European Commission

Secure societies - Protecting freedom and security of Europe and its citizens

Highlights

Work Programme 2020

(Cybersecurity, Digital Privacy and data protection, Artificial Intelligence, Critical infrastructure protection)

Unit B4 Safeguarding Secure Society

Research Executive Agency

info: *nikolaos.panagiotarakis@ec.europa.eu*

Presentation Content

- ***General information on the Call***
- ***Cybersecurity, Digital Privacy and data protection***
  - *SU-DS02-2020:* ***Intelligent security and privacy management*** *(IA/ RIA)*
  - *SU-DS03-2019-2020:* ***Digital Security and privacy for citizens and Small and Medium Enterprises and Micro Enterprises*** *(IA)*
  - *SU-DS04-2018-2020:* ***Cybersecurity in the Electrical Power and Energy System (EPES): an armour against cyber and privacy attacks and data breaches*** *(IA)*
- ***Artificial Intelligence*** *and security: providing a balanced assessment of opportunities and challenges for Law Enforcement in Europe*
- ***Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe***

General information on the Call

General info
Call 2020

European Commission

Digital Security

Opening	Closing
12 March 2020	27 August 2020

Topic	Indicative budget (m€)	Info link	Project average EU contribution (m€)
SU-DS02-2020 (IA) – Sub Topic 1	18.00	(*)	2-5
SU-DS02-2020 (IA) – Sub Topic 2			2-5
SU-DS02-2020 (RIA) – Sub Topic 3	20.00		2-5
SU-DS02-2020 (RIA) – Sub Topic 4			3-6
SU-DS03-2019-2020 (IA)- Sub Topic 1	10.80	(*)	4-5
SU-DS03-2019-2020 (IA)- Sub Topic 2			3-4
SU-DS04-2018-2020 (IA)	20.00	(*)	6-8
Overall indicative budget	68.80		

Research Executive Agency

General info
Call 2020

European Commission

Artificial **Intelligence**

Opening	Closing
12 March 2020	27 August 2020

Topic	Indicative budget (m€)	Info link	Project average EU contribution (m€)	Practitioners (LEAs) minimum	Practitioners Countries minimum
SU-AI01-2020 (CSA)	1.50	(*)	1.50	3	3
SU-AI02-2020 (IA)	17.00	(*)	17.00	5	5
SU-AI03-2020 (CSA)	1.50	(*)	1.50	3	3
Overall indicative budget	20.00				

Research Executive Agency

General info Call 2020

INFRA

Opening	Closing
12 March 2020	27 August 2020

Topic	Indicative budget (m€)	Info link	Project average EU contribution (m€)	Operators minimum	Operator Countries (MS or Associates)
SU-INFRA01-2018-2019-**2020** (IA)	20.70	(*)	7-8	2	2
Overall indicative budget	20.70				

With reference to the topic **SU-INFRA01-2018-2019-2020: "Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe" applicants are informed that the Commission has funded, 3 topics under the INFRA01 Call, on Energy (Gas networks), Transport (Airports) and Sensitive industrial sites and plants.**

Six further projects were funded under the call CIP-2016-2017, in the domains Energy Infrastructures, Transport infrastructure (Port infrastructure) and Water infrastructure, Financial infrastructure, Health infrastructure and Communications infrastructure. Detailed information on all these 6 projects from the CIP-2016-2017 call **can be found in CORDIS following this link.**

Research Executive Agency

Cybersecurity, Digital Privacy and data protection

Legal background

- ✓ *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (**NIS Directive**)*
- ✓ *Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (**Data protection Directive for police and criminal justice Authorities**)*
- ✓ *Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (**eIDAS**)*
- ✓ *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (**General Data Protection Regulation - GDPR**)*

