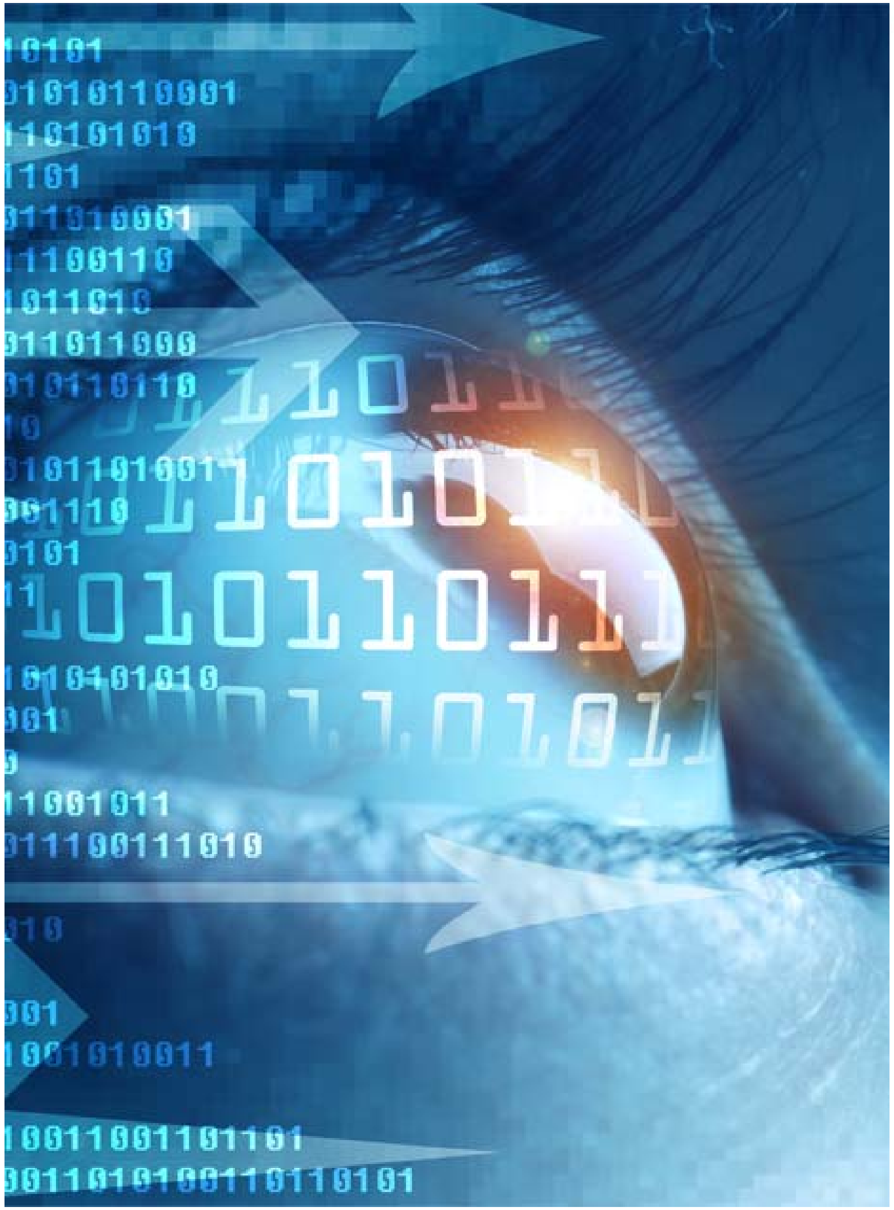
European Commission



Horizon 2020 Secure Societies WP 2016 Infoday

DG Migration and Home Affairs

DG Communication Networks, Content and Technology

Warsaw 10th May 2016

Matching pan-European solutions to pan-European needs

- Contributing to the implementation of latest EU security policies
- Boosting the "Europeanisation" of practitioners' demand for innovative solutions and the industrial offers of innovations
- Combining cyber and physical aspects of security
- Increased number of PCPs

WP 2016-2017

- **30 topics**. Total budget: €382 million
- **Areas** of activity:
  - Critical Infrastructure Protection
  - Disaster-resilience: safeguarding and securing society
  - Fight against Crime and Terrorism
  - Border Security and External Security
  - Digital Security
- **Call dates**:

2016: Opening: 15 Mar 2016, Deadline: 25 Aug 2016
2017: Opening: 01 Mar 2017, Deadline: 24 Aug 2017

EU policy initiatives 1/3

The European Agenda on Security

COM(2015) 185 final (28 April 2015)

http://europa.eu/rapid/press-release_IP-15-4865_en.htm

*"**Research and innovation** is essential if the EU is to keep up-to-date with evolving security needs. Research can identify new security threats and their impacts on European societies. It also contributes to creating social trust in research-based new security policies and tools. Innovative solutions will help to mitigate security risks more effectively by drawing on knowledge, research and technology.*

The European Agenda on Migration

COM(2015) 240 final (13 May 2015)

http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/european-agenda-migration/background-information/index_en.htm

