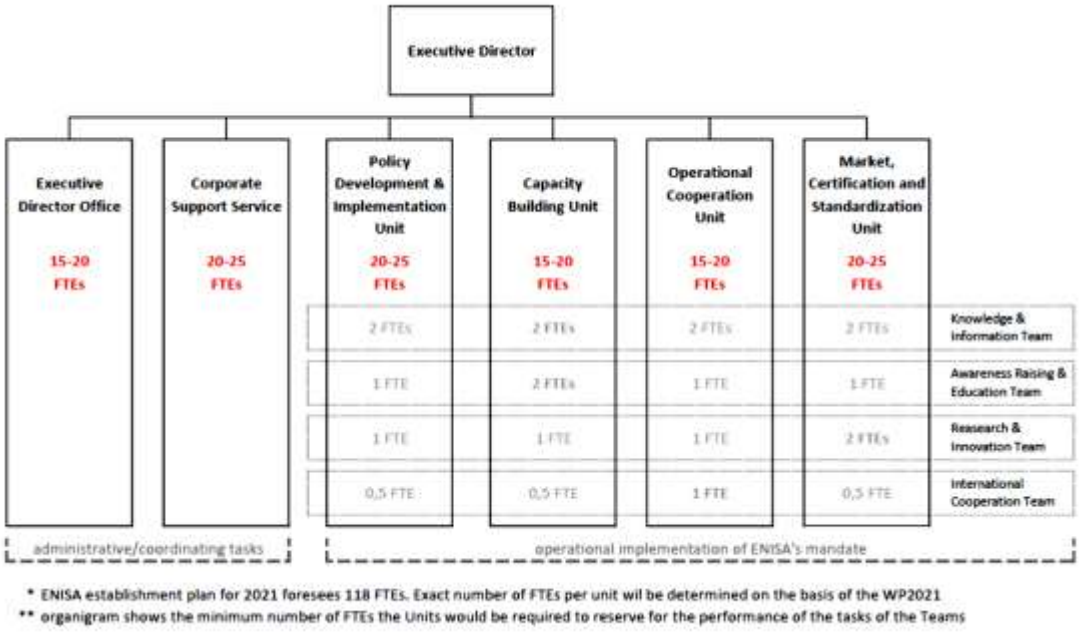
VALIDATION	TARGET GROUPS AND BENEFICIARIES
• Management Team • Joint Reclassification Committee • IT Management Committee • Task Force on relocation of the Agency • Staff Committee	• ENISA staff members and employees

ANNEX A

I. ORGANISATION CHART AS OF 01.01.2021



Administrative Organigramme



* ENISA establishment plan for 2021 foresees 118 FTEs. Exact number of FTEs per unit wil be determined on the basis of the WP2021
** organigram shows the minimum number of FTEs the Units would be required to reserve for the performance of the tasks of the Teams

II. RESOURCE ALLOCATION PER ACTIVITY 2021 - 2023

The allocation of the total 2021 financial and human resources following the activities as described in part 3.1 in Section III and the corporate activities as described in part 3.2 in Section III are presented in the table[8] below. The allocation has been done following direct budget and FTEs indicated for each activity with indirect budget being assigned based on causal relationships.

The following assumptions are used in the simplified ABB methodology:

- Direct Budget is the cost estimate of each of the 9 operational activities as indicated under Section 3.1 of the SPD 2021-2023 (carried out under Articles 5-12) in terms of goods and services to be procured.
- Indirect Budget is the cost estimate of salaries and allowances, mission costs, buildings, IT, equipment and miscellaneous operating costs, attributable to each activity. The indirect budget is allocated to activities based on different drivers. Main driver for costs allocation was number of foreseen FTEs for each operational activity in 2021.
- For the purpose of allocation of human and financial resources, ED Office activity (budget and FTEs) which includes coordination, compliance, communication, and administration executed by 15 FTEs has been allocated for all Agency's activities.
- For the purpose of allocation of human and financial resources Corporate Support Service activity including HR, IT services, procurement and finance, facilities and logistics activity was created.

[8] Pending final review

		2021		2022		2023	
Allocation of human and financial resources	**Activities as referred to in Section 3.1**	**Full budget allocation (in EUR)**	**Full FTE allocation**	**Full budget allocation (in EUR)**	**Full FTE allocation**	**Full budget allocation (in EUR)**	**Full FTE allocation**
Providing assistance on policy development	Activity 1	1.309.867,31	8,14	1.636.062,06	8,96	1.636.062,06	8,96
Supporting implementation of Union policy and law	Activity 2	3.388.023,72	18,99	3.874.144,81	20,91	3.874.144,81	20,91
Building capacity	Activity 3	3.974.668,28	20,34	5.015.155,16	22,41	5.015.155,16	22,41
Enabling operational cooperation	Activity 4	2.483.156,41	10,85	1.555.051,72	7,47	1.555.051,72	7,47
Contribute to cooperative response at Union and Member States level	Activity 5	2.573.156,41	10,85	2.414.093,09	13,44	2.414.093,09	13,44
Development and maintenance of EU cybersecurity certification framework	Activity 6	2.929.734,62	16,28	3.572.124,13	17,93	3.572.124,13	17,93
Supporting European cybersecurity market and industry	Activity 7	2.034.800,97	12,21	1.908.187,71	8,96	1.908.187,71	8,96
Knowledge on emerging cybersecurity challenges and opportunities	Activity 8	2.699.800,97	12,21	2.137.072,41	10,46	2.137.072,41	10,46
Outreach and education	Activity 9	2.039.867,31	8,14	2.115.172,41	10,46	2.115.172,41	10,46
TOTAL		**23.433.076,00**	**118,00**	**24.227.063,50**	**121,00**	**24.227.063,50**	**121,00**

III. FINANCIAL RESOURCES 2021 - 2023

Table 1: Revenue

Revenues	2020 *	2021
	Revenues estimated by the agency	Revenues estimated by the agency
EU contribution	20.646.000	22.248.000
Other revenue	1.036.884	1.185.076
Total revenues	**21.682.884**	**23.433.076**

* as adopted in the Amending Budget 1/2020 (MB Decision No MB/2020/18)

REVENUES	2019 Executed Budget	2020 Revenue estimated by the agency *	2021 As requested by the agency	VAR 2021 / 2020	Envisaged 2022	Envisaged 2023
1 REVENUE FROM FEES AND CHARGES						
2 EU CONTRIBUTION	15.400.829	20.646.000	22.248.000	8%	23.023.000	23.023.000
- of which assigned revenues deriving from previous years' surpluses **	*-85.534,89*	*-110.505,47*	*-579.112,99*	524%		
3 THIRD COUNTRIES CONTRIBUTION (incl. EEA/EFTA and candidate countries)	370.696	503.120	545.076	8%	564.064	564.064
- of which EEA/EFTA (excl. Switzerland)	370.696	503.120	545.076	8%	564.064	564.064
- of which Candidate Countries						
4 OTHER CONTRIBUTIONS	435.844	533.764	640.000	0%	640.000	640.000
5 ADMINISTRATIVE OPERATIONS						
- of which interest generated by funds paid by the Commission by way of the EU contribution (FFR Art. 58)						
6 REVENUES FROM SERVICES RENDERED AGAINST PAYMENT						
7 CORRECTION OF BUDGETARY IMBALANCES						
TOTAL REVENUES	**16.207.370**	**21.682.884**	**23.433.076**	**8%**	**24.227.064**	**24.227.064**

* as adopted in the Amending Budget 1/2020 (MB Decision No MB/2020/18)

** The 2019 surplus (as indicated under column 2021 request by the agency) has increased by more than 5 times the amount of previous year (+524%) which can partially be explained by the late adoption in June 2019 of ENISA's new mandate (the CyberSecurity Act) resulting in the delay of the 2019 implementation of deliverables which has negatively impacted by domino's effect the 2020 budget. Furthermore, with its renewed mandate, ENISA was conferred greater competences but as well greater financial resources multiplying almost by a factor of two its budget in less than three years period.

