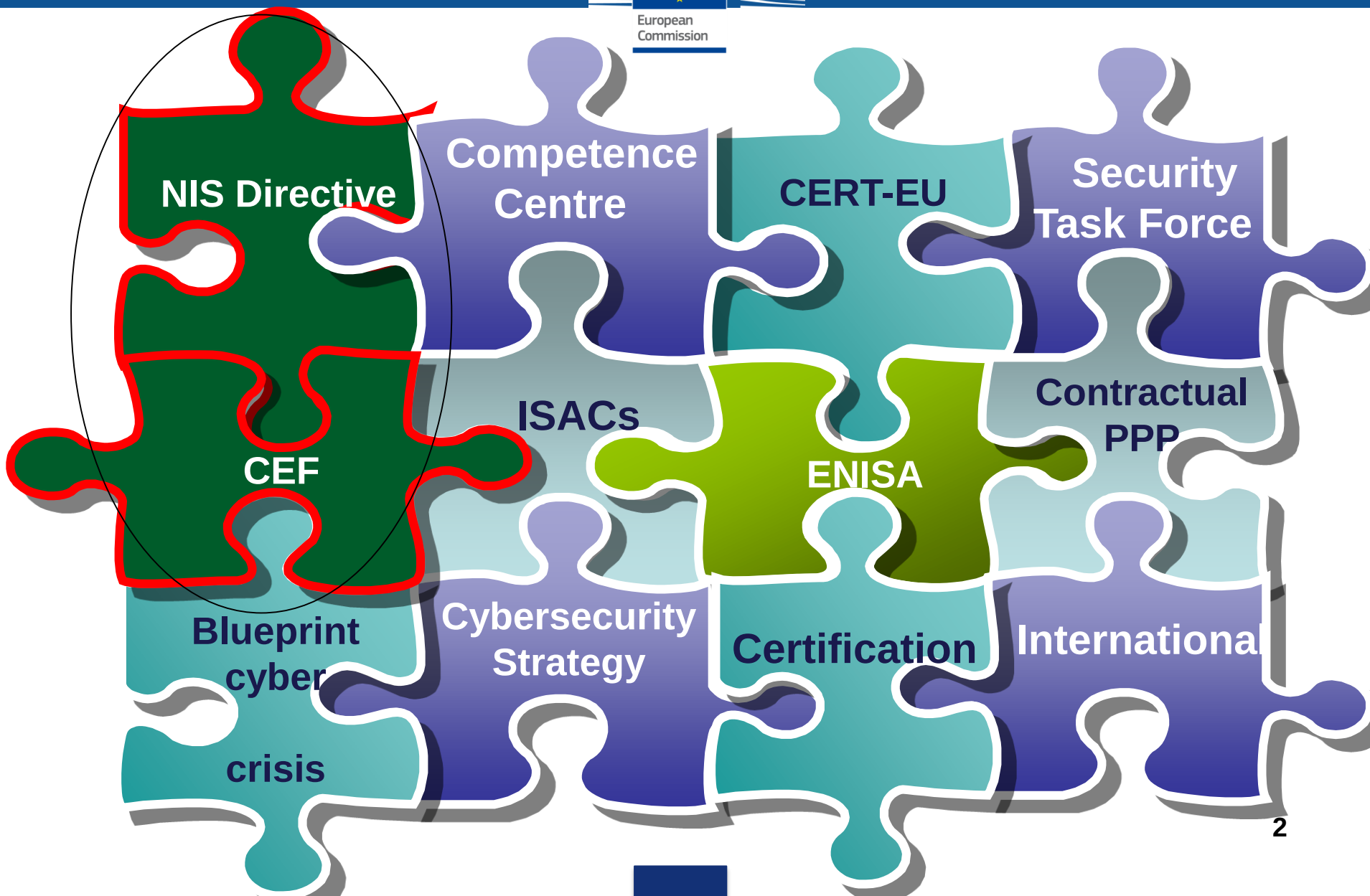
CEF: Capacity Building for Resilient Critical Information Infrastructure

NSA/ENISA Workshop on NIS Directive & CIIP

JCAFFREY, DG CONNECT, H1, 30th November, 2018

Cybersecurity Law & Policy



European Commission

NIS Directive: Main Features

GREATER CAPABILITIES

Member States have to improve their cybersecurity capabilities.