EU policy initiatives 2/3

- **2008 EU Action Plan on Enhancing the Security of Explosives**
- **Regulation (EU) No 98/2013 on the marketing and use of explosives precursors**
- **Final implementation report of the EU Internal Security Strategy 2010-2014**
  COM(2014) 365 final
- **Towards a stronger European disaster response: the role of civil protection and humanitarian assistance,**
  COM(2010)600
- **2006 EU Action Plan on combating terrorism**
- **The Security Industry Policy Action Plan**
  COM (2012)417 final

EU policy initiatives 3/3

- **Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace** COM (2013) 1
- **The EU Strategy towards the Eradication of Trafficking in Human Beings 2012–2016,** COM(2012) 286
- **European Programme for Critical Infrastructure Protection (EPCIP), COM(2006)786**
- **Civilian Headline Goal 2008**
- **EU Maritime Security Strategy** *(adopted by Council - General Affairs on 24/6/2014)* **and its action plan** *(adopted by Council - General Affairs – 16/12/2014)*
- **EU Civil Protection Mechanism** (Decision 1313/2013/EU)

Call - CRITICAL INFRASTRUCTURE PROTECTION

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

The reasoning behind the CIP call

The lines between the physical and the cyber worlds are increasingly blurred. Recent events demonstrate the increased interconnection among the impact of hazards, of the two kinds of attacks and, conversely, the usefulness for operators to combine cyber and physical security-solutions to protect installations of the critical infrastructure of Europe: A comprehensive, yet installation-specific approach is needed

Exclusive list of CI

- Water Systems,
- Energy Infrastructure (power plants and distribution [in an all-encompassing meaning]);
- Transport Infrastructure and means of transportation;
- Communication Infrastructure;
- Health Services;
- Financial Services.

Scope

- Prevention, detection, response, and in case of failure, mitigation of consequences over the life span of the infrastructure;
- All aspects of both physical and cyber threats and incidents, but also systemic security management issues, interconnections, and cascading effects;
- Sharing information with the public in the vicinity of the installations, protection of rescue teams, security teams and monitoring teams.

Expected Impact

- **Short term:**

  Analysis of physical/cyber detection technologies as well as vulnerabilities.

- **Mid term:**

  Tested solutions to prevent, detect, respond and mitigate physical and cyber threats.

- **Long term:**

  Convergence of safety and security standards, and the pre-establishment of certification mechanisms.

Eligibility criteria

At least **2 operators** of the chosen type of critical infrastructure operating in **2 countries** must be beneficiaries (possibly, but not necessarily: coordinator) of the grant agreement and should be directly involved in the carrying out of the tasks foreseen in the grant. The participation of **industry able to provide security** solutions is required.

Technical aspects

- A maximum of one project will be selected per critical infrastructure. Unsuccessful proposals can submit on the second year if the CI is not yet covered
- The participation of SMEs is strongly encouraged.
- International cooperation in research and innovation is encouraged.
- Indicative budget: €8M per proposal -TRL 7

Call - SECURITY (2)

Disaster-resilience: safeguarding and securing society

SEC-01-DRS-2016: Integrated tools for response planning and scenario building

SEC-02-DRS-2016: Situational awareness systems to support civil protection preparation and operational decision making

SEC-03-DRS-2016: Validation of biological toxins measurements after an incident: Development of tools and procedures for quality control

SEC-04-DRS-2017: Broadband communication systems

SEC-05-DRS-2016-2017: Chemical, biological, radiological and nuclear (CBRN) cluster

European
Commission

Disaster Resilient Society

DG HOME
Internal Security

COM(2009) 273 final
CBRN Action Plan
+ **COM(2014)247 final**
CBRN-E risks
+ **European Agenda on Security**

DG ECHO
Civil Protection

Decision 1313/2013
EU Civil Protection Mechanism

Environmental threats

DG ENV
Environment

Decision 1386/2013
Environment Action Programme
Directive 2012/18/EU
(Seveso III Directive)

Climate threats

DG CLIMA
Climate action

EU Climate Adaptation Strategy

Health threats

DG SANCO
Consumer Health

Decision 1082/2013
Serious cross-border threats to health

DG ENER
Energy

Regulation 347/2013
Tran-European Energy Instrastructure
Directive 2009/7/EU
Safety of nuclear installations

DG MOVE
Transport

Decision 661/2010
Tran-European Transport Network

DG TAXUD
Customs

EU Custom policy for supply chain security and use of customs detection technology for CBRN-E

International

DG DEVCO
International cooperation

CBRN-E Centres of Excellence

EEAS
Ext. security

Intergovernmental

+ UN Bodies, NATO

Nuclear non-proliferation treaty
Chemical Weapons Convention
Biological Weapons Convention

DG GROW
Enterprise & Industry

Security Industrial policy
COM(2012)417 final
Internal Security Strategy
COM(2010)673 final
European Agenda on Security