Table 2: Expenditure

EXPENDITURE	2020 *		2021	
	Commitment appropriations	Payment appropriations	Commitment appropriations	Payment appropriations
Title 1	11.203.334	11.203.334	10.775.409	10.775.409
Title 2	3.150.568	3.150.568	3.507.667	3.507.667
Title 3	7.328.981	7.328.981	9.150.000	9.150.000
Total expenditure	**21.682.884**	**21.682.884**	**23.433.076**	**23.433.076**

* as adopted in the Amending Budget 1/2020 (MB Decision No MB/2020/18)

EXPENDITURE (in EUR)	Commitment and Payment appropriations *					
	Executed budget 2019	Budget 2020 **	Draft Budget 2021 Agency request	VAR 2021 / 2020	Envisaged in 2022	Envisaged in 2023
Title 1. Staff Expenditure	**7.458.310**	**11.203.334**	**10.775.409**	**-4%**	**11.245.821**	**11.245.821**
11 Staff in active employment	5.627.276	7.126.084	8.810.319	24%	9.107.970	9.107.970
12 Recruitment expenditure	254.762	704.686	410.087	-42%	423.982	423.982
13 Socio-medical services and training	222.200	375.738	1.084.064	189%	1.120.796	1.120.796
14 Temporary assistance	1.354.073	2.996.826	470.939	-84%	593.073	593.073
Title 2. Building, equipment and miscellaneous expenditure	**4.346.742**	**3.150.568**	**3.507.667**	**11%**	**3.013.739**	**3.013.739**
20 Building and associated costs	783.366	929.820	1.364.624	47%	1.867.710	1.867.710
21 Movable property and associated costs	45.391	54.074	99.000	83%	151.981	151.981
22 Current corporate expenditure	81.829	98.702	798.696	709%	129.235	129.235
23 ICT	3.436.156	2.067.972	1.245.347	-40%	864.813	864.813
Title 3. Operational expenditure	**4.402.318**	**7.328.981**	**9.150.000**	**25%**	**9.967.504**	**9.967.504**
30 Activities related to meetings and missions	910.929	628.966	650.000	3%	51.694	51.694
32 Horizontal operational activities	524.689	1.517.962	0	-100%	992.528	992.528
36/37 Core operational activities	2.966.700	5.182.053	8.500.000	64%	8.923.282	8.923.282
TOTAL EXPENDITURE	**16.207.370**	**21.682.884**	**23.433.076**	**8%**	**24.227.064**	**24.227.064**
* ENISA operates with non-differentiated appropriations, therefore commitment appropriations equal payment appropriations						
** as adopted in the Amending Budget 1/2020 (MB Decision No MB/2020/18)						

Table 3: Budget outturn and cancellation of appropriations

Budget outturn	2017	2018	2019
Revenue actually received (+)	11.223.387	11.572.995	16.740.086
Payments made (-)	-9.901.545	-10.345.736	-11.980.352
Carry-over of appropriations (-)	-1.376.730	-1.348.657	-4.357.734
Cancellation of appropriations carried over (+)	90.916	108.302	62.522
Adjustment for carry-over of assigned revenue appropriations carried over (+)	49.519	124.290	116.393
Exchange rate difference (+/-)	-12	-689	-1.802

Adjustment for negative balance from previous year (-)	-	-	-
Total	**85.535**	**110.505**	**579.113**

III.a Cancellation of appropriations

- Cancellation of Commitment Appropriations

In 2019 Commitment Appropriations were cancelled for an amount of EUR 521 426 representing 3 % of the total budget. ENISA demonstrates a commitment rate of 97 % of C1 appropriations of the year at the year-end (31/12). The consumption of the 2019 budget at year-end shows the capacity of the Agency to fully implement its annual appropriations. The payment rate reached 70 % and the amount carried forward to 2020 is EUR 4 347 332 representing 27 % of total C1 appropriations in 2019.

- Cancellation of Payment Appropriations for the year

No payment appropriations were cancelled during 2019.

- Cancellation of Payment Appropriations carried over

(Fund source “C8” – appropriations carried over automatically from 2018 to 2019.)

The appropriations of 2018 carried over to 2019 were utilised at a rate of 95 % (automatic carry-overs) which indicates a satisfactory capability of estimation of needs. From the amount of EUR 1 232 263 carried forward, the amount of EUR 62 522 was cancelled, due to the fact that the estimated expenditure deviated from the actual paid amount. This cancellation represents 0,4 % of the total budget 2019.

IV. HUMAN RESOURCES- QUANTITATIVE

Overview of all categories of staff and its evolution

Staff policy plan for 2021 - 2023

Table 1: Staff population and its evolution; Overview of all categories of staff

Statutory staff and SNE

STAFF	2019			2020	2021	2022	2023
ESTABLISHMENT PLAN POSTS	**Authorised Budget**	**Actually filled as of 31/12/2019**	**Occupancy rate %**	**Authorised staff**	**Envisaged staff**	**Envisaged staff**	**Envisaged staff**
Administrators (AD)	43	37	86.%	51	57	60	60
Assistants (AST)	16	14	88%	18	19	19	19
Assistants/Secretaries (AST/SC)							
TOTAL ESTABLISHMENT PLAN POSTS	59	51	87%	69	76	79	79
EXTERNAL STAFF	**FTE corresponding to the**	**Executed FTE as of 31/12/2019**	**Execution Rate %**	**Headcount as of 31/12/2020**	**FTE corresponding to the**	**Envisaged FTE**	**Envisaged FTE**

	authorised budget				authorised budget		
Contract Agents (CA)	30	226	87%	26	30	30	30
Seconded National Experts (SNE)	9	4	44%	4	12	12	12
TOTAL EXTERNAL STAFF	5	12	**100%**	**12**	**5**	**5**	**5**
TOTAL	**44**	**42**	**95%**	**42**	**47**	**47**	**47**
TOTAL STAFF	**103**	**93**	**90%**	**111**	**118**	**121**	**121**

Additional external staff expected to be financed from grant, contribution or service-level agreements

Human Resources	2020	2021	2022	2023
	Envisaged FTE	Envisaged FTE	Envisaged FTE	Envisaged FTE
Contract Agents (CA)	n/a	n/a	n/a	n/a
Seconded National Experts (SNE)	n/a	n/a	n/a	n/a
TOTAL	n/a	n/a	n/a	n/a

Other Human Resources

- Structural service providers

	Actually in place as of 31/12/2019
Security	4
IT	

- Interim workers

	Actually in place as of 31/12/2019
Number	30

Table 2: Multi-annual staff policy plan Year 2019, 2020, 2021, 2022, 2023

Function group and grade	2019				2020		2021		2022		2023	
	Authorised budget		Actually filled as of 31/12		Authorised budget		Envisaged		Envisaged		Envisaged	
	Permanent posts	Temporary posts	Permanent posts	Temporary posts	Perm. posts	Temp. posts	Perm. Posts	Temp. posts	Perm. posts	Temp. posts	Perm. posts	Temp. posts
AD 16												
AD 15		1				1		1		1		1
AD 14				1								
AD 13								1		2		2
AD 12		6		6		6		5		4		4
AD 11								2		2		2
AD 10		5		3		5		3		4		4
AD 9		12		4		12		12		11		11
AD8		19		10		21		21		22		22
AD 7				6		3		8		8		8
AD 6				6		3		4		6		6
AD 5				1								
AD TOTAL		43		37		51		57		60		60
AST 11												
AST 10												
AST 9												
AST 8								1		2		2
AST 7		3		2		4		4		3		3
AST 6		7		2		8		8		8		8
AST 5		5		4		5		5		5		5
AST 4		1		4		1		1		1		1
AST 3				1								
AST 2				1								
AST 1												
AST TOTAL		16		14		18		19		19		19
AST/SC 6												
AST/SC 5												
AST/SC 4												
AST/SC 3												
AST/SC 2												
AST/SC 1												
AST/SC TOTAL												
TOTAL		59		51		69		76		79		79
GRAND TOTAL	59		51		69		76		79		79	