- NATIONAL COMPUTER SECURITY INCIDENT RESPONSE TEAM (CSIS-RT)
- NATIONAL NIS STRATEGY
- NATIONAL NIS AUTHORITY

COOPERATION

Increased EU-level cooperation

- EU MEMBER STATES COOPERATION GROUP (STRATEGIC)
  - EU MEMBER STATES; EUROPEAN COMMISSION; EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY
- EMERGENCY TEAMS (CSIRTS) NETWORK (OPERATIONAL)
  - EU MEMBER STATES; CERT-EU; EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY

RISK MANAGEMENT

Operators of essential services and Digital Service Providers have to adopt risk management practices and notify significant incidents to their national authorities.

- SECURITY MEASURES
- NOTIFICATION OF MAJOR INCIDENTS

European Commission

European Commission › Strategy › Digital Single Market › Policies ›

Digital Single Market

POLICY

NIS Cooperation Group

https://ec.europa.eu/digital-single-market/en/nis-cooperation-group

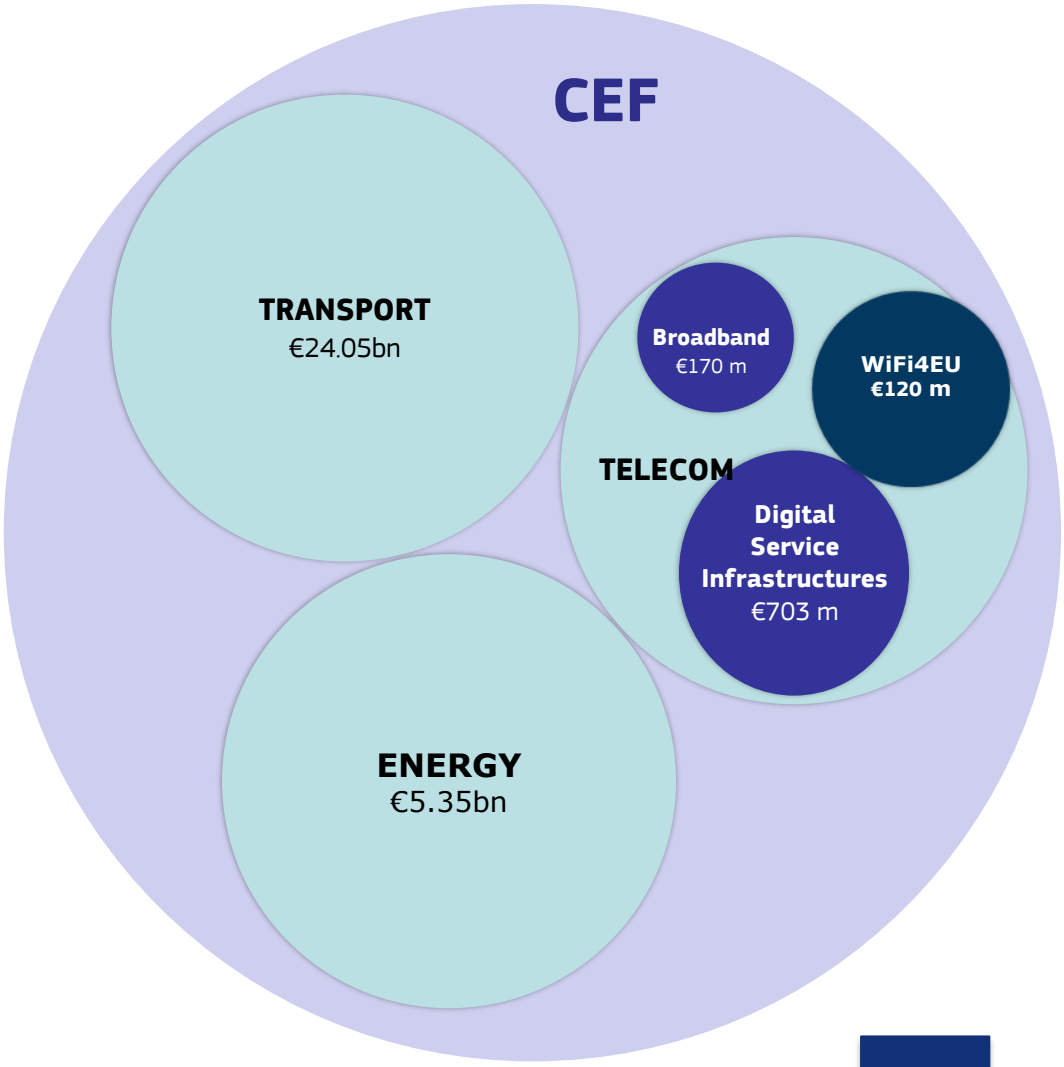
Publications

Among the key outputs of the NIS Cooperation Group, there are non-binding guidelines to the EU Members States to allow effective and coherent implementation of the NIS Directive across the EU and to address wider cybersecurity policy issues.