DG TRADE

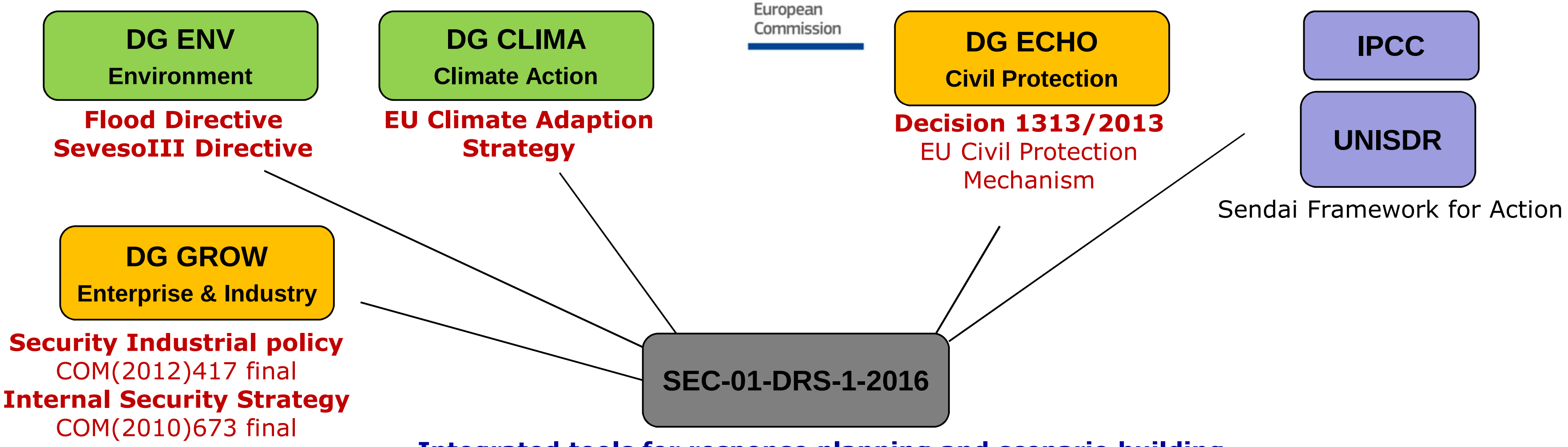
Regulation 428/2009
Transit of dual use items

HORIZON
2020

EU Reseach

EDA
Defense

Joint Investment Programme / EFC



DG ENV
Environment

Flood Directive
SevesoIII Directive

DG CLIMA
Climate Action

EU Climate Adaption Strategy

DG ECHO
Civil Protection

Decision 1313/2013
EU Civil Protection Mechanism

IPCC

UNISDR

Sendai Framework for Action

DG GROW
Enterprise & Industry

Security Industrial policy
COM(2012)417 final
Internal Security Strategy
COM(2010)673 final

SEC-01-DRS-1-2016

Integrated tools for response planning and scenario building

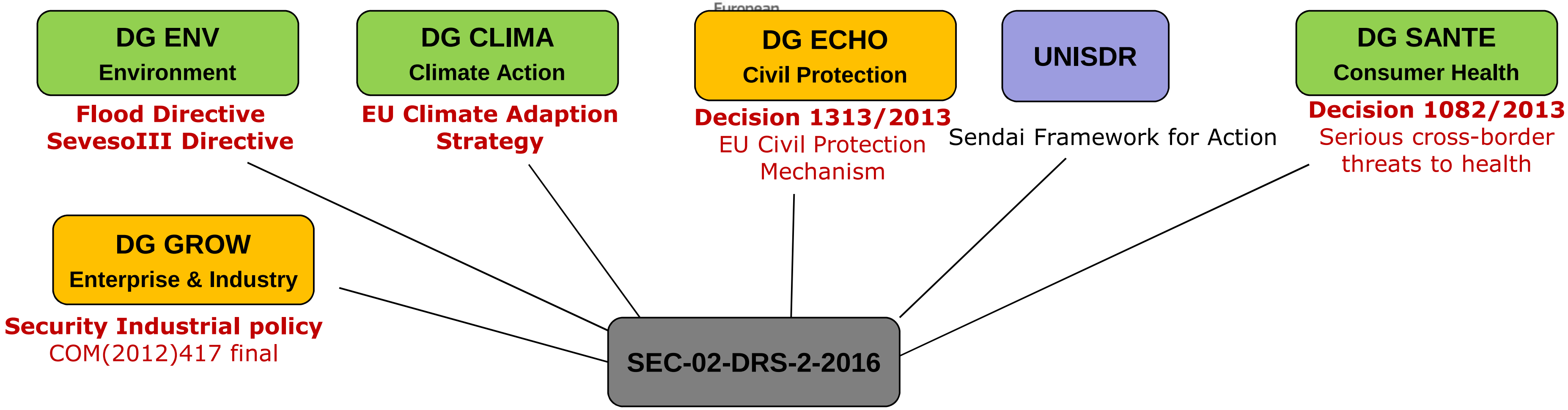
Insufficient inter-linkage among sectors, disciplines and actors involved in disaster risk management, preventing efficient response planning and the building of realistic multidisciplinary scenarios. Needs to develop **integrated tools**, and stronger **partnerships** among research, policy, monitoring institutes, industry/SMEs and practitioners (in particular first responders). **Scope on disaster risks** (natural, accidental, or intentional) and **emergency situations** in the context of the EU Civil Protection Mechanism, consideration of IPCC recommendations and Sendai Framework for Action.