External personnel

Contract Agents

Contract agents	FTE corresponding to the authorised budget N-1	Executed FTE as of 31/12/N-1	Headcount as of 31/12/N-1	FTE corresponding to the authorised budget 2020	FTE corresponding to the authorised budget 2021	FTE corresponding to the authorised budget 2022	FTE corresponding to the authorised budget 2023
Function Group IV	28	17	17	28	28	28	28
Function Group III	2	8	8	2	2	2	2
Function Group II	0	0	0	0	0	0	0
Function Group I	0	1	1	0	0	0	0
TOTAL	30	26	26	30	30	30	30

Seconded National Experts

Seconded National Experts	FTE corresponding to the authorised budget 2019	Executed FTE as of 31/12/2019	Headcount as of 31/12/2019	FTE corresponding to the authorised budget 2020	FTE corresponding to the authorised budget 2021	FTE corresponding to the authorised budget 2022	FTE corresponding to the authorised budget 2023
TOTAL	9	4	4	12	12	12	12

Table 3: recruitment forecasts 2021 following retirement / mobility or new requested posts (indicative table)

Job title in the agency	TYPE OF CONTRACT (OFFICIAL, TA OR CA)		TA/OFFICIAL		CA
			Function group/grade of recruitment internal (Brackets) and external (single grade) foreseen for publication *		Recruitment Function Group (I, II, III and IV)
	Due to foreseen retirement/ mobility	New post requested due to additional tasks	Internal (brackets)	External (brackets)	
Safety, Security and Facilities Officer	Retirement in 2021	n/a	n/a	n/a	n/a
Experts		6 AD posts	n/a	n/a	n/a
Assistant		1 AST post	n/a	n/a	n/a

V. HUMAN RESOURCES QUALITATIVE

A. Recruitment policy

Implementing rules in place:

		YES	NO	If no, which other implementing rules are in place
Engagement of CA	Model Decision C(2019)3016	x		
Engagement of TA	Model Decision C(2015)1509	x		
Middle management	Model decision C(2018)2542	x		
Type of posts	Model Decision C(2018)8800		x	C(2013) 8979

B. Appraisal and reclassification/promotions

Implementing rules in place:

		YES	NO	If no, which other implementing rules are in place
Reclassification of TA	Model Decision C(2015)9560	x		
Reclassification of CA	Model Decision C(2015)9561	x		

Table 1: Reclassification of TA/promotion of official

The reclassification for 2020 will be concluded i**n Q3.**

AVERAGE SENIORITY IN THE GRADE AMONG RECLASSIFIED STAFF							
Grades	**Year 2016**	**Year 2017**	**Year 2018**	**Year 2019**	**Year 2020**	**Actual average over 5 years**	**Average over 5 years (According to decision C(2015)9563)**
AD05	-	-	-	-	-	-	2.8
AD06	1	1	2	3	-	3,7	2.8
AD07	1	-	-	-	-	4	2.8
AD08	1	-	1	1	-	5,7	3
AD09	-	-	-	1	-	10	4
AD10	-	-	-	-	-	-	4
AD11	-	1	-	-	-	3	4
AD12	-	-	-	-	-	-	6.7
AD13	-	-	-	-	-	-	6.7
AST1	-	-	-	-	-	-	3
AST2	-	-	-	-	-	-	3
AST3	2	1	1	1	-	4,42	3
AST4	-	1	1	1	-	5,67	3
AST5	1	-	1	-	-	5,5	4
AST6	1	-	-	-	-	4	4

AST7	-	-	-	-	-	-	4
AST8	-	-	-	-	-	-	4
AST9	-	-	-	-	-	-	N/A
AST10 (Senior assistant)	-	-	-	-	-	-	5

We do not have any AST/SCs at ENISA: n/a

AST/SC1							4
AST/SC2							5
AST/SC3							5.9
AST/SC4							6.7
AST/SC5							8.3

Table 2: Reclassification of contract staff

Function group	Grade	Staff in activity at 1.01.2018	How many staff members were reclassified in year 2019	Average number of years in grade of reclassified staff members	Average number of years in grade of reclassified staff members according to decision c(2015)9561
CA IV	17	-	-	-	Between 6 and 10 years
	16	1	-	-	Between 5 and 7 years
	15	1	-	-	Between 4 and 6 years
	14	11	-	-	Between 3 and 5 years
	13	3	-	-	Between 3 and 5 years
CA III	11	1	-	-	Between 6 and 10 years
	10	2	-	-	Between 5 and 7 years
	9	7	3	5,77	Between 4 and 6 years
	8	2	1	4,8	Between 3 and 5 years
CA II	6	-	-	-	Between 6 and 10 years
	5	-	-	-	Between 5 and 7 years
	4	-	-	-	Between 3 and 5 years
CA I	3	1	-	-	n/a
	2	-	-	-	Between 6 and 10 years
	1	-	-	-	Between 3 and 5 years

C. Gender representation

Table 1: Data on 31/12/2019 statutory staff (only officials, AT and AC)

		OFFICIAL		TEMPORARY		CONTRACT AGENTS		GRAND TOTAL	
		Staff	%	Staff	%	Staff	%	Staff	%
Female	Administrator level	-	-	10	-	15	-	-	-
	Assistant level (AST & AST/SC)	-	-	8	-	-	-	-	-
	Total	-	-	18	54,5	15	45,5	33	45%
Male	Administrator level	-	-	24	-	11	-	-	-

	Assistant level (AST & AST/SC)	-	-	5	-	-	-	-	-
	Total	-	-	29	72,5	11	27,5	40	55%
Grand Total		-	-	47	64%	26	36%	73	100%

Table 2: Data regarding gender evolution over 5 years of the Middle and Senior management

	2015		2019	
	Number	%	Number	%
Female Managers	0	0	2	20
Male Managers	10	100	8	80

The focus of the Agency being cybersecurity hints at the reason for a certain gender imbalance. Nevertheless, an improvement has been noted during the past five years. Continuous efforts to encourage female involvement in this domain have borne fruit, however, further efforts should be envisaged in order to achieve a higher percentage of female middle and senior managers at ENISA in the upcoming years.

D. Geographical Balance

Table 1: Data on 31/12/2019 - statutory staff only (officials, AT and AC)

NATIONALITY	AD + CA FG IV		AST/SC- AST + CA FGI/CA FGII/CA FGIII		TOTAL	
	Number	% of total staff members in AD and FG IV categories	Number	% of total staff members in AST SC/AST and FG I, II and III categories	Number	% of total staff
BE	3	6	2	8	5	6,8%
BG	2	4	-	-	2	2,7%
CY	-	-	1	4	1	1,4%
CZ	1	2	-	-	1	1,4%
DE	1	2	-	-	1	1,4%
Double *9	4	8	3	12,5	7	9,6%
EE	1	2	-	-	1	1,4%
ES	2	4	1	4	3	4,1%

[9] Double nationalities comprise staff members who also have non-EU nationalities (i.e. Italian/Australian, Belgian/British, Cypriot/Greek, German/Greek, Dutch/Greek etc.).

FR	3	6	1	4	4	5,5%
GR	19	38,8	10	41	29	39,7%
IT	2	4	-	-	2	2,7%
LT	-	-	1	4	1	1,4%
LV	2	4	-	-	2	2,7%
NL	2	4	-	-	2	2,7%
PL	1	2	1	4	2	2,7%
PT	3	6	1	4	4	5,5%
RO	2	4	2	8	4	5,5%
SE	1	2	-	-	1	1,4%
SK	-	-	1	4	1	1,4%
TOTAL	49	67,1	24	32,9	73	100

Double nationalities comprise staff members who also have non-EU nationalities (i.e. Italian/Australian, Belgian/British, Cypriot/Greek, German/Greek, Dutch/Greek etc.).