Since its establishment, the Group has published seven working documents:

- CG Publication 01/2018 - Reference document on security measures for Operators of Essential Services
- CG Publication 02/2018 - Reference document on incident notification for Operators of Essential Services (circumstances of notification)
- CG Publication 03/2018 - Compendium on cyber security of election technology
- CG Publication 04/2018 - Cybersecurity incident taxonomy
- CG Publication 05/2018 - Guidelines on notification of Operators of Essential Services incidents (formats and procedures)
- CG Publication 06/2018 - Guidelines on notification of Digital Service Providers incidents (formats and procedures)
- CG Publication 07/2018 - Reference document on the identification of Operators of Essential Services (modalities of the consultation process in cases with cross-border impact)

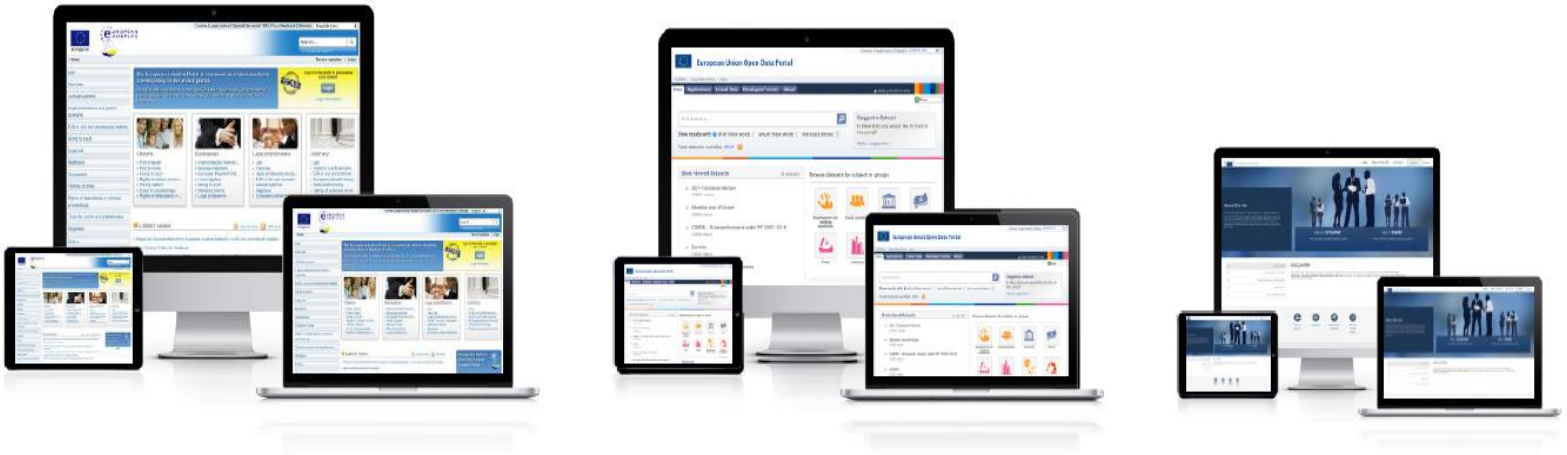
Connecting Europe Facility (CEF) 2014 to 2020



Infrastructure programme to support the establishment of trans-European networks to reinforce an interconnected Europe

European Commission

Connecting Europe Facility: Cybersecurity



DIGITAL SERVICE INFRASTRUCTURES (DSIs)