Integration of support tools that can be used by a large variety of decision-makers and first responders, building upon previous and on-going FP7 projects and preliminary results from H2020 to **avoid duplication**. Demonstrations in **representative and realistic** environments with **involvement** of fire fighting units, medical emergency services, police departments and civil protection units.

Int. Cooperation encouraged.

Expected impacts: More efficient response capacity and improved strategy for response planning (short term), enhanced autonomy, resilience of rescue/first aid organisations in case of a disaster, updated knowledge, best practices and lessons learned from similar, past incidents, enhanced understanding of human factors in relation to events affecting CIs, development of new tools and adaptive networking of existing technologies, demonstrating interoperability for use in all-hazards situations, with consideration of EU guidelines and recommendations. Development of scenarios with local authorities and end-users, tools for **enhancing stakeholders and population awareness**, societal acceptance of autonomous systems entities (satellite etc), greater cooperation among actors in crisis management, and **stronger practitioner's involvement in validating and testing** tools, concepts etc.

Type of action:Innovation Action (+/- 8 M€) Development up to TRL 7 or 8



CSA on situational awareness systems to support civil protection preparation and operational decision making

Insufficient integration of existing technologies and prototype tools to improve situational awareness in time of crisis. Needs to **better understand** the psychological, cultural, language and societal dimension of **situational awareness** in order to prevent, prepare and manage crisis situations. Systems for EU, national, regional and local buyers should be cost effective and interoperable, **integrate different technologies** (e.g. sensors, EWS, communication, satellite-based systems) and demonstrate resilience and self-sufficiency. In addition, systems should be **customizable** by specific civil protection authorities and adaptable to **various risks and crisis scenarios** (e.g. range of natural hazards, industrial accidents, biohazards etc.) especially in the context of **cross-border** cooperation.

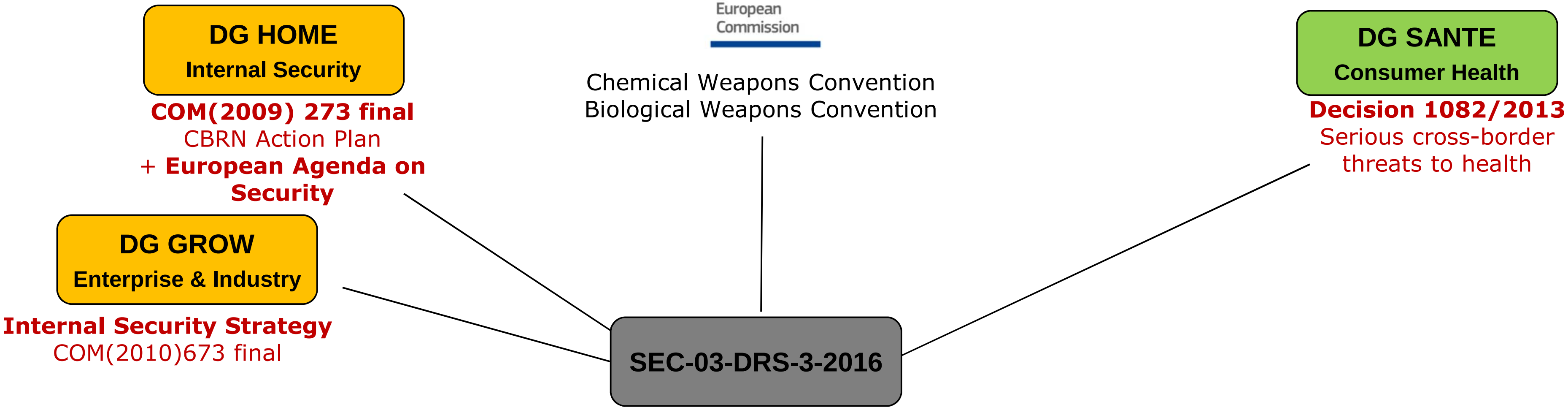
Action to **identify new and promising solutions**, develop/agree on **core set of specifications** for a given system, **on roadmap for research** still needed, and related **tender documents** upon which to base future (research services and system) procurements. Subsequent actions (PCP, PPI, others) to implement tender procedures to develop, test, validate prototypes may be envisaged.

Int. Cooperation encouraged.

Expected impacts: Improved cooperation among civil protection services across the EU and Associated countries, between hazard-monitoring institutes and civil protection services, exchange of experiences among stakeholders within the DRM cycle, improved response capacity. On the long term, lower operating costs for European humanitarian actions.