Legal background

- ✓ *Proposal for a Regulation of the European Parliament and of the Council - COM(2017) 10 final of 10.1.2017 (ePrivacy Regulation)*
- ✓ *Regulation on ENISA, the "EU Cybersecurity Agency", and on Information and Communication Technology cybersecurity certification (Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019)* ***EU Cybersecurity Act ,*** *relevant information in (COM(2017)0477 – C8-0310/2017 – 2017/0225(COD))*
- ✓ *(not referred in the Work-programme but relevant to SU-DS04-2018-2020) Commission Recommendation of 3.4.2019 on* ***cybersecurity in the energy sector*** *{SWD(2019) 1240 final}*

Challenges

- *Minimise security risks through integration of state-of-the-art approaches (Artificial Intelligence and automation) to constantly forecast, monitor and update the security of their ICT systems, relying as appropriate on, and reducing the level of human intervention*
- Addressing Security threats to complex ICT infrastructures, via collaboration and seamlessly sharing of information related to security and privacy management between Organisations
- Automatically monitor/ mitigate security risks due to increasing prevalence and sophistication of the Internet of Things (IoT) and Artificial Intelligence (AI) , including those related to data and algorithms
- Increased dependency to trusted third parties

SU-DS02-2020

Intelligent security and privacy management

European Commission

- ***Four sub-topics*** *(A proposal should address* ***one*** *of them)*
  - **Dynamic governance, risk management and compliance (IA – target TRL 7 - EUR 2 to 5M)**
  - **Cyber-threat information sharing and analytics (IA – target TRL 7 - EUR 2 to 5M)**
  - **Advanced security and privacy solutions for end users or software developers (RIA – target TRL 6 - EUR 2 to 5M)**
  - **Distributed trust management and digital identity solutions (RIA – target TRL 5-6 - EUR 3 to 6M)**

- *Proposals should:*
  - **Foresee actions to collaborate with the four pilot projects are launched under Horizon 2020 LEIT ICT, as a result of the call H2020-SU-ICT-2018, topic SU-ICT-03-2018 "Establishing and operating a pilot for a Cybersecurity Competence Network to develop and implement a common Cybersecurity Research & Innovation Roadmap".**
  - **Foresee actions to collaborate with similar ongoing projects funded under H2020, and**
  - **take account of the results and work done in other relevant H2020 projects on cybersecurity/privacy**

Intelligent security and privacy management

European Commission

Important to note :

- ***Dynamic governance, risk management and compliance***
  - **integrate beyond SoA approaches to security and privacy management which are: automated, dynamic and adaptive, allowing to identify the vulnerabilities, threats, such as advanced persistent threats, and attacks (including zero-day attacks)**
  - **include pilots with significant scale involving complex ICT systems and addressing several of the following: forecasting, risk-based situation awareness, evidence-based system and software assessment, visualisation techniques, real-time monitoring and alerts with high level of accuracy, support to fair automated decision-making, run-time adaptation and autonomous recovery from faulty states**
  - **technical, operational, financial and ethical dimensions of cybersecurity should be addressed. Adapted tools, techniques and formats for collaborative security/privacy event management and reporting should be proposed. Solutions involving advanced, highly representative simulation environments (cyber-ranges) might be proposed**

European Commission

Important to note :

- ***Cyber-threat information sharing and analytics –***

Develop/ Test:

- Threat detection frameworks
  i. collaborative, open, and dynamic repositories of information on threats and vulnerabilities;
  ii. Ontologies, taxonomies and models (build on and update existing) ;
  iii. Automated detection , response and recovery;
  iv. Accountability and audit
  v. synchronised real time self- encryption/decryption schemes with recovery capabilities
- technical aspects, but also human aspects
  - behavioural patterns, gender differences, privacy, ethics, sovereignty, psychology, linguistic and cultural boundaries should be considered
- Tools supporting the operations and networks of CERTs/CSIRTs
- Incident response tools and test respective processes for coordinated response to large-scale cross-border cybersecurity incidents and crises

Important to note :

- ***Advanced security and privacy solutions for end users or software developers***
  - develop automated tools for checking the security and privacy of data, systems, online services and applications, in view to support end users or software developers (possibly including developers of AI solutions) in their efforts to select, use and create trustworthy digital services
  - Proposals should address real application cases and at least one of the following services: automatic code generation, code and data auditing, trustworthy data boxes, forensics, certification and assurance, cyber insurance, cyber and AI ethics, and penetration testing

