H2020 WP2018-2020
Cybersecurity and Digital Privacy

Overview
24th October 2018
Policy context (1/3)

- NIS Directive – Directive (EU) 2016/1148 of 6/7/2016 concerning measures for a high common level of security of network and information systems across the Union;
- General Data Protection Regulation (GDPR) - Regulation (EU) 2016/679 of 27.4.2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data;
Policy context (2/3)

- Contractual Public-Private Partnership on Cybersecurity – July 2016;
  - Counterpart: European Cybersecurity Organization (ECSO)
  - Strategic Research and Innovation Agenda (SRIA)
Policy context (3/3)

- State of the Union 2017 - speech of the President of the Commission (13/09/2017)
- Cybersecurity Package 2017 (13/09/2017)
  - Joint Communication JOIN(2017)450 - Resilience, Deterrence and Defence: Building strong cybersecurity for the EU

New:
Common 'virtual' call titles and call identifiers

- For calls evaluated by DG CONNECT, two focus areas are relevant, namely:

  1. Digitising and transforming European industry and services:
     H2020-DT-2018-2020

  2. Boosting the effectiveness of the Security Union:
     H2020-SU-ICT-2018-2020

- Contribution to the cPPP on Cybersecurity
Focus Area

'Boosting the effectiveness of the Security Union'

Covers the main actions in Work Programmes which contribute to developing the EU as a Security Union:

- reacting to & recovering from natural and man-made disasters
- fighting crime (including cybercrime) and terrorism
- improving border security
- protecting infrastructure and public spaces
- digital security and privacy
- better understanding of societal contexts of security challenges

SDGs:

Total indicative budget (2018-2020):
EUR 1 billion
Focus Area

'Boosting the effectiveness of the Security Union'

New solutions and technologies for end-users (police, customs, firefighters, etc)

Involving researchers, industry and end-users in the entire research cycle

Objectives

Promoting market uptake of research results

A strong security industry underpinning EU autonomy
'Boosting the effectiveness of the Security Union'

**Focus Area**

- **Cyber and Digital Security**: all topics in calls 'Cyber Security' (LEIT-ICT) and 'Digital Security' (SC7), €290 million

- **Space (LEIT-Space)**: topics in calls 'Space 2018-2020' and EGNSS market uptake 2019-2020', €90 million

- **Health (SC1)**: topics in Call 'Trusted digital solutions and Cybersecurity in Health and Care', €36 million

- **Energy (SC3)**: contribution to topic on Electrical Power and Energy System in SC7 call 'Digital Security', €20 million

- **Inclusive Societies (SC6)**: topics on trafficking of cultural goods, drivers of violent extremism, addressing radicalisation through inclusion, €30 million

- **Secure Societies (SC7)**: all topics in calls 'Security' and 'Infrastructure Protection', €615 million
Cybersecurity in WP 2018-2020

5.i. Information and Communication Technologies (LEIT-ICT):
- Cybersecurity Call;
- Cybersecurity embedded in several other topics;

14. Societal Challenge 7 - Secure Societies (SC7):
- Digital Security (DS) Call: addresses cybersecurity preparedness; digital security, privacy, data protection in critical sectors; cybersecurity in energy;
- Protecting the infrastructure of Europe and the people in the European smart cities (INFRA) Call: addresses combined physical and cyber threats;
Cybersecurity Call in LEIT-ICT

SU-ICT-01-2018: Dynamic countering of cyber-attacks (IA)

SU-ICT-02-2020: Building blocks for resilience in evolving ICT systems (RIA)

SU-ICT-03-2020: Advanced cybersecurity and digital privacy technologies

SU-ICT-04-2019: Quantum Key Distribution testbed (IA)
Other topics in LEIT-ICT relevant for Cybersecurity & Digital Privacy

**ICT-08-2019**: Security and resilience for collaborative manufacturing environments

**ICT-13-2018-2019**: Supporting the emergence of data markets and the data economy

**ICT-20-2019-2020**: 5G Long Term Evolution

...and more along the WP2018-20 as this is a cross-cutting issue
## Call Cybersecurity: 2019 Planning