Further to the CSA achievement: **possible PCC/PPI co-fund action** in the future

Type of Action: Coordination & Support Action (+/- 1.5 M€)



DG HOME

Internal Security

COM(2009) 273 final
CBRN Action Plan
+ European Agenda on Security

DG GROW

Enterprise & Industry

Internal Security Strategy
COM(2010)673 final

Chemical Weapons Convention
Biological Weapons Convention

DG SANTE

Consumer Health

Decision 1082/2013
Serious cross-border threats to health

SEC-03-DRS-3-2016

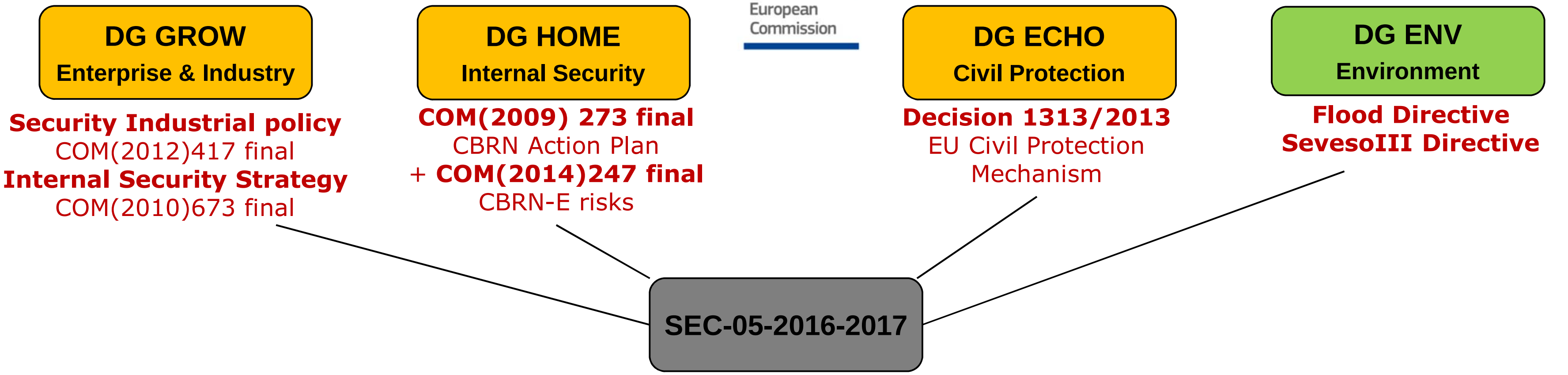
Validation of biological toxins measurements after an incident: Development of tools and procedures for quality control

Poor comparability of results from different laboratories casts doubts about method validation, and hence on decisions in case of bioterrorist act using compounds such as e.g. ricin, saflatoxin, botulinum, neurotoxins, enterotoxins etc. (covered by the Chemical and Biological Weapons Conventions). Lack of QA/QC tools and SOPs hampering EU-wide comparability of biological toxin measurement data. Need to develop an EU-wide approach for enhancing validating analytical capacities.

Action to develop QC tools as well as SOPs for the establishment of a mechanism to **systematically validate laboratory-based measurement techniques**, including sampling strategies and in-situ analyses by mobile and quickly deployable laboratories.

Expected impacts: Development of **CRMs for biotoxin determinations**, **stepwise learning inter-laboratory programme** to improve laboratory skills and development of **European Proficiency Testing scheme** from sampling to detection. Improved capabilities for validating and testing existing and emerging techniques, incl. Sample preparation strategies, in-situ analyses and technical approaches for forensic analysis. Replacement of old "gold standards" employing animal experiments by modern in vitro methods as requested by EU regulations. On the long term, based on the EPT scheme, development of SOPs for validating analytical techniques, including in-situ techniques for biotoxin determinations in human specimens, environmental and food samples.

Type of Action: Innovation Action (+/- 8 M€)



DG GROW
Enterprise & Industry

Security Industrial policy
COM(2012)417 final
Internal Security Strategy
COM(2010)673 final

DG HOME
Internal Security

COM(2009) 273 final
CBRN Action Plan
+ **COM(2014)247 final**
CBRN-E risks

DG ECHO
Civil Protection

Decision 1313/2013
EU Civil Protection
Mechanism

DG ENV
Environment

Flood Directive
SevesoIII Directive

SEC-05-2016-2017

Chemical, biological, radiological and nuclear (CBRN) cluster

Part a) "Integrating" function:

✓CSA to gather European companies capable and willing to market their products globally
✓CSA to provide platforms to integrate technologies and innovations developed by other companies in RIAs of Part b)
✓CSA to issue a list of technologies to be developed and further integrated
✓Participant(s) in the CSA to enter into "Collaboration Agreement" with RIA proposed under Part b)

"Service" function:

✓CSA to develop interfaces with financial institutions
✓CSA to provide commercial and other services enabling access to the global market for the results of the RIA selected for support under Part b)
✓CSA to report and provide feedback on the impact of the business deals with RIAs of Part b)

- ➢The larger the number of European companies involved in the CSA, the higher its impact
- ➢Only one such CSA may be supported

In 2017: RIAs on novel CBRN technologies and innovations identified in the catalogue issued by the CSA, establishing a collaboration agreement with CSA on how results from the RIA will be exploited and integrated into platforms managed by CSA

Expected impact:

- Shorter time to market for novel CBRN technologies and innovations
- More business deals among CBRN industrial players
- More industrial products of interest to more practitioners in Europe (and world-wide)