Information exchange Co-operation Mechanism

EUROPEAN COMMISSION

MEMBER STATES

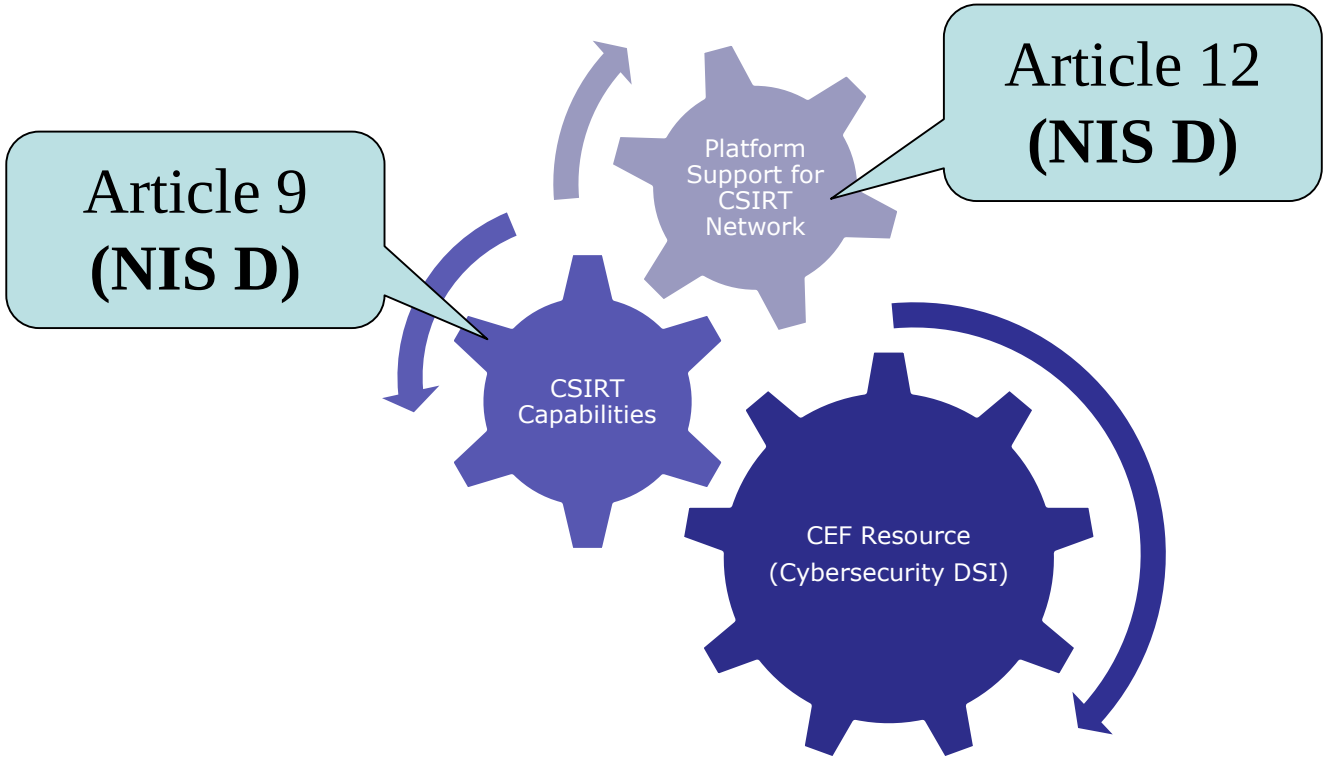
MS CSIRTs: Capabilities and Connecting to CSP

CORE SERVICE PLATFORM
(Services offered by the European Commission)