### Opening dates - deadlines for submission

<table>
<thead>
<tr>
<th>Topic(s)</th>
<th>SU-ICT-02-2020 (RIA)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Opening</strong></td>
<td>25 Jul 2019</td>
</tr>
<tr>
<td><strong>Deadline</strong></td>
<td>19 Nov 2019</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Topic</th>
<th>Instrument</th>
<th>Funding (M EUR)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SU-ICT-02-2020</td>
<td>RIA</td>
<td>47.00</td>
</tr>
</tbody>
</table>
Digital Security call in SC7

SU-DS01-2018: Cybersecurity preparedness - cyber range, simulation and economics

SU-DS02-2020: Management of cyber-attacks and other risks


SU-DS05-2018-2019: Digital security, privacy, data protection and accountability in critical sectors
INFRA call in SC7

SU-INFRA01-2018-2019-2020: Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe

SU-INFRA02-2019: Security for smart and safe cities, including for public spaces
## Call Digital Security: 2019 Planning

### Opening dates - deadlines for submission

<table>
<thead>
<tr>
<th>Topic(s)</th>
<th>SU-DS03-2019-2020 (IA)</th>
<th>SU-DS05-2018-2019 (RIA &amp; IA)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Opening</strong></td>
<td></td>
<td>14 March 2019</td>
</tr>
<tr>
<td><strong>Deadline</strong></td>
<td></td>
<td>22 August 2019</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Topic</th>
<th>Instrument</th>
<th>Funding (M EUR)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SU-DS03-2019-2020</td>
<td>IA</td>
<td>13</td>
</tr>
<tr>
<td>SU-DS05-2018-2019</td>
<td>RIA</td>
<td>10</td>
</tr>
<tr>
<td>SU-DS05-2018-2019</td>
<td>IA</td>
<td>10</td>
</tr>
</tbody>
</table>
## Call INFRA : 2019 Planning

### Opening dates - deadlines for submission

| Topic(s)                                      | SU-INFRA01-2018-2019-2020 (IA)  
<table>
<thead>
<tr>
<th></th>
<th>SU-INFRA02-2019 (IA)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Opening</strong></td>
<td>14 March 2019</td>
</tr>
<tr>
<td><strong>Deadline</strong></td>
<td>22 August 2019</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Topic</th>
<th>Instrument</th>
<th>Funding (M)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SU-INFRA01-2018-2019-2020</td>
<td>IA</td>
<td>22.00</td>
</tr>
<tr>
<td>SU-INFRA02-2019</td>
<td>IA</td>
<td>16.00</td>
</tr>
</tbody>
</table>
Thank you for your attention!

Questions
SU-DS03-2019-2020
Digital Security and privacy for citizens and Small and Medium Enterprises and Micro Enterprises
What are you looking for?

- Citizens and SMEs&MEs are better protected and become active players in the Digital Single Market, including implementation of the NIS directive and the application of the General Data Protection Regulation.
- 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
3. Is this new or has it been called before?

This topic is linked with previous WP topic
DS-02-2016 Cyber Security for SMEs, local public administration and Individuals

It is linked to other topics in the current WP:
Cybersecurity Call in LEIT – ICT
Digital Security Call in SC7
INFRA Call in SC7
SU-DS03-2019-2020 – topic evolution

4. Current project portfolio (if relevant)

FORTIKA

GHOST

SMESEC

COMPACT

CS-AWARE
6. Is there a key group of actors (eg. cPPP or other) driving this?

DG CONNECT
Cybersecurity cPPP
Future Outlook

8. Do you have information about future trends, emerging initiatives, roadmaps, key players in this area? How are you bridging to Horizon Europe?