European Commission

Call - SECURITY (3)

Fight against Crime and Terrorism

SEC-06-FCT-2016: Developing a comprehensive approach to violent radicalization in the EU from early understanding to improving protection

SEC-07-FCT-2016-2017: Human Factor for the Prevention, Investigation, and Mitigation of criminal and terrorist acts

SEC-08-FCT-2016: Forensics techniques on: a) trace qualification, and b) broadened use of DNA

SEC-09-FCT-2017: Toolkits integrating tools and techniques for forensic laboratories

SEC-10-FCT-2017: Integration of detection capabilities and data fusion with utility providers' networks

SEC-11-FCT-2016: Detection techniques on explosives: Countering an explosive threat, across the timeline of a plot

SEC-12-FCT-2016-2017: Technologies for prevention, investigation, and mitigation in the context of fight against crime and terrorism

SEC-06-FCT-2016: Developing a comprehensive approach to violent radicalization in the EU from early understanding to improving protection

Scope:

- *Engaging the whole of society and requiring a holistic treatment and a multidisciplinary approach*
- *Building on national and EU projects and involving the RAN*

Expected impact:

- *set of policy-recommendations and tools for policy-makers & LEAs to timely prevent and detect radicalisation*
  - ✓ *policy comparative analysis*
  - ✓ *description of competencies and skills of practitioners*
  - ✓ *information exchange among different involved actors*
  - ✓ *field validation*

Type of action: Research and Innovation action (max €3M)

SEC-07-FCT-2016-2017: Human Factor for the Prevention, Investigation, and Mitigation of criminal and terrorist acts

Scope:

- *Proposals should contribute to the definition of the European Security Model defined in the European Agenda for Security*
- *Only one sub-topic should be dealt with per proposal, mandatorily taking into account the societal dimension*

Expected impact:

- *Policy-toolkit for security policy-makers*
- *Common approaches including acceptance tests and cost-benefit considerations*
- *Advancing understanding by LEAs of perception and feeling of security by citizens*
- *Toolkit for LEAs to improve perception and feeling of security by citizens*

Type of action: Research and Innovation action (max €3M)

SEC-08-FCT-2016: Forensics techniques on: a) trace qualification, and b) broadened use of DNA

Scope:

- *Increase knowledge about trace qualification and composition*

and/or

- *Extended use and exploitation of DNA*

For both, proposals must address: admissibility of evidence, new adapted curricula, methodologies for the comparison of results across EU

Expected impact:

Quicker and more [cost]efficient forensic processes in view of better administration of justice

Type of action: Research and Innovation action (max €5M) TRL 5

SEC-11-FCT-2016: Detection techniques on explosives: Countering an explosive threat, across the timeline of a plot

Scope:

- *Assessment of existing methods and techniques to counter terrorist use of explosives listed in the topic*
- *No technological development is foreseen but rather a basis for future development of new and innovative detection techniques*

Expected impact:

- *Better understanding of the effectiveness and weakness of the supporting method/technology used to counter the terrorist use of an explosive threat;*
- *Stronger involvement of practitioners in making the assessment and selection of new tools and technologies in the field*

Type of action: Research & Innovation action (max. €5m)

SEC-12-FCT-2016-2017: Technologies for prevention, investigation, and mitigation in the context of fight against crime and terrorism

Scope:

- *New knowledge and targeted technologies to combat crime and terrorism*
- *Test and demonstration by LEAs*
- *Innovative curricula, training and exercises to facilitate take-up of new technologies*
- *Only one sub-topic should be dealt with per proposal, mandatorily taking into account the societal dimension*

Expected impact:

- *Improved investigation capabilities*
- *Better technological tools for LEAs*
- *Better identification and understanding of criminal activities*

Type of action: Research & Innovation action (max. €5m) TRL 6

Call - SECURITY (1)

Border Security and External Security

SEC-13–BES–2017: Next generation of information systems to support EU external policies

SEC-14-BES–2016: Towards reducing the cost of technologies in land border security applications

SEC-15-BES–2017: Risk-based screening at border crossing

SEC-16-BES–2017: Through-foliage detection, including in the outermost regions of the EU

SEC-17-BES-2017: Architectures and organizations, big data and data analytics for customs risk management of the international goods supply chain trade movements

SEC-18-BES–2017: Acceptance of "no gate crossing point solutions"

SEC-19-BES-2016: Data fusion for maritime security applications

SEC-20-BES-2016: Border Security: autonomous systems and control systems

Border Security and External Security

Development of technologies, capabilities and solutions to:

Improve EU border security*:*

- *Flow of people: research will support the exploitation of the potential given by the European Border Surveillance System (**EUROSUR** - Regulation No 1052/2013) and promote an enhanced use of new technology for border checks in relation to the SMART BORDERS legislative initiative* ***(DG HOME)***
- *Flow of goods: research will address, in the context of the EU's customs policy, supply chain security trying to strike the right balance with trade facilitation* ***(DG TAXUD)***

Support the EU External Security Policies in civilian tasks (EEAS)

SEC-14-BES–2016: Towards reducing the cost of technologies in land border security applications (1)

Scope:

- *EU Border management = enforcement of common policies & implementation of common rules.*
- *Pressure to process large volumes (and smuggling) of people at border crossing points.*
- *External land borders of the EU = wide range of challenges*
- *Without investments in technology and information systems, not feasible to manage borders and border crossing points.*
- *Broad variety of heterogeneous IT applications and systems deployed.*
- *This makes management increasingly complex and (too) costly.*
- *Innovative, cost-efficient technologies needed, or existing ones to become more affordable.*
- *Border authorities in the best position to identify benefits.*

Expected impact:

Novel technologies, tools and systems demonstrating very substantial cost-reduction compared to existing technologies, tools and systems.

