

Diskussion

Digital Security/Critical infrastructure protection

hans.frennberg@foi.se

Diskussioner

Upplägg

13.45-14.30

Digital Security/Critical Infrastructure Protection

- Mer detaljerad diskussion och analys kring utlysningarna
- Önskvärda framtida förmågor
- Vilka svenska utvecklingsbehov kan tillvaratas i de olika utlysningarna
- Finns tentativa projektidéer i gruppen?

DS - Digital Security

- ICT-driven transformations bring opportunities across important sectors but also **vulnerabilities to critical infrastructures and digital services**
- Can have **significant consequences** on the functioning of society, economic growth and the technological innovation potential of Europe.
- Cross-cutting; *ICT, Health and Security*
- **Assurance and Certification**
- **Improved addressing of basic cyber security threats**
 - SMEs, local public administration and Individuals
- **Digital security for eHealth related solutions**
- **Economic metrics of cyber security**
 - cost-benefit framework, incentives and business models
- **Improved dialogue**, within the EU and internationally

CIP - Critical infrastructure protection

- **Societies and their economics are strongly dependent upon the operation of our countries' infrastructure**
- **Disruptions may result from many kinds of hazards and physical and/or cyber-attacks on installations and systems**
- **Comprehensive, yet installation-specific approach is needed**
 - Water Systems,
 - Energy Infrastructure (power plants and distribution)
 - Transport Infrastructure and means of transportation
 - Communication Infrastructure
 - Health Services
 - Financial Services
- **Solutions to increase security and resilience of all functions performed**
 - Prevention, detection, response, and in case of failure, mitigation of consequences
 - Physical, cyber or combined threats, and potential cascading effects

DS / CIP, topics 2016

- DS-01-2016: Assurance and Certification for Trustworthy and Secure ICT systems, services and components
- DS-02-2016: Cyber Security for SMEs, local public administration and Individuals
- DS-03-2016: Increasing digital security of health related data on a systemic level
- DS-04-2016: Economics of Cybersecurity
- DS-05-2016: EU Cooperation and International Dialogues in Cybersecurity and Privacy Research and Innovation

- CIP-01-2016-2017: Prevention, detection, response and mitigation of the combination of physical and cyber threats to the critical infrastructure of Europe.

Digital Security, topics 2016

- **DS-01-2016: Assurance and Certification for Trustworthy and Secure ICT systems, services and components**
- Assurance
- Certification
- Support actions
 - Building trustworthiness
 - Engage with multidisciplinary communities and stakeholders

Digital Security, topics 2016

- **DS-02-2016: Cyber Security for SMEs, local public administration and Individuals**
- Expected impact
 - Increased resilience against widespread cyber security threats facing SMEs, local public administrations and individuals.
 - Increased effectiveness of cybersecurity solutions through usability advancements and increased automation.

Digital Security, topics 2016

- **DS-03-2016:Increasing digital security of health related data on a systemic level**
- Expected Impact:
 - Better acceptance of eHealth solutions among patients
 - Encouraging Member States to widen the use of eHealth
 - Ensuring the right of patients to cross-border healthcare
 - Supporting the development of European legal and operational standards for cross-border data exchange and patient privacy protection
 - Better protection against unauthorised use of personal data, breach of confidentiality and cybercrime
 - Increasing the awareness of stakeholders, private and public ones, on the current level of data security.
 - Definition of clear architectures that will promote interoperability between eHealth solutions

Digital Security, topics 2016

- **DS-04-2016:Economics of Cybersecurity**
- Cybersecurity cost-benefit framework
- Incentives and business models
- Expected Impact:
 - Improved societal understanding of information security failures and how they should be addressed.
 - Improved risk-based information security investment.
 - Increased societal resilience to cyber security risks through more efficient and effective institutional and incentives structures.
 - Progress beyond the state of the art in information security economics models.

Digital Security, topics 2016

- **DS-05-2016:EU Cooperation and International Dialogues in Cybersecurity and Privacy Research and Innovation**
- Expected Impact:
 - Identify and prioritise R&I topics across the EU.
 - Foster and promote European cybersecurity innovation activities
 - Increase the international visibility of EU activities in cybersecurity.
 - Identify potential European and international common approaches in addressing cybersecurity challenges from a R&I as well as a governance and institutional perspective.

Critical infrastructure protection, topics 2016

- **CIP-01-2016-2017: Prevention, detection, response and mitigation of the combination of physical and cyber threats to the critical infrastructure of Europe.**
- Water Systems, Energy Infrastructure (power plants and distribution), Transport Infrastructure and means of transportation, Communication Infrastructure, Health Services, Financial Services.