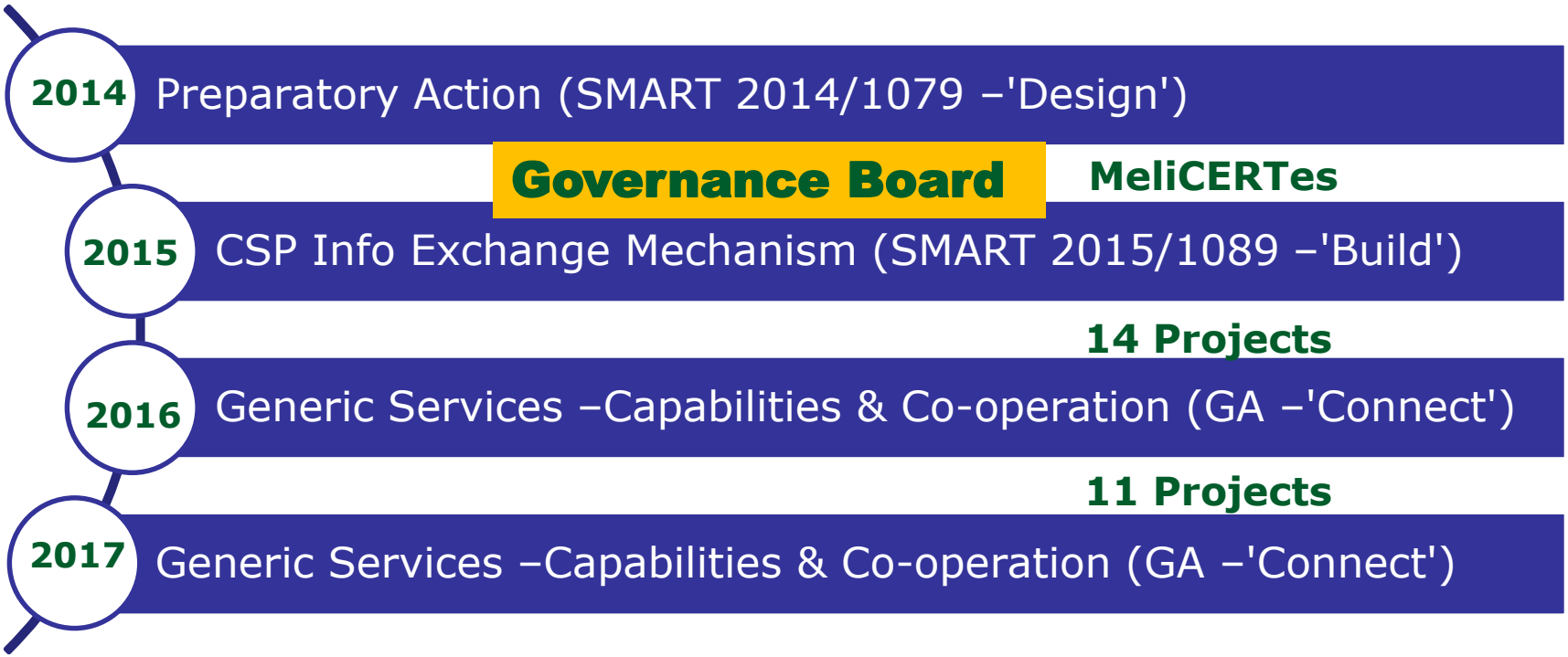
GENERIC SERVICES
(Grants for projects in the Member States)