Proposal for a European Cybersecurity Competence Network and Centre
(COM 2018) 630 final
Upcoming events / Information days

9. Please list upcoming information days and other events of relevance to this area

**ICT 2018: Imagine Digital - Connect Europe,**

**Vienna 4-6 December 2018**
Future Outlook

8. Do you have information about future trends, emerging initiatives, roadmaps, key players in this area? How are you bridging to Horizon Europe?
Upcoming events / Information days

9. Please list upcoming information days and other events of relevance to this area
Digital security, privacy, data protection and accountability in critical sectors
1. What are you looking for? **Short term (1/3):**

- The technological and operational enablers of co-operation in Response and Recovery will contribute to the development of the CSIRT Network across the EU, which is one of the key targets of the NIS Directive.
- Identified relevant generic and specific aspects related to cybersecurity and digital privacy in the respective critical domains/sectors addressed.
- Advanced holistic systems and innovative proof concepts for managing cybersecurity and privacy risks in the respective critical domains/sectors addressed.
What are you looking for? **Short term (2/3):**

- Advances in the state-of-the-art analysis of specific aspects of the respective critical domains/sectors addressed, such as related cyber threats, attacks and vulnerabilities;
- Sound analysis of cascading effects of specific related cyber threats within the supply chain of the respective critical domains/sectors addressed.
- Improved cybersecurity information sharing and collaboration among stakeholders of the respective critical domains/sectors addressed, and with CERTs/CSIRTs.
What are you looking for? **Short term (3/3):**

- More targeted and acceptable security management solutions addressing specificities of the respective critical domains/sectors addressed.
- Trigger the fast adoption of cybersecurity/privacy/personal data protection best practices in the respective critical domains/sectors addressed.
What are you looking for? **Medium term (1/2)**

- Better response and recovery technologies and services that will help organizations in the respective critical domains/sectors addressed to significantly reduce the impact of propagated and cascaded threats, vulnerabilities and breaches.

- Enhanced protection against emerging novel advanced threats in the respective critical sectors/domains addressed.
What are you looking for? Medium term (2/2)

- Improved security governance of the respective critical domains/sectors addressed
- Greater and more mature EU cybersecurity market in the respective critical domains/sectors addressed.
- Reduce the impact of breaches with various levels of success in penetrating the defences.
Topic SU-DS05-2018-2019

What are you looking for? *Long term*

- Better cybersecurity for specific standards in the respective critical domains/sectors addressed, that will trigger fast adoption of best practices in the related industry.
- Established trust chains among all entities in the ecosystems of the respective critical domains/sectors addressed.
- Better implementation of the relevant EU legislation (e.g. NIS, eIDAS, GDPR) in the respective critical domains/sectors addressed.
- Companies/organisations in the respective critical domains/sectors addressed are more willing to promote cyber security, privacy and personal data protection in the whole EU-specific ecosystem.
SU-DS05-2018-2019 – topic evolution

3. Is this new or has it been called before?

This topic is mainly new.

It is linked to other topics in the current WP:
Cybersecurity Call in LEIT – ICT
Digital Security Call in SC7
INFRA Call in SC7
6. Is there a key group of actors (eg. cPPP or other) driving this?

DG CONNECT
Cybersecurity cPPP
8. Do you have information about future trends, emerging initiatives, roadmaps, key players in this area? How are you bridging to Horizon Europe?

Proposal for a European Cybersecurity Competence Network and Centre
(COM 2018) 630 final
Upcoming events / Information days

9. Please list upcoming information days and other events of relevance to this area

ICT 2018: Imagine Digital - Connect Europe,

Vienna 4-6 December 2018
SU-INFRA01-2018-2019-2020

Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe
What are you looking for? **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.
What are you looking for? **Medium Term (1 of 2)**

- 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.
What are you looking for? **Medium Term (2 of 2)**

- 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
What are you looking for? **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.
Topic SU-INFRA01-2018-2019-2020

3. Is this new or has it been called before?

the predecessor topic in WP2016-2017 was

CIP-2016-2017 Prevention, detection, response and mitigation of the combination of physical and cyber threats to the critical infrastructure of Europe.

In 2018 the topic SU-INFRA01-2018-2019-2020 was also called.
4. Current project portfolio

SAURON  https://www.sauronproject.eu/
DEFENDER  http://defender-project.eu/
STOP-IT  https://stop-it-project.eu/
6. Is there a key group of actors (eg. cPPP or other) driving this?