Critical infrastructure protection, topics 2016

- **CIP-01-2016-2017: Prevention, detection, response and mitigation of the combination of physical and cyber threats to the critical infrastructure of Europe.**
- Expected Impact:
 - Short term:
 - State-of-the-art analysis of physical/cyber detection technologies and risk scenarios
 - Analysis of both physical and cyber vulnerabilities of a specific critical infrastructure,.
 - Medium term
 - Innovative, solutions to prevent, detect, respond and mitigate physical and cyber threats.
 - Innovative approaches to monitoring the environment, to protecting and communicating with inhabitants
 - In situ demonstrations of efficient and cost-effective solutions.
 - Security risk management plans integrating systemic and both physical and cyber aspects.
 - Tools, concepts, and technologies for combatting both physical and cyber threats
 - Where relevant, test beds for industrial automation and control system for critical infrastructure
 - Test results and validation of models
 - Establishment and dissemination throughout the relevant user communities
 - Long term
 - Convergence of safety and security standards, and the pre-establishment of certification mechanisms.

Utlysningarna Webportalen

Innehåller all information om utlysningarna

- *Challenge*
- *Scope*
- *Expected impact*
- *Projekttyp*
- *Deadlines*
- Teknikmognad
- Ungefärlig budget
- Villkor

The screenshot displays the 'RESEARCH & INNOVATION Participant Portal' website. The page title is 'Calls for Proposals'. On the left, there is a sidebar with 'EU Programmes 2014-2020' and 'FP7 & CIP Programmes 2007-2013'. The main content area shows a list of 'Calls for Proposals' under the 'Horizon 2020' section. A red circle highlights the 'Secure societies - protecting freedom and security of Europe and its citizens' call. Below the list, there are several call cards with titles like 'CRITICAL INFRASTRUCTURE PROTECTION', 'SECURITY', 'Digital Security Focus Area', 'Disaster-resilience: safeguarding and securing society...', 'Border Security and External Security', 'Fight against crime and Terrorism', 'Digital Security: Cybersecurity, Privacy and Trust', and 'Industrial Leadership'. A red arrow points to the 'Industrial Leadership' card. At the bottom, there is a footer with '© European Commission' and navigation links for 'HORIZON 2020', 'RESEARCH ON EUROPA', 'CORDIS', and 'OLAF'.

<http://ec.europa.eu/research/participants/portal>

Samverkansplattform H2020
säkra samhällen

Utlysningarna - teknikmognad

Technology readiness levels (TRL)

I utlysningstexten anges det ofta vilken “mognadsgrad” ett projekt bör sikta på

TRL 1	basic principles observed
TRL 2	technology concept formulated
TRL 3	experimental proof of concept
TRL 4	technology validated in lab
TRL 5	technology validated in relevant environment
TRL 6	technology demonstrated in relevant environment
TRL 7	system prototype demonstration in operational environment
TRL 8	system complete and qualified
TRL 9	actual system proven in operational environment

Utlysningssområden 2016

- **CIP - Critical infrastructure protection**
Budget 20 M€, deadline 25/8 2016
- **SEC - Security**
 - **DRS - Disaster Resilience**
Budget 19.5 M€, deadline 25/8 2016
 - **FCT - Fight Against Crime and Terrorism**
Budget 44.25 M€, , deadline 25/8 2016
 - **BES - Border Security and External Security**
Budget 34 M€, , deadline 25/8 2016
 - **GM – General Matters**
Budget 15,5 M€, , deadline 25/8 2016
- **DS - Digital Security**
Budget 63.5 M€, deadlines 16/2, 12/4 och 25/8

Inför eftermiddagens diskussioner

Potentiella intresseområden - förslag

FCT

- Fortifikationsverket
- FRA
- Kustbevakningen
- LFV
- Polismyndigheten
- Tullverket

BES

- Kustbevakningen
- Polismyndigheten
- Tullverket

DRS

- Fortifikationsverket
- Jordbruksverket
- Lantmäteriet
- LFV
- Lst / regioner
- Polismyndigheten
- Statens Veterinärmedicinska Anstalt
- Landsting

DS+CIP

- Arbetsförmedlingen, SOES ordf
- Fortifikationsverket
- FRA
- Lantmäteriet
- LFV
- Lst / regioner
- Riksgälden
- Landsting