SEC-14-BES–2016: Towards reducing the cost of technologies in land border security applications (2)

- Research and Innovation Action
- Total budget: €10M
- Ind. Budget per proposal: €5M
- Overlap with EWISA project should be avoided (www.ewisa.eu)
- Coordination with EDA activities
- Enhanced SME participation
- Up to TRL 6 (technology demonstrated in relevant environment)
- At least 3 border guard authorities from 3 different EU/Schengen MS

SEC-19-BES-2016: Data fusion for maritime security applications

Scope:

- *Develop methods and tools to fuse and make mutually understandable raw data, taking account the technical characteristics of existing systems, and the specific context of the variety of aspects of maritime security.*
- *Build on existing results, focus on gaps and avoid duplication with previous endeavours.*
- *For semantic interoperability, the CISE data model www.eucise2020.eu to be used to avoid duplications.*

Expected impact:

- *Improved and extended maritime border situational awareness;*
- *Improved operational support to search-and-rescue activities;*
- *Improved border surveillance systems in terms of information exchange, situational awareness, and decision-making and reaction capabilities.*

Solutions to be demonstrated in the context of interagency and cross-border cooperation, and to be interfaced with existing infrastructure (systems, platforms and networks of sensors).

SEC-20-BES-2016: Border Security: autonomous systems and control systems

Scope:

Different prototypes of unmanned vehicles transformed into autonomous, long-enduring agents. Proposals to cover one of the two following sub-topics:

***Sub-topic 1**. Autonomous surveillance to support missions ranging from surveillance to detection of marine pollution incidents, including early identification and tracking of illegal activities.*

***Sub-topic 2**.Enhanced command and control systems for the surveillance of borders in a 3D environment Autonomous surveillance*

Expected impact:

- *Further development of EUROSUR;*
- *Provision of more information to be exchanged across sectors and borders (as through CISE);*
- *New technologies for autonomous surveillance systems;*
- *Improved, cost-effective and efficient unmanned platforms for border surveillance, and detection of marine pollution incidents;*
- *Adaptation of technologies to the specific requirements of borders control;*
- *Interoperability with existing, multi-country European infrastructure.*

Technical aspects

<u>*Type of action:*</u> *Innovation Action (max €24M)-International cooperation encouraged*

SEC-19-BES-2016:

- ✓ Coordination with EDA activities
- ✓ TRL 7 (system prototype demonstration in operational environment)
- ✓ <u>At least 3 border guard authorities from 3 MS/AC</u>
- ✓ <u>At least 3 independent industry organizations from 3 different MS/AC.</u>

SEC-20-BES-2016:

- ✓ Cover 1 sub-topic:
    1. Autonomous surveillance
    2. Enhanced command and control systems for the surveillance of borders in a 3D environment Autonomous surveillance
- ✓ SMEs are strongly encouraged
- ✓ TRL 6 or 7
- ✓ <u>Practitioners from various disciplines, including Border guard authorities from at least 5 EU/Schengen MS</u>

Call – DIGITAL SECURITY FOCUS AREA

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

DS-06-2017: Cryptography

DS-07-2017: Addressing Advanced Cyber Security Threats and Threat Actors

DS-08-2017: Privacy, Data Protection, Digital Identities

European Commission

Call – Digital Security Focus Area – Topics

- **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;
- **DS-06-2017**: Cryptography;
- **DS-07-2017**: Addressing Advanced Cyber Security Threats and Threat Actors;
- **DS-08-2017**: Privacy, Data Protection,

  Digital Identities;

- **Situation:** ICT-driven transformations bring opportunities across many important sectors.
- **Complication**: "Smart", "Connected", "Digital" also introduce vulnerabilities...
- **R&D&I challenge:** Innovative and multidisciplinary actions addressing cyber security, data protection and privacy across individual H2020 pillars and calls.

DS-02-2016: Cyber Security for SMEs, local public administration and Individuals (IA)

- Considering the adequate level of security commensurate with the considered use-case, proposals may address one types of end-user: SMEs, local PA, individual citizens.