DG HOME
DG CONNECT
Cybersecurity cPPP
SU-INFRA01-2018-2019-2020

7. Are there any additional / background documents?

*NIS Directive*
Future Outlook

8. Do you have information about future trends, emerging initiatives, roadmaps, key players in this area? How are you bridging to Horizon Europe?

Proposal for a European Cybersecurity Competence Network and Centre
(COM 2018) 630 final
Upcoming events / Information days

9. Please list upcoming information days and other events of relevance to this area

ICT 2018: Imagine Digital - Connect Europe,

Vienna 4-6 December 2018
SU-INFRA02-2019

Security for smart and safe cities, including for public spaces
1. What are you looking for? (1/2)

- Creation of dedicated, harmonised, advanced cybersecurity solutions for smart cities adopting common approaches with all involved stakeholders (e.g. administrators of smart city/port/transport) balancing their – sometimes conflicting – goals (e.g. urban development, efficiency, growth, competitiveness, resilience).

- In situ demonstrations of efficient and cost-effective solutions to the largest audience, beyond the project participants.

- An easier level of integration by developing a holistic cyber-security framework for smart cities that benefits all smart infrastructures hosted within it (e.g. smart buildings, smart ports, smart railways, smart...
1. **What are you looking for? (2/2)**

- IoT ecosystems (rather than distributed IoT infrastructures) built adopting common approaches in their cybersecurity management, achieving economies of scale (e.g. avoiding duplication of efforts in the analysis of IoT data, selection of cybersecurity controls).
- Novel concepts of operations taking account of multiple, heterogeneous data sources and the social media.
- Novel tools and systemic approaches to protect citizens against threats to soft targets in a Smart City.
SU-INFRA02-2019 – topic evolution

3. Is this new or has it been called before?

This topic is mainly new.

It is linked to other topics in the current WP: Cybersecurity Call in LEIT – ICT Digital Security Call in SC7 INFRA Call in SC7
6. Is there a key group of actors (e.g. cPPP or other) driving this?

DG HOME
DG CONNECT
Cybersecurity cPPP
8. Do you have information about future trends, emerging initiatives, roadmaps, key players in this area? How are you bridging to Horizon Europe?

Proposal for a European Cybersecurity Competence Network and Centre
(COM 2018) 630 final
Upcoming events / Information days

9. Please list upcoming information days and other events of relevance to this area

**ICT 2018: Imagine Digital - Connect Europe, Vienna 4-6 December 2018**
SU-ICT-02-2020

Building blocks for resilience in evolving ICT systems
What are you looking for? **Short/medium term**

- Improved market opportunities for the EU vendors of security components.
- Increased trust both by developers using/integrating the ICT components and by the end-users of IT systems and services.
- Protect the privacy of citizens and trustworthiness of ICT.
- Acceleration of the development and implementation of certification processes.
Topic SU-ICT-02-2020

What are you looking for? **Long term**

- Advanced cybersecurity products and services will be developed improving trust in the Digital Single Market.
- The use of more harmonized certification schemes will increase the business cases for cybersecurity services as they will become more reliable.
- Validation platforms will provide assessments with less effort compared with nowadays and assure a better compliance with relevant regulations and standards.
Topic SU-ICT-02-2020 – topic evolution

3. Is this new or has it been called before?

This topic is linked with previous WP topic ICT-32-2014 Cybersecurity, Trustworthy ICT

it is linked to other topics in the current WP: Cybersecurity Call in LEIT – ICT Digital Security Call in SC7 INFRA Call in SC7
6. Is there a key group of actors (eg. cPPP or other) driving this?

DG CONNECT
Cybersecurity cPPP
Future Outlook

8. Do you have information about future trends, emerging initiatives, roadmaps, key players in this area? How are you bridging to Horizon Europe?

Proposal for a European Cybersecurity Competence Network and Centre
(COM 2018) 630 final
Upcoming events / Information days

9. Please list upcoming information days and other events of relevance to this area

ICT 2018: Imagine Digital - Connect Europe,

Vienna 4-6 December 2018