Intelligent security and privacy management

European Commission

Important to note :

- ***Distributed trust management and digital identity solutions***
  - Particular consideration to IoT contexts,
  - Propose, test/pilot (real application cases) innovative approaches addressing / developing:
    i. distributed, dynamic and automated trust management and recovery solutions; and
    ii. novel approaches to manage the identity of persons and/or objects, including self-encryption/decryption schemes. with recovery ability

Intelligent security and privacy management

Anticipated impacts – Short term:

- *reduced number and impact of cybersecurity incidents*
- *efficient and low-cost implementation of the NIS and GDPR Directives*
- *effective and timely co-operation and information sharing between and within organisations as well as self-recovery;*
- *availability of comprehensive, resource-efficient, and flexible security analytics and threat intelligence, keeping pace with new vulnerabilities and threats;*
- *availability of advanced tools and services to the CERTs/CSIRTs and networks of CERTs/CSIRTs;*
- *an EU industry better prepared for the threats to IoT, ICS (Industrial Control Systems), AI and other systems;*
- *self–recovering, interoperable, scalable, dynamic privacy-respecting identity management schemes*

Intelligent security and privacy management

Anticipated impacts – Medium/long term:

- *availability of better standardisation and automated assessment frameworks for secure networks and systems, allowing better-informed investment decisions related to security and privacy;*
- *availability and widespread adoption of distributed, enhanced trust management schemes including people and smart objects;*
- *availability of user-friendly and trustworthy on-line products, services and business;*
- *better preparedness against attacks on AI-based products and systems;*
- *a stronger, more innovative and more competitive EU cybersecurity industry, thus reducing dependence on technology imports;*
- *a more competitive offering of secure products and services by European providers in the Digital Single Market.*

Challenges

- *Personal data breach may facilitate abuse by third parties, including cyber-threats such as coercion, extortion and corruption*
- Protect the freedom, security and privacy, and ensure personal data protection of the citizens in Europe. Need to increase citizens' capacity to modulate the level and accuracy of the monitoring tools used by services (e.g. via cookies, positioning, tokens) and to enable them assess the risk involved in their digital activities and configure their own security, privacy and personal data protection settings
- SMEs& microSMEs are an easier target of attacks(e.g. ransomware). Need for tailored research to support their cybersecurity

- ***Two sub-topics*** *(A proposal should address* ***one*** *of them)*
  - **Protecting citizens' security, privacy and personal data (IA – target TRL 7 - EUR 4 to 5M)**
  - **Small and Medium-sized Enterprises and Micro Enterprises (SMEs&MEs): defenders of security, privacy and personal data protection (IA – target TRL 7 - EUR 3 to 4M)**

Important to note :

- ***Protecting citizens' security, privacy and personal data***
  - **Develop new solutions & applications and technologies for:**
    - i. improving resilience against personal data breaches and cyber threats (e.g. profiling, eavesdropping, data misuse)
    - ii. identifying, removing and reporting potential harmful content and abusive interactions
    - iii. exercising citizens' "right-to-be-forgotten“ and data portability
    - iv. providing transparent information and empowering them to modulate their data protection (e.g. by activating encryption)
    - v. protecting or providing rights for any access/audit/interference with citizens' "smart terminals" or their Internet-based communications in a data protection compliant way
    - vi. developing "one-stop-shop" on-line help-desks services enabling citizens in reporting any cyber or privacy related incident and data breach.