Table 2: Evolution over 5 years of the most represented nationality in the Agency

Most represented nationality	2015		2019	
	Number	%	Number	%
Greek	18 (out of 63)	28,5	29 (out of 73)	39,7

The imbalance related to the most represented nationality at ENISA is related to several factors, such as, for example, the level of posts and related salaries which may be perceived as less appealing for job seekers in relatively more advanced member state economies; the fact that ENISA has a better position as employer compared to average conditions offered in the Greek job market; the small job market in Greece for cybersecurity professionals; historic decisions taken by previous AIPNs. Another reason that may be cited is the need for stability during the start up phase of the Agency, as staff from the hosting member state (Greece) is less prone to resign (resulting in lesser turnover), which in combination with the relatively young age of the Agency compared to others, still has its original impact; the relatively better academic profile of Greek candidates that bears for lower level posts; the relatively smaller payroll cost for staff that is relatively better qualified than average while costing less if expatriation allowance is considered, as well as the general predisposition to retain a lower level position in the home country.

E. Schooling

Agreement in place with the European School of Heraklion	
Contribution agreements signed with the EC on type I European schools	No
Contribution agreements signed with the EC on type II European schools	Yes
Number of service contracts in place with international schools:	For the school year 2019-2020, there are 12 service level agreements in place.

VI. ENVIRONMENT MANAGEMENT

While ENISA has not yet adopted a formal environment management policy, it has nevertheless implemented several greening measures such as: recycling of office materials, reduction in electricity usage for lighting and heating/cooling, the use of video conferencing equipment instead of physical meetings involving travel, use of teleworking, provision of bicycle racks to promote the use of public transport, implementing Green Public Procurement (GPP).

All the measures were taken within the scope of the agency's activities and to the extent possible given its infrastructure and location.

ENISA presently occupies part of a leased building in Athens. This unfortunately does not allow the Agency to control the heating/cooling system, or to access to autonomous electricity meters. The Agency is therefore unable to directly monitor those systems and assess the impact of greening measures implemented.

Therefore ENISA could not seek to obtain the EMAS certification for our main office building considering the leasing restrictions. However, this certification will be envisaged for the new premises to be provided by the Hellenic Authorities. In anticipation of this, the Agency plans to conduct an environmental audit of its activities as well as pursue options to offset its carbon emissions (including occurred through missions).

VII. BUILDING POLICY

As per the existing Seat Agreement between ENISA and the Hellenic Republic which entered into force on the 04/10/2019, the Agency will continue having premises in Athens and Heraklion. The permanent seat of the Agency is in Athens were the majority of its staff is based and Heraklion is a support office.

At the time of this document the premises of ENISA in Athens are privately owned and rented by the Agency, and in Heraklion the premises are located in a public building made available by the Hellenic Authorities. The payment of rents for the premises in Athens and Heraklion are covered by the Hellenic Authorities who make available the amount of up to 640K per year.

The current building in Athens will not suffice to accommodate all the new staff that will be joining the Agency in virtue of the new Mandate with the additional challenge that the current renting contract expires on 31/12/2021 with not envisaged possibility of extension. ENISA is currently requesting to the Hellenic Authorities to find suitable premises to accommodate the Agency in Athens. The Ministry of Digital Governance, representing the Hellenic Authorities, is in charge of this dossier and expresses the commitment to find an adequate long term premises for the Agency. The selection of the new premises of ENISA in Athens will need to be completed in Q3 2020 to allow a smooth transition and installation in the new premises.

VIII. PRIVILEGES AND IMMUNITIES

Agency privileges	Privileges granted to staff	
	Protocol of privileges and immunities / diplomatic status	Education / day care
In accordance with Art. 23 of Regulation (EU) No 2019/881 of the European Parliament and of the Council of 17 April 2019, the protocol No 7 on the privileges and immunities of the European Union annexed to the TEU and the TFEU applies to the Agency and its staff. The Greek Government and ENISA signed a Seat Agreement the 13 November 2018, which was ratified by Greek Law 4627/2019 on the 25 September 2019 and entered in to force on the 04 October 2019 and is applicable to ENISA and its staff.	In accordance with Article 35 of Regulation (EU) No 2019/881 of the European Parliament and of the Council of 17 April 2019, the protocol No 7 on the privileges and immunities of the European Union annexed to the TEU and the TFEU applies to the Agency and its staff. The Greek Government and ENISA signed a Seat Agreement the 13 November 2018, which was ratified by Greek Law 4627/2019 on the 25 September 2019 and entered in to force on the 04 October 2019 and is applicable to ENISA and its staff.	A public School of European Education, Type 2, was founded in 2005 by the Greek government in Heraklion – Crete for the children of the staff of ENISA. There is no European School operating in Athens.

IX. EVALUATIONS

External consultant are contracted to carry annual ex-post evaluation of operational activities. The scope of the evaluation focusses on ENISA's operational activities. The overall aim of the annual evaluations is to evaluate the effectiveness, efficiency, added value, utility, coordination and coherence.

ENISA uses an internal monitoring system that intends to support the project management function, which includes the project delivery and resources allocation. The regular reporting and the ENISA management team uses this information for managerial purposes. Moreover, ENISA have implemented a mid-term review procedure and regular monthly management team meetings. ENISA expects to undertake a study to upgrade the use of the electronic tool in the internal project management and overall delivery of the Agency WP.

X. STRATEGY FOR THE ORGANISATIONAL MANAGEMENT AND INTERNAL CONTROL SYSTEMS

The Agency's strategy for an effective internal control is based on best international practices and on the Internal Control Framework (COSO Framework's international Standards).

The Control Environment is the set of standards of conduct, processes and structures that provide the basis for carrying out internal control across ENISA. The Management Team set the tone at the top with respect to the importance of the internal control, including expected standards of conduct.

Risk assessment is the Agency's dynamic and iterative process for identifying and assessing risks which could affect the achievement of objectives, and for determining how such risks should be managed.

The control activities ensure the mitigation of risks related to the achievement of policy, operational and internal control objectives. They are performed at all levels of the organisation, at various stages of business processes, and across the technology environment. They may be preventive or detective and encompass a range of manual and automated activities as well as segregation of duties.

Information is necessary for the organisation to carry out internal control and to support the achievement of objectives. In this aspect it is needed to consider external and internal communication. External communication provides the specific Agency stakeholders and globally the EU citizens with information on ENISA's policy, objectives, actions and achievements. Internal communication provides to ENISA staff with the information required to support the achievement of objectives and the awareness for day-to-day controls.

Continuous and specific assessments are used to ascertain whether each of the five components of internal control is present and functioning. Continuous assessments, built into business processes at different levels of the organisation, provide timely information on any deficiencies. Findings are assessed and deficiencies are communicated and corrected in a timely manner, with serious matters reported as appropriate.

The Common Approach on EU Decentralised Agencies foresees that EU agencies should be more active concerning fraud prevention issues and that the related communication forms an essential part of its success. In order to implement this, the European Anti-Fraud Office (OLAF) recommended that each agency should adopt an anti-fraud strategy that is proportionate to its fraud risks. Rules for the prevention and management of conflicts of interests are part of the anti-fraud strategy of the Agency.

XI. PLAN FOR GRANT, CONTRIBUTION OR SERVICE-LEVEL AGREEMENTS

ENISA does not receive any form of grant.

As part of the host country agreement an annual contribution from the Hellenic Authorities to cover its leasing expenditures of its offices (as per seat agreement - Greek law 4627 /2019). The 2019 contribution amounted to EUR 435 844.

ENISA has signed a service level agreement with EU-LISA, an European Union Agency, for the purposes of sharing its knowledge and resources related to the organisation of EU-LISA security exercises in 2019 and 2020 as well as making available its online exercise platform. The generated income amounts to EUR 97 920 per year to cover staff costs and overheads (2 FTEs, equivalent to CA post, are allocated to this tasks). The values agreed in the agreement have a base of cost recovery policy, not generating any additional financial value for the parties.