- Basic cyber security threats
- Organisation size and budgetary constraints
- Individuals, the "weakest link‟ ?
- Human factors, behaviour
- Usability, automation
- Guidance, best practices and standards

DS-04-2016: Economics of Cybersecurity (RIA)

- [...] combining methods from microeconomics, econometrics, qualitative social sciences, behavioural sciences, decision making, risk management and experimental economics.
- Cost-benefit
  - Intangible assets, metrics, optimal investement, insurance
- Incentives and business models
  - Incentives, cooperative and regulatory approaches
  - Information security markets (e.g. bug bounties, vulnerability disclosure)
  - Revenue models for criminal activity
- Institutional innovation

DS-05-2016: EU Cooperation and International Dialogues in Cybersecurity and Privacy Research and Innovation (CSAs)

- ➢ A better overview of EU, MS and regional activities.
- ➢ Exchange of views on global level; promote EU stakeholder participation.
- ➢ 3 separate CSAs
  - ➢ Synergies between H2020, EU Member States and associated countries R&I activities and cybersecurity innovation clusters.
    - ✓ 4 years
  - ➢ International dialogue with Japan
  - ➢ International dialogue with the USA

Call - DS – 2016 - Planning

Three separate opening dates - deadlines for submission		
Topic(s)	DS-01-2016	DS-02-2016 DS-04-2016 DS-05-2016
Opening	20 Oct 2015	15 Mar 2016
Deadline	**12 Apr 2016**	25 Aug 2016

Topic	Instr.	Funding (M)	
DS-01-2016	RIA IA CSA	13.50 9.0 1.0	➢ Only the best proposal may be funded for part c) Coordination and Support Action
DS-02-2016	RIA	22.0	
DS-04-2016	RIA	4.0	
DS-05-2016	CSA 3 strands	2;0.5;0.5	➢ Only the best proposal may be funded for strands 1, 2 and 3. ➢ Proposals addressing strand 1 shall be of a 4 year duration.

General Matters

SEC-21–GM-2016-2017: Pan European Networks of practitioners and other actors in the field of security

Pan-European networks of practitioners

To free security practitioners from operational work to focus on forward-looking problem-solving by:

- exchanging views across borders,
- analysing the gaps in the tools they need to operate, and
- prioritising future R&D efforts

Categories of Networks

a. Practitioners from **the same discipline** and from across Europe

b. Practitioners **from different disciplines** and concerned with current or future security or disaster risk and crisis management issues **in a particular geographical area**

c. Entities from around Europe that manage **demonstration and testing sites, training facilities** for practitioners

a. Practitioners in the same discipline and from across Europe

1. *monitor research and innovation projects with a view to recommending the uptake or the industrialisation of results;*
2. *express common requirements as regards innovations that could fill in gaps and improve their performance in the future;*
3. *indicate priorities as regards domains requiring more standardization.*

Eligibility Criteria (a.)

- Practitioner participation from at least 8 Member States or Associated Countries
- Each proposal must include a plan, and a budget amounting at least 25% of the total cost of the action, to interact with industry, academia, and other providers of innovative solutions
- Each consortium must commit to produce, every 6 or fewer months, a report about their findings in the 3 lines of actions
- Each proposal must include a workpackage to disseminate their findings, including an annual workshop

➢ Only one network per discipline may be supported over the 2016-2017 period

b. Practitioners from different disciplines addressing security issues in a particular geographical area

1. *monitor research and innovation projects;*
2. *express common requirements for innovation;*
3. *indicate priorities as regards standardization.*

Selected geographical areas:

- The Mediterranean region (including the Black Sea):
- The Arctic and North Atlantic region
- The Danube river basin
- The Baltic region

Eligibility Criteria (b.)

- Practitioner participation from at least 2 Member States or Associated Countries from outside the region
- Each proposal must include a plan, and a budget amounting at least 25% of the total cost of the action, to interact with industry, academia, and other providers of innovative solutions
- Each consortium must commit to produce, every 6 or fewer months, a report about their findings in the 3 lines of actions
- Each proposal must include a workpackage to disseminate their findings, including an annual workshop

➢ Only one network per region may be supported over the 2016-2017 period

c. Entities that manage demonstration and testing sites, training facilities for security practitioners

1. *establish and maintain a roster of capabilities and facilities;*
2. *organize to share expertise;*
3. *plan to pool and share resources with a view to optimize investments.*

Eligibility Criteria (c.)

- Practitioner participation from at least 8 Member States or Associated Countries
- Each consortium must commit to produce, every 6 or fewer months, a report about their findings in the 3 lines of actions
- Each proposal must include a workpackage to disseminate their findings, including an annual workshop

➢ *Only one such (category c) network may be supported over the 2016-2017 period*

Expected Impact

- *Common understanding of innovation potential*
- *Expression of common innovation and standardization needs among practitioners in the same discipline*
- *Coordinated uptake of innovative solutions among practitioners from different disciplines who are called to act together to face major crisis.*
- *Optimized use of investments in demonstration, testing, and training facilities for security practitioners*

Topics

- ✓ **SME Instrument:**
  covers any aspect of "Secure Societies"

- ✓ **Fast track to Innovation** – Pilot:
  covers any aspect of "Secure Societies"

Thank you for your attention!

Alberto Pietro Contaretti
Programme Officer – EU Policies
B.4: Innovation and Industry Security
DG Migration and Home Affairs

E-mail: alberto-pietro.contaretti@ec.europa.eu