Important to note :

- ***Protecting citizens' security, privacy and personal data***
  - **Build bridges/ synergies with CERTs/CSIRTs**
  - **Involve citizens in the design/ implementation of solutions to ensure the usability and acceptability**
  - **Assurance and transparency about the digital security, privacy and personal data protection levels embedded in products and services should be easily accessed, identified and monitored by all citizens, independently of their physical condition or ICT skills**

Important to note :

- ***Small and Medium-sized Enterprises and Micro Enterprises (SMEs&MEs):*** *defenders of security, privacy and personal data protection*

  i. **Develop targeted, user-friendly and cost-effective solutions enabling SMEs&MEs to:**
     - i. Manage, dynamically monitor, forecast and assess their security, privacy and personal data protection risks in an easy and affordable way
     - ii. Become more aware of vulnerabilities, attacks and risks that influence their business;
     - iii. Build on-line collaboration between SMEs&MEs associations and CERTs/CSIRTs, enabling thus individual SMEs&MEs to report any incident
     - iv. Increase the knowledge sharing in digital security across SMEs&MEs and between SMEs&MEs and larger providers
     - v. Democratize access to tools and solutions of varied sophistication level matching specific needs and available resources

  ii. **Facilitate the participation of user SMEs&MEs in cyber ranges for cybersecurity**

Anticipated impacts

- *Citizens and SMEs&MEs are better protected and become active players in the Digital Single Market, including implementation of the NIS & GDPR Directives.*
- *Security, privacy and personal data protection are strengthened as shared responsibility along all layers in the digital economy, including citizens and SMEs&MEs.*
- *Reduced economic damage caused by harmful cyber-attacks and privacy incidents and data (including personal data) protection breaches.*
- *Pave the way for a trustworthy EU digital environment benefitting all economic and social actors.*

Challenges

- *power outage can have direct impact on the availability of other services;*
- *growing use of digital technologies in EPES and IoT increasingly exposing them to external threats (worms, viruses, hackers and data privacy breaches)*
- *Legacy devices (SCADA/ ICS) were designed in times when cybersecurity was not part of the technical specifications for the system design*
- *A distributed energy system, microgrid operations and/or islanding could be further exploited against cyber-attacks and cascading effects in the EPES*
- *New security approaches are required to ensure integration of renewables to mitigate cyber-attack threats*
- *(New 2020 wp) Alignment with Cybersecurity Act and the Recommendation C(2019)240 final and staff working document SWD(2019)1240 final that identify the main actions required to preserve cybersecurity and be prepared to possible cyberattacks in the energy sector*

European Commission

Scope (1):

- *demonstrate (using sand-boxing, simulation and real life pilots) how the actual EPES can be made resilient to growing and more sophisticated cyber and privacy attacks and data breaches*
- *apply measures to new assets or to existing equipment where data flows were not designed to be cyber protected*
- *Implement activities to make the electric system cyber secure: (i) assessing vulnerabilities and threats of the system in a collaborative manner (involving all stakeholders in the energy components provision supply chain); (ii) on that basis, designing adequate security measures to ensure a cyber-secure system and describing the advantages of the solutions adopted compared to others and which aim to guarantee the level of cybersecurity and resilience vital for EPES in an evolving system; (iii) implementing both organisational and technical measures in representative demonstrator to test the cyber resilience of the system with different types of attacks/severity; and (iv) demonstrating the effectiveness of the measures with a cost-benefit analysis. The activities may include the testing of micro-grid and/or islanding as a means to reduce the vulnerability to cyber-attacks*

European Commission

Scope (2):

The proposals shall also:

- *(i) develop security information and event management system collecting logs and other security-related documentation for analysis that can also be used for information sharing across operators of essential infrastructures and CERTs*
- *(ii) define cybersecurity design principles with a set of common requirements to inherently secure EPES*
- *(iii) formulate recommendations for standardisation and certification in cybersecurity at component, system and process level; and*
- *(iv) propose policy recommendations on EU exchange of information*

Notes:
The proposals are encouraged to include the following types of entities: TSO, DSO, electricity generators, utilities, equipment manufacturers, aggregators, energy retailers, and technology providers
The proposals may refer to Industry 4.0 and other proposals and/or projects dealing with cybersecurity in energy. They should also foresee activities and envisage resources for clustering (in particular under the BRIDGE initiative)

Anticipated impacts (1)