Table below provides a summary of the SLA and agreements of the agency including contracted amount where necessary:

Title	Type	Contractor	Contracted amount
SLA with EU-Lisa - Cyber Exercise (new)	SLA	EU-LISA - EUROPEAN AGENCY	
SLA with CEDEFOP	SLA	CEDEFOP	
10th Amendment of SLA with CERT-EU-001-00	SLA	EUROPEAN COMMISSION	€ 24.000,00
Service Level Agreement and Service Delivery Agreement with DG Budget Implementation and usage of ABAC System	SLA	DG BUDG	
SLA for the "Issuance process of the laissez-passer" with EC	SLA	EC	
Collaboration between DG HR and ENISA - SYSPER services	SLA		
SLA with DG HR	SLA	DG HR	
Global SLA with DIGIT	SLA	EUROPEAN COMMISSION	
SLA with Office for Official Publications of the European Communities	SLA	Office for OPEC	
SLA for ABAC System with DG Budget	SLA		

SLA with European Administrative School	SLA	EAS	
Agreement for Provision of ICCA services with BEREC	SLA	OFFICE OF THE BODY OF EUROPEAN REGULATORS FOR ELECTRONIC COMMUNICATIONS (BEREC OFFICE)	€ 15.000,00
SLA for Provision of electronic data back up services with BEREC	SLA	OFFICE OF THE BODY OF EUROPEAN REGULATORS FOR ELECTRONIC COMMUNICATIONS (BEREC OFFICE)	
SLA with EASA - Permanent Secretariat	SLA	EASA	
SLA for Shared Support Office (SSO)_EUAN	SLA	EUROPEAN FOOD SAFETY AUTHORITY - EFSA	€ 2.459,00
SLA with Veritas School	SLA	VERITAS EDUCATION - EDUCACAO E SERVICOS SA	
SLA with Leonteios School	SLA	LEONTEIO LYKEIO PATISION AEE	
SLA with ACS School	SLA	AMERICAN COMMUNITY SCHOOLS OF ATHENS INC	
SLA with Douka School	SLA	DOUKA EKPAIDEFTIRIA AE	
SLA with Neue Schule 2019/20	SLA	NEUE SCHULE AE	
SLA with Trianemi School 2019/20	SLA	TRIANEMI	
SLA with Platon School 2019/20	SLA	PLATON IB SCHOOL	
SLA with Lycee Franco-Hellenique 2019/20	SLA	LYCÉE FRANCO-HELLÉNIQUE EUGÈNE DELACROIX	
SLA with Arsakeio School 2019/20	SLA	H EN ATHINAIS FILEKPAIDEFTIKI ETAIRIA (Arsakeio)	
SLA with Campion School 2019/20	SLA	CAMPION SCHOOL INC	
SLA with Ionios School	SLA	IONIOS SXOLI SA TRAINING COMPANY	
SLA with S.Catherine's 2019/20	SLA	ST. CATHERINES BRITISH SCHOOL	
SLA with Papakosmas Datatechnica No 2020/003, P7EM-100, 1452152	SLA	PAPAKOSMAS NTATATECHNIKA EPE	
SLA with Papakosmas Datatechnica No 2020/004, P7EM-075, 1452165	SLA	PAPAKOSMAS NTATATECHNIKA EPE	
Amendment 3 of the SLA_Implementation and usage of ABAC System	SLA		
Amendment to SLA btwn ENISA and BEREC	SLA	OFFICE OF THE BODY OF EUROPEAN REGULATORS FOR ELECTRONIC COMMUNICATIONS (BEREC OFFICE)	

SLA with PMO	SLA		
SLA with EPSO and EUSA (updated)	SLA	EUROPEAN PERSONNEL SELECTION OFFICE (EPSO)	
Cooperation between EDA and ENISA	Agreement	EUROPEAN DEFENCE AGENCY - EDA	
Agreement with the Hellenic Ministry of Infrastructure, Transport and Networks	Agreement	REPUBLIQUE HELLENIC - HELLENIC MINISTRY OF INFRASTRUCTURE, TRANSPORT AND NETWORKS	
ABAC DWH extraction and transfer for ENISA's needs	Agreement		€ 27.000,00
Mandate and Service agreement for "Type II European School" with EC	Agreement		
Administrative arrangement with DG HR.DS	Agreement		
Agreement with Translation Centre for the Bodies of the EU	Agreement		
Provision of water fountain and water bottles for Athen's office	Agreement		
Collaboration Agreement with CEN & CENELEC	Agreement		
Austrian signature scheme for e-card and mobile signature_A-Trust	Agreement	A-TRUST GESELLSCHAFT FUR SICHERHEITSSYSTEME IM ELEKTRONISCHEN DATENVERKEHR GMBH	
Agreement for Courier Services	Agreement	TNT SKYPAK HELLAS EPE	
Mission Charter of the IAS of the EC	Agreement		
Agreement on Strategic Co-operation with EUROPOL	Agreement	EUROPEAN UNION AGENCY FOR LAW ENFORCEMENT COOPERATION (EUROPOL)	
Agreement with Edenred (Ticket Restaurant Meal Vouchers)	Agreement	VOUCHERS SERVICES SA	
Joint ENISA - EUROPOL /EC3 WG on Security and Safety Online	Agreement	EUROPEAN POLICE OFFICE EUROPOL	
NoN-Disclosure Agreement CT1607860_Confidential and proprietary document between 12 Parties	Agreement		
Working Arrangement Agreement with eu-LISA (MoU)	Agreement	EU-LISA - EUROPEAN AGENCY	
Lease Agreement Athens office (Main building)	Agreement	ATHENIAN PROPERTIES LIMITED	
Lease Agreement Athens office (East Wing)	Agreement	ATHENIAN PROPERTIES LIMITED	

Agreement with Hellenic Postal Services A.E. - Heraklion office	Agreement	ELLINIKA TACHYDROMEIA*ELTA AE	
Agreement with Hellenic Postal Services A.E. - Athens office	Agreement	ELLINIKA TACHYDROMEIA*ELTA AE	
Inter-Agencies Cost-Sharing Agreement (EUAN)	Agreement	EUROPEAN FOOD SAFETY AUTHORITY - EFSA	€ 982,00
Agreement for courier services with DHL	Agreement	DHL INTERNATIONAL SA	
Mission Charter of the IAS_REVISED	Agreement		

XII. STRATEGY FOR COOPERATION WITH THIRD COUNTRIES AND/OR INTERNATIONAL ORGANISATIONS

Strategy for cooperation with third countries and/or international organisations has been approved by the Management Board in 2017. Following the entry into force of the CSA in 2019, it is foreseen that in the course of 2021 the Agency will elaborate a new international strategy.

XX-00-00-000-XX-X

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
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN 000-00-0000-000-0
doi: 0000.0000/000000

Statement of Estimates 2021 (Budget 2021)

European Union Agency for Cybersecurity

CONTENTS

1. GENERAL INTRODUCTION

Explanatory statement

Legal Basis:

1. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity)

Reference acts

1. Impact assesment submitted by the Commission on 13 September 2017, on ENISA, the 'EU Cybersecurity Agency', as part of the draft 'Cybersecurity Act' (COM(2017) 477 final)
2. ENISA Financial Rules adopted by the Management Board on 15 October 2019

2. JUSTIFICATION OF MAIN HEADINGS

2.1 Revenue in 2021

The 2021 total revenue amounts to € 23473060 and consists of a subsidy of € 22248000 from the General Budget of the European Union, EFTA countries' contributions € 585060 and a subsidy from the Greek Government for the rent of the offices of ENISA in Greece €640000

2.2 Expenditure in 2021

The total forecasted expenditure is in balance with the total forecasted revenue.

Title 1 - Staff

The estimate of Title 1 costs is based on the Establishment Plan for 2021, which contains 76 Temporary Agent posts.