European Commission

Context for CEF Cybersecurity DSI (2014-2017): NIS Directive



CEF Cybersecurity DSI



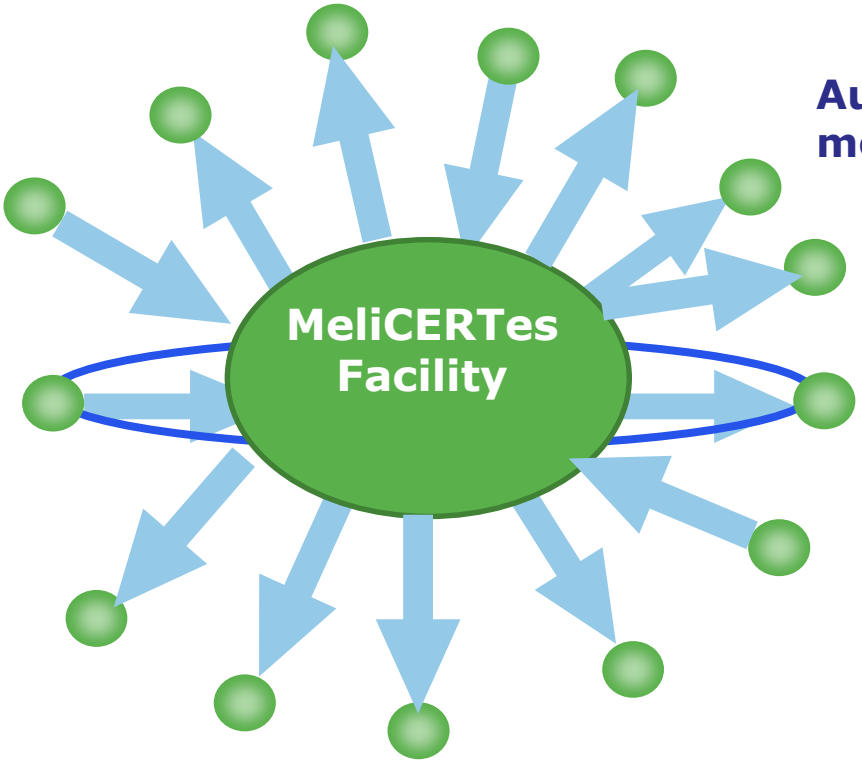
Cybersecurity DSI: Themes

1. *Capabilities Development*
   - **Infrastructure –e.g. software tools**
   - **Soft Measures –e.g. development of skills and structural support**
2. *Operational Co-operation between Member States*
   - **CSP Co-operation Mechanism –MeliCERTes**
   - **Multi-lateral exchanges –Ad hoc**

CSIRTs Co-operation Mechanism

Generic Services: 18 MS CSIRTs

Common Suite of Tools



Autonomous, modular approach

Cross Border Data Exchange

Voluntary Information Sharing

Capabilities Development

CEF Cybersecurity Initiatives Public Information

Cyber Security

Cyber Security overview

The list of individual action fiches below is not exhaustive and additional fiches will be included as they become available.

2016-AT-IA-0089
Strengthening the CERT Capacity and IT security readiness in Austria

2016-CY-IA-0129
Development and Enhancement of the capabilities of the Cyprus National CSIRT

2016-CZ-IA-0107
Strengthening cyber-security capacities in the Czech Republic

2016-EE-IA-0113
Platform for exploit kit hunting

2016-EL-IA-0123
CERTCOOP: Trans-European and Greek CERTs collaboration project

2016-ES-IA-0084
Improvement of national cyber security capabilities to enhance intelligence sharing at the EU

https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/projects-by-dsi/cyber-security

Example of Grant Action Details on Public Website

https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/2016-at-ia-0089

Strengthening the CERT Capacity and IT security readiness in Austria

Programme:
CEF Telecom

Call year:
2016

Member State(s):
Austria

Implementation schedule:
September 2017 to August 2019

Maximum EU contribution:
€748,030

Estimated total cost:
€997,373

Percentage of EU support:
75%

Coordinator:
nic.at GmbH
https://www.nic.at/en/good_to_know/security/cert

Status:
Ongoing

DSI:
Cyber Security

Additional information:

2016-AT-IA-0089

The Action will prepare the Austrian National Computer Emergency Response Team - CERT.at - for the requirements and tasks arising from the Directive on Security of Network and Information Systems (NIS Directive). With the Action, CERT.at will ensure that the CERT's team is adequately staffed including professional capacities of individual team members, to create adequate cybersecurity capabilities and to strengthen physical security.

The Action also aims at facilitating the cross-border cooperation, especially by developing and providing to national and/or governmental Computer Emergency Response Teams (CERTs) and Computer Security Information Response Teams (CSIRTs) in Europe re-usable building blocks represented by several software tools designed as an extension of selected components of the Cybersecurity Core Service Platform (CSP) MeliCERTes. The cross-border cooperation will also be facilitated by participation in the Computer Security Information Response Teams (CSIRT) network according to Art.12 of the NIS Directive and in the meetings of the Task Force on Computer Security Incident Response Teams (TF-CSIRT).

European

CyberExchange

Cyber Exchange

Programme:
CEF Telecom

Call year:
2017

Member State(s):
Austria, Croatia, Czech Republic, Greece, Latvia, Luxembourg, Malta, Poland, Romania, Slovakia

Implementation schedule:
November 2018 to October 2020

Maximum EU contribution:
€550,726

Estimated total cost:
€734,301

Percentage of EU support:
75%

Coordinator:
CZ.NIC

z. s. p. o.
https://www.nic.cz/

Status:
Ongoing

DSI:
Cyber Security

2017-EU-IA-0118

The Cybersecurity Digital Service Infrastructure (DSI) is underpinned by the European Strategy for Cybersecurity: it provides an information sharing platform ("MeliCERTes") facilitating operational cooperation among Computer Security Incident Response Teams (CSIRTs), as well as funding for CSIRTs to effectively take part in its activities.

The aim of the Action is to strengthen the know-how and capabilities of the participating national and government Computer Security Incident Response Teams/Computer Emergency Readiness Teams (CSIRTs/CERTs) by enhancing cross-border cooperation.

The Action has the following specific objectives:

- Increasing the knowledge and capacities of individual