- *Built/increase resilience against different levels of cyber and privacy attacks and data breaches (including personal data breaches) in the energy sector.*
- *Ensured continuity of the critical business energy operations and resilience against cyberattacks, including large scale, demonstrating effective solutions to :*
  - **a) the real-time constraints of an electric system,**
  - **b) barriers to the cascading effect and**
  - **c) the adaptation of legacy equipment or their coexistence with state of the art technology.**

Anticipated impacts (2)

- *The energy sector is better enabled to easily implement the NIS Directive*
- *A set of standards and rules for certification of cybersecurity components, systems and processes in the energy sector will be made available*
- *Cyber protection policy design and uptake at all levels from management to operational personnel, in the energy sector*
- *Manufacturers providing more accountability and transparency, enabling third parties monitoring and auditing the privacy, data protection and security of their energy devices and systems.*

Artificial Intelligence

Artificial Intelligence (AI) refers to any machine or algorithm that is capable of observing its environment, learning, and that, based on the knowledge and experience gained, can take intelligent actions or propose decisions. There are many different technologies that fall under this broad AI definition and they very much refer to machine learning, data science, robotics, internet of things and use of big data

Legal background

- ✓ *Regulation (EU) 2016/679 95/46/EC (General Data Protection Regulation - GDPR)*
- ✓ *JOIN(2017) 450 final - Resilience, Deterrence and Defense: Building strong cybersecurity for the EU*
- ✓ *"Artificial Intelligence – A European Perspective", EUR 29425 EN, 2018*
- ✓ *COM(2018) 237 - Artificial Intelligence for Europe*
- ✓ *COM(2018) 795 final - Coordinated Plan on Artificial Intelligence*
- ✓ *Guidelines of the European Group on Ethics in Science and New Technologies (regulatory framework to be ready in March 2019)*

Relevant Initiatives/ projects referrenced into the work programme

- ✓ *ASGARD project - aims to contribute to LEA Technological Autonomy, by building a sustainable, long-lasting community for LEAs and the R&D industry*
- ✓ *SIRIUS, launched by Europol in October 2017, is a secure web platform for law enforcement professionals in internet-facilitated crime investigations, with a special focus on counter-terrorism.*
- ✓ *EPE (Europol Platform for Experts) is a secure, collaborative web platform for specialists in a variety of law enforcement areas.*
- ✓ *Networks of practitioners such as ILEAnet and I-LEAD*
- ✓ *AI4EU developing the AI-on-demand platform, central access point to AI resources and tools:.*
- ✓ *Partnership for Robotics in Europe*
- ✓ *Big data projects of LEIT such as AEGIS, Lynx or FANDANGO*
- ✓ *IoT projects e.g. MONICA, SecureIoT*

Challenges

- *Need to better understand (From LEA's perspective) how AI-based systems, services and products could enhance the objectives of the security sector; how AI technologies can be protected from attacks; how to address any potential abuse of AI for malicious purposes; how to establish cybersecurity requirements for AI*

Scope

- *Proposals under this topic should provide an EU AI roadmap for LEAs, meeting their specific operational and cooperation needs, identifying:*
- *the key areas in which AI would be beneficial for LEAs and those it could pose a threat,*
- *means of prevention and mitigation of malicious use of AI*
- *provide recommendations for further work*

SU-AI02-2020

Secure and resilient Artificial Intelligence technologies, tools and solutions in support of Law Enforcement and citizen protection, cybersecurity operations and prevention and protection against adversarial Artificial Intelligence(IA – TRL 7-8, EUR 17M)

European Commission

Challenges

- *Security dimension of AI a matter of priority. How to mostly benefit from the AI based technologies in enhancing EU's resilience against newly emerging security threats*
- *"interoperability", "security by design" and "ethics by design" so that developed AI systems are trustworthy, accountable, responsible and transparent*

Scope

- *Building on best practices (such as ASGARD project) develop AI tools (e.g. robotics or Natural Language Processing) and solutions in support of LEAs daily work to better prevent, detect and investigate criminal activities and terrorism and monitor borders*
- *Develop cybersecurity tools and solutions for the protection of AI based technologies in use or to be used by LEAs*
- *Exploit AI technologies for cybersecurity operation purposes, including the prevention, detection and response of cybersecurity incidents through advanced threat intelligence and predictive analytics technologies and tools targeting Cybercrime units , CSIRTs, PCCCs, Joint Investigation Teams*
- *Tackle the dual nature (resilience/ protection against adversarial/ malicious AI)*