Total expenditure under Title 1 amounts to **€10.775.408,90**

Title 2 - Buildings, equipment and miscellaneous operating expenditure

Total expenditure under Title 2 amounts to **€3.547.651,09**

(including € 640.000,00 for the rent of two offices in Greece, subsidised by the Greek Government)

Title 3 - Operational expenditure

Operational expenditure is mainly related to the implementation of Work Programme 2021 and amounts to **€9.150.000,00**

3. STATEMENT OF REVENUE 2021

Title	Heading	Voted Appropriations 2018 in €	Voted Appropriations 2019 in €	Voted Appropriations - Amending Budget 1/2020 in €	Draft Proposed Appropriations 2021 €	Remarks - budget 2021
1	EUROPEAN COMMUNITIES SUBSIDY	10.529.000	15.910.000	20.646.000	22.248.000	Total subsidy of the European Communities
2	THIRD COUNTRIES CONTRIBUTION	248.626	382.952	503.120	585.060	Contributions from Third Countries.
3	OTHER CONTRIBUTIONS	640.000	640.000	435.844	640.000	Subsidy from the Government of Greece
4	ADMINISTRATIVE OPERATIONS	10.500	0	97.920	0	Other expected income.
	GRAND TOTAL	**11.428.126**	**16.932.952**	**21.682.884**	**23.473.060**	

Article Item	Heading	Voted Appropriations 2018 in €	Voted Appropriations 2019 in €	Voted Appropriations - Amending Budget 1/2020 in €	Draft Proposed Appropriations 2021 €	Remarks - budget 2021
1	EUROPEAN COMMUNITIES SUBSIDY					
10	EUROPEAN COMMUNITIES SUBSIDY					
100	*European Communities subsidy*	10.529.000	15.910.000	20.646.000	22.248.000	Regulation (EU) N° 526/2013 establishing an European Union Agency for Network and Information Security.
	CHAPTER 10	10.529.000	15.910.000	20.646.000	22.248.000	
	TITLE 1	**10.529.000**	**15.910.000**	**20.646.000**	**22.248.000**	
2	THIRD COUNTRIES CONTRIBUTION					
20	THIRD COUNTRIES CONTRIBUTION					
200	*Third Countries contribution*	248.626	382.952	503.120	585.060	Contributions from Associated Countries.
	CHAPTER 2 0	248.626	382.952	503.120	585.060	
	TITLE 2	**248.626**	**382.952**	**503.120**	**585.060**	
3	OTHER CONTRIBUTIONS					
30	OTHER CONTRIBUTIONS					
300	*Subsidy from the Ministry of Transports of Greece*	640.000	640.000	435.844	640.000	Subsidy from the Government of Greece.
	CHAPTER 30	640.000	640.000	435.844	640.000	
	TITLE 3	**640.000**	**640.000**	**435.844**	**640.000**	
4	ADMINISTRATIVE OPERATIONS					
40	ADMINISTRATIVE OPERATIONS					
400	*Administrative Operations*	10.500	0	97.920	0	Revenue from administrative operations.
	CHAPTER 40	10.500	0	97.920	0	
	TITLE 4	**10.500**	**0**	**97.920**	**0**	
	GRAND TOTAL	**11.428.126**	**16.932.952**	**21.682.884**	**23.473.060**	

4. STATEMENT OF EXPENDITURE 2021

Title	Heading	Voted Appropriations 2018 in €	Voted Appropriations 2019 in €	Voted Appropriations - Amending Budget 1/2020 in €	Draft Proposed Appropriations 2021 €	Remarks - budget 2021
1	STAFF	6.386.500	9.387.948	11.203.334	10.775.409	Total funding for covering personnel costs.
2	BUILDINGS, EQUIPMENT AND MISCELLANEOUS OPERATING EXPENDITURE	1.687.500	2.677.000	3.150.568	3.547.651	Total funding for covering general administrative costs.
3	OPERATIONAL EXPENDITURE	3.354.126	4.868.004	7.328.981	9.150.000	Total funding for operational expenditures.
	GRAND TOTAL	**11.428.126**	**16.932.952**	**21.682.884**	**23.473.060**	
1	STAFF					
11	STAFF IN ACTIVE EMPLOYMENT					
110	*Staff holding a post provided for in the establishment plan*					

1100	Basic salaries		3.779.100	5.000.000	5.484.400	6.453.819	Staff Regulations applicable to officials of the European Communities and in particular Articles 62 and 66 thereof. This appropriation is intended to cover salaries, allowances and employee contributions on salaries of permanent officials and Temporary Agents (TA).
		Article 1 1 0	3.779.100	5.000.000	5.484.400	6.453.819	
111	***Other staff***						
1110	Contract Agents		1.168.300	1.650.000	1.476.000	2.106.500	Conditions of employment of other servants of the European Communities and in particular Article 3 and Title III thereof. This appropriation is intended to cover salaries, allowances and employee contributions on salaries of Contract Agents (CA).
1113	Seconded National Experts (SNEs)		239.000	144.000	165.684	250.000	This appropriation is intended to cover basic salaries and all benefits of SNEs.
		Article 111	1.407.300	1.794.000	1.641.684	2.356.500	
		CHAPTER 11	**5.186.400**	**6.794.000**	**7.126.084**	**8.810.319**	
12	**RECRUITMENT/DEPARTURE EXPENDITURE**						
120	***Expenditure related to recruitment***						
1200	Expenditure related to recruitment		19.000	97.000	275.308	49.087	This appropriation is intended to cover expenditure related to recruitment, e.g. incurred for interviewing candidates, external selection committee members, screening applications and other related costs.
		Article 1 2 0	19.000	97.000	275.308	49.087	
121	***Expenditure on entering/leaving and transfer***						
1210	Expenses on Taking Up Duty and on End of Contract		9.600	40.000	48.201	32.000	Staff Regulations applicable to officials of the European Communities and in particular Articles 20 and 71 thereof and Article 7 of Annex VII thereto. This appropriation is intended to cover the travel expenses of staff (including members of their families).
1211	Installation, Resettlement and Transfer Allowance		68.000	356.042	137.424	145.000	Staff Regulations applicable to officials of the European Communities and in particular Articles 5 and 6 of Annex VII thereto. This appropriation is intended to cover the installation allowances for staff obliged to change residence after taking up their duty.
1212	Removal Expenses		68.000	247.000	111.462	72.000	Staff Regulations applicable to officials of the European Communities and in particular Articles 20 and 71 thereof and Article 9 of Annex VII thereto. This appropriation is intended to cover the removal costs of staff obliged to change residence after taking up duty.
1213	Daily Subsistence Allowance		96.500	228.906	132.291	112.000	Staff Regulations applicable to officials of the European Communities and in particular Articles 20 and 71 thereof and Article 10 of Annex VII thereto, as well as Articles 25 and 67 of the Conditions of Employment of other Servants. This appropriation is to cover the costs of daily subsistance allowances.
		Article 1 2 1	242.100	871.948	429.378	361.000	
		CHAPTER 1 2	**261.100**	**968.948**	**704.686**	**410.087**	

13	**SOCIO-MEDICAL SERVICES AND TRAINING**						
131	***Medical Service***						
1310	Medical Service		35.000	75.000	45.310	53.882	This appropriation is intended to cover the costs of annual medical visits and inspections, occupational doctor services as well as pre-recruitment medical costs and other costs related to medical services.
		Aticle 1 3 1	35.000	75.000	45.310	53.882	
132	***Training***						
1320	Language Courses and Other Training		155.000	250.000	330.428	280.182	This appropriation is intended to cover the costs of language and other training needs as well as teambuilding activities.
		Article 1 3 2	155.000	250.000	330.428	280.182	
133	***Social welfare***						
1330	Other welfare expenditure		n/a	n/a	n/a	250.000	This appropriation is intended to cover other welfare expenditure such as health related activities to promote well-being of staff, other activities related to internal events, other welfare measures.
1331	Schooling & Education expenditure		n/a	n/a	n/a	500.000	This appropriation is intended to cover the subsidy for the functioning of the School of European Education of Heraklion and other expenditure relevant to schooling & education of children of the Agency staff.
		Article 1 3 3	0	0	0	750.000	
		CHAPTER 1 3	**190.000**	**325.000**	**375.738**	**1.084.064**	
14	**TEMPORARY ASSISTANCE**						
140	***European Commission Management Costs***						
1400	EC Management Costs		54.000	58.000	39.149	70.939	This appropriation is intended to cover the EC management costs.
		Article 1 4 0	54.000	58.000	39.149	70.939	
141	***Social welfare***						
1411	Other welfare expenditure		130.000	110.000	172.537	n/a	*As from 2021, whereas the budget structure has been aligned with the SPD, this budget line has been moved to budget line 1330*
1412	Schooling & Education expenditure		300.000	420.000	470.000	n/a	*As from 2021, whereas the budget structure has been aligned with the SPD, this budget line has been moved to budget line 1331*
		Article 1 4 1	430.000	530.000	642.536	0	
142	***Temporary Assistance***						
1420	Interim Service		155.000	572.000	1.673.006	400.000	This appropriation is intended to cover the costs of temporary assistance (trainees and interim services).
1421	Consultants		95.000	115.000	625.135	n/a	*As from 2021, whereas the budget structure has been aligned with the SPD, this budget line has been moved to budget line 2220*
1422	Internal Control and Audit		15.000	25.000	17.000	n/a	*As from 2021, whereas the budget structure has been aligned with the SPD, this budget line has been moved to budget line 2220*
		Article 1 4 2	265.000	712.000	2.315.141	400.000	
		CHAPTER 1 4	**749.000**	**1.300.000**	**2.996.826**	**470.939**	
		Total Title 1	**6.386.500**	**9.387.948**	**11.203.334**	**10.775.409**	
2	**BUILDINGS, EQUIPMENT AND MISCELLANEOUS OPERATING EXPENDITURE**						
20	**BUILDINGS AND ASSOCIATED COSTS**						
200	**Buildings and associated costs**						
2000	Rent of buildings		640.000	640.000	435.844	640.000	This appropriation is intended to cover the payment of rent for buildings or parts of buildings occupied by the Agency and the hiring of parking spaces.
2002	Building Insurance		5.500	6.000	4.500	n/a	*As from 2021, whereas the budget structure has been aligned with the SPD, this budget line has been moved to budget line 2003*
2003	Water, gas, electricity, heating and insurance		85.000	130.000	58.500	76.050	This appropriation is intended to cover the costs of utitlities and insurance of the premises of the Agency.
2004	Cleaning and maintenance		55.000	74.000	100.120	120.000	This appropriation is intended to cover the costs of cleaning and upkeeping of the premises used by the Agency.

2005	Fixtures and Fittings		15.000	25.000	25.650	50.000	This appropriation is intended to cover the fitting-out of the premises and repairs in the building.
2006	Security equipment		15.000	25.000	64.651	n/a	*As from 2021, whereas the budget structure has been aligned with the SPD, this budget line has been moved to budget line 2007*
2007	Security Services and Equipment		110.000	140.000	134.084	140.000	This appropriation is intended to cover expenditure on buildings connected with security and safety, in particular contracts governing building surveillance as well as purchases and maintenance cost of equipment related to security and safety of the building and the staff.
2008	Other expenditure on buildings		75.000	60.000	106.470	378.558	The appropriation is intended to cover expenditure on buildings not specially provided for in the articles in Chapter 20, for example market survey costs for rent of buildings, costs of moving to and/or establishing new premises of the Agency and other handling costs.
		Article 2 0 0	1.000.500	1.100.000	929.820	1.404.608	
		CHAPTER 2 0	**1.000.500**	**1.100.000**	**929.820**	**1.404.608**	

21	**MOVABLE PROPERTY AND ASSOCIATED COSTS**						
210	***Technical Equipment and installations***						
2100	Technical Equipment and services		15.000	25.000	10.968	30.000	This appropriation is intended to cover expenditure of acquiring technical equipment, as well as maintenance and services related to it.
		Article 2 1 0	15.000	25.000	10.968	30.000	
211	***Furniture***						
2110	Furniture		30.000	15.000	16.303	49.000	This appropriation is intended to cover the costs of purchasing, leasing, and repairs of furniture.
		Article 2 1 1	30.000	15.000	16.303	49.000	
212	***Transport Equipment***						
2121	Maintenance and Repairs of transport equipment		10.000	12.000	9.000	10.000	This appropriation is intended to cover the costs of maintenance and repairs of transport equipment as well as insurance and fuel.
		Article 2 1 2	10.000	12.000	9.000	10.000	
213	***Library and Press***						
2130	Books, Newspapers and Periodicals		5.000	6.000	17.803	10.000	This appropriation is intended to cover the purchase of publications and subscriptions to information services necessary for the work of the Agency, including books and other publications, newspapers, periodicals, official journals and subscriptions.
		Article 2 1 3	5.000	6.000	17.803	10.000	
		CHAPTER 2 1	**60.000**	**58.000**	**54.074**	**99.000**	
22	**CURRENT CORPORATE EXPENDITURE**						
220	***Stationery, postal and telecomunications***						
2200	Stationery and other office supplies		30.000	60.000	52.233	30.000	This appropriation is intended to cover the costs of office stationery and the purchase of office kitchen consumables.
2201	Postage and delivery charges		19.000	20.000	30.000	20.000	This appropriation is intented to cover post office and special courrier costs.
2203	Other Office Supplies		12.000	23.000	15.469	n/a	*As from 2021, whereas the budget structure has been aligned with the SPD, this budget line has been moved to budget line 2200*
		Article 2 2 0	61.000	103.000	97.702	50.000	
221	***Financial charges***						
2210	Bank charges and interest paid		1.000	1.000	1.000	1.000	This appropriation is intended to cover bank charges, interest paid and other financial and banking costs.
		Article 2 2 1	1.000	1.000	1.000	1.000	
222	***Outsourcing consultancy services for corporate activities***						
2220	Outsourcing consultancy services for corporate activities		n/a	n/a	n/a	747.696	This appropriation is intended to cover expenditure of contracting consultants linked to administrative support services and horizontal tasks, e.g. in HR area, IT area, financial, accounting, internal controls, legal consultancy, advisory, audit, external evaluation, strategic consultancy and/or other administrative support services provided by third parties.
		Article 2 2 2	0	0	0	747.696	
		CHAPTER 2 2	**62.000**	**104.000**	**98.702**	**798.696**	
23	**ICT**						
230	***ICT***						
2304	Service Transition		130.000	600.000	741.135	n/a	*As from 2021, whereas the budget structure has been aligned with the SPD, these budget lines have been moved to Article 231 Corporate ICT expenditure*
2305	Service Operations		95.000	220.000	184.018	n/a	
2307	Service External		340.000	595.000	1.142.819	n/a	
		Article 2 3 0	565.000	1.415.000	2.067.972	0	
231	***Corporate ICT expenditure***						
2310	Corporate ICT recurrent costs		n/a	n/a	n/a	585.347	This appropriation is intended to cover recurrent corporate ICT costs on hardware, software, services and maintenance as well as ENISA website and portals support.
2311	Corporate ICT new investments and one-off projects		n/a	n/a	n/a	660.000	This appropriation is intended to cover new investments on corporate ICT as well as one-off projects for hardware, software, services and maintenance as well as ENISA website and portals support.
		Article 2 3 1	0	0	0	1.245.347	

CHAPTER 2 3	**565.000**	**1.415.000**	**2.067.972**	**1.245.347**
Total Title 2	**1.687.500**	**2.677.000**	**3.150.568**	**3.547.651**