Challenges

- *lack of transparency of AI technologies and tools complicates their acceptance by users and citizens. Ethical and secure-by-design algorithms are necessary to build trust in this technology. Engagement of civil society is crucial. There is a need to find ways to build a human-centred and socially driven AI*
- *Possible side effects of AI need to be considered carefully, both from the point of view of citizens and from the point of view of Law Enforcement:*

Scope

- *exhaustive analysis of human, social, gender and organisational aspects related to the use of AI tools*
- *suggest approaches that are needed to overcome these concerns and that stimulate the acceptance of AI tools by civil society and by Law Enforcement*
- *Resources should become available for clustering*

Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe

Challenges

- *A comprehensive, yet installation-specific, approach is needed to secure existing or future, public or private, connected and interdependent installations, plants and systems*
- New security solutions must be more accurate, efficient and cost-effective, and possibly more automated than the ones currently available

Projects should:

a) assess in detail all aspects of interdependent physical & cyber threats

b) demonstrate the accuracy of their risk assessment approach

c) develop improved real-time, evidence-based security management of physical and cyber threats considering ageing

d) provide scenarios and recommendations for policy planning, engagement of the civil society, and investment measures encompassing all aspects of prevention-detection-response-mitigation

SU-INFRA01-2018-2019-2020

Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe

European Commission

Scope in 2020:

- *While keeping the coverage of the assessment of risks, prevention, detection, response and mitigation of consequences, proposals should also address the interrelations between different types of critical infrastructure with the objective of developing tools and methods to minimise cascading effects and allow rapid recovery of service*
- *Consortia should involve the largest variety of relevant beneficiaries, including infrastructure owners and operators, first responders, industry (SMEs incl), technologists and social scientists*
- *International cooperation is encouraged, and in particular with international research partners in the context of the International Forum to Advance First Responder Innovation*

Notes

- List of infrastructures excluded from the Call will be published on the Funding and Tenders Portal
- Up to TRL7 expected
- contribution from the EU of about EUR 7 to 8 million per project

Research Executive Agency

Anticipated impacts – Short term:

- *State-of-the-art analysis of physical/cyber detection technologies and risk scenarios, in the context of a specific critical infrastructure.*
- *Analysis of both physical and cyber vulnerabilities of a specific critical infrastructure, including the combination of both real situation awareness and cyber situation awareness within the environment of the infrastructure.*
- *In situ demonstrations of efficient and cost-effective solutions to the largest audience, beyond the project participants.*

Anticipated impacts – Medium term

- *Innovative (novel or improved), integrated, and incremental solutions to prevent, detect, respond and mitigate physical and cyber threats to a specific Critical Infrastructure.*
- *Innovative approaches to monitoring the environment, to protecting and communicating with the inhabitants in the vicinity of the critical infrastructure.*
- *Security risk management plans integrating systemic and both physical and cyber aspects.*
- *Tools, concepts, and technologies for combatting both physical and cyber threats to a specific critical infrastructure.*
- *Where relevant, test beds for industrial automation and control system for critical infrastructure in Europe, to measure the performance of critical infrastructure systems, when equipped with cyber and physical security protective measures, against prevailing standards and guidelines.*
- *Test results and validation of models for the protection of a specific critical infrastructure against physical and cyber threats.*
- *Establishment and dissemination throughout the relevant user communities of specific models for information sharing on incidents, threats and vulnerabilities with respect to both physical and cyber threats.*

Anticipated impacts – Long term

- *Convergence of safety and security standards, and the pre-establishment of certification mechanisms.*
- *Secure, interoperable interfaces among different critical infrastructures to prevent from cascading effects.*
- *Contributions to relevant sectorial frameworks or regulatory initiatives.*

European Commission

Thank you!

Questions?

Research Executive Agency