3	**OPERATIONAL EXPENDITURE**						
30	**ACTIVITIES RELATED TO OUTREACH AND MEETINGS**						
300	***Outreach, meetings and representation expenses***						
3001	Outreach, meetings, translations and representation expenses		120.000	120.000	69.198	650.000	This appropriation is intended to cover costs of outreach activities (communications, stakeholders' management, publication and translations), meetings (including meetings of ENISA's statutory bodies i.e. MB, AG, NLOs, and meetings with other stakeholders) and other representation costs. It also covers mission costs related to the implementation of Activities 10-11 as defined in the SPD 2021-2023 mainly covering horizontal tasks and other administrative services.
		Article 3 0 0	120.000	120.000	69.198	650.000	
301	***Mission and Representation Costs***						
3011	Entertainment and Representation expenses		2.500	15.394	5.000	n/a	*As from 2021, whereas the budget structure has been aligned with the SPD, these budget lines*
3016	Missions		590.000	897.930	550.767	n/a	*have been moved to budget line 3001*
		Article 3 0 1	592.500	913.324	555.767	0	
302	***Other meetings***						
3021	Other Operational meetings		2.500	10.000	4.000	n/a	*As from 2021, whereas the budget structure has been aligned with the SPD, this budget line has been moved to budget line 3001*
		Article 3 0 2	2.500	10.000	4.000	0	
		CHAPTER 3 0	**715.000**	**1.043.324**	**628.966**	**650.000**	
32	**HORIZONTAL OPERATIONAL ACTIVITIES**						
320	***Conferences and Joint Events***						
3200	Horizontal Operational meetings		165.000	214.608	65.448	n/a	*As from 2021, whereas the budget structure has been aligned with the SPD, this budget line has been moved to budget line 3001*
		Article 3 2 0	165.000	214.608	65.448	0	
321	***Communication and Information dissemination***						
3210	Communication activities		80.000	150.000	205.763	n/a	*As from 2021, whereas the budget structure has been aligned with the SPD, these budget lines*
3211	Internal Communication		20.000	0	45.000	n/a	*have been moved to budget line 3001*
3212	Stakeholders' communication		160.000	113.000	291.358	n/a	
		Article 3 2 1	260.000	263.000	542.121	0	
323	***Translation and interpretation services***						
3230	Translations		15.000	30.072	120.000	n/a	*As from 2021, whereas the budget structure has been aligned with the SPD, this budget line has been moved to budget line 3001*
		Article 3 2 3	15.000	30.072	120.000	0	
325	***Operational Systems***						
3250	Operational Systems including website development		80.000	57.000	146.079	n/a	*As from 2021, whereas the budget structure has been aligned with the SPD, this budget line has been moved to Article 231 Corporate ICT expenditure*
		Article 3 2 5	80.000	57.000	146.079	0	
326	***Strategy and Evaluation***						
3260	Strategic consultancy		40.000	50.000	251.215	n/a	*As from 2021, whereas the budget structure has been aligned with the SPD, these budget lines*
3261	External Evaluations		100.000	0	393.100	n/a	*have been moved to budget line 2220*
		Article 3 2 6	140.000	50.000	644.315	0	
		CHAPTER 3 2	**660.000**	**614.680**	**1.517.962**	**0**	

36	**CORE OPERATIONAL ACTIVITIES**					
363	***Activity: Expertise***					
3630	Activity: Expertise	536.626	875.000	1.282.536	n/a	
	Article 3 6 3	536.626	875.000	1.282.536	0	
364	***Activity: Policy***					
3640	Activity: Policy	646.500	1.150.000	1.742.210	n/a	
	Article 3 6 4	646.500	1.150.000	1.742.210	0	*As from 2021, whereas the budget structure has been aligned with the SPD, these budget lines have been moved to Chapter 37*
365	***Activity: Capacity***					
3650	Activity: Capacity	300.000	535.000	798.982	n/a	
	Article 3 6 5	300.000	535.000	798.982	0	
366	***Activity: Community***					
3660	Activity: Community	496.000	650.000	1.358.326	n/a	
	Article 3 6 6	496.000	650.000	1.358.326	0	
	CHAPTER 3 6	**1.979.126**	**3.210.000**	**5.182.053**	**0**	
37	**CORE OPERATIONAL ACTIVITIES**					
371	***Activity 1 - Providing assistance on policy development***					
3710	Activity 1 - Providing assistance on policy development	n/a	n/a	n/a	280.000	This appropriation is intended to cover direct operational costs relevant to the Activity 1 (including operational ICT and mission costs).
	Article 3 7 1	0	0	0	280.000	
372	***Activity 2 - Supporting implementation of Union policy and law***					
3720	Activity 2 - Supporting implementation of Union policy and law	n/a	n/a	n/a	985.000	This appropriation is intended to cover direct operational costs relevant to the Activity 2 (including operational ICT and mission costs).
	Article 3 7 2	0	0	0	985.000	
373	***Activity 3 - Capacity building***					
3730	Activity 3 - Capacity building	n/a	n/a	n/a	1.400.000	This appropriation is intended to cover direct operational costs relevant to the Activity 3 (including operational ICT and mission costs).
	Article 3 7 3	0	0	0	1.400.000	
374	***Activity 4 - Enabling operational cooperation***					
3740	Activity 4 - Enabling operational cooperation	n/a	n/a	n/a	1.110.000	This appropriation is intended to cover direct operational costs relevant to the Activity 4 (including operational ICT and mission costs).
	Article 3 7 4	0	0	0	1.110.000	
375	***Activity 5 - Contribute to cooperative response at Union and Member States level***					
3750	Activity 5 - Contribute to cooperative response at Union and Member States level	n/a	n/a	n/a	1.200.000	This appropriation is intended to cover direct operational costs relevant to the Activity 5 (including operational ICT and mission costs).
	Article 3 7 5	0	0	0	1.200.000	
376	***Activity 6 - Development and maintenance of EU cybersecurity certification framework***					
3760	Activity 6 - Development and maintenance of EU cybersecurity certification framework	n/a	n/a	n/a	870.000	This appropriation is intended to cover direct operational costs relevant to the Activity 6 (including operational ICT and mission costs).
	Article 3 7 6	0	0	0	870.000	
377	***Activity 7 - Supporting European cybersecurity market and industry***					
3770	Activity 7 - Supporting European cybersecurity market and industry	n/a	n/a	n/a	490.000	This appropriation is intended to cover direct operational costs relevant to the Activity 7 (including operational ICT and mission costs).
	Article 3 7 7	0	0	0	490.000	
378	***Activity 8 - Knowledge on emerging cybersecurity challenges and opportunities***					
3780	Activity 8 - Knowledge on emerging cybersecurity challenges and opportunities	n/a	n/a	n/a	1.155.000	This appropriation is intended to cover direct operational costs relevant to the Activity 8 (including operational ICT and mission costs).
	Article 3 7 8	0	0	0	1.155.000	

379	***Activity 9 - Outreach and education***						
3790	Activity 9 - Outreach and education		n/a	n/a	n/a	1.010.000	This appropriation is intended to cover direct operational costs relevant to the Activity 9 (including operational ICT and mission costs).
		Article 3 7 9	0	0	0	1.010.000	
		CHAPTER 3 7	**0**	**0**	**0**	**8.500.000**	
		TITLE 3	**3.354.126**	**4.868.004**	**7.328.981**	**9.150.000**	
		GRAND TOTAL	**11.428.126**	**16.932.952**	**21.682.884**	**23.473.060**	

European Union Agency
for Cybersecurity
Vasilissis Sofias Str 1
151 24 Maroussi | Attiki | Greece
Tel: +30 28 14 40 9711
E-mail: info@enisa.europa.eu
www.enisa.europa.eu

Draft Establishment plan 2021

Category and grade	Establishment plan in voted EU Budget 2020		Establishment plan 2021	
	Off.	TA	Off.	TA
AD 16				
AD 15		1		1
AD 14				
AD 13				1
AD 12		6		5
AD 11				2
AD 10		5		3
AD 9		12		12
AD 8		21		21
AD 7		3		8
AD 6		3		4
AD 5				
Total AD		**51**		**57**
AST 11				
AST 10				
AST 9				
AST 8				1
AST 7		4		4
AST 6		8		8
AST 5		5		5
AST 4		1		1
AST 3				
AST 2				
AST 1				
Total AST		**18**		**19**
AST/SC1				
AST/SC2				
AST/SC3				
AST/SC4				
AST/SC5				
AST/SC6				
Total AST/SC				
TOTAL		**69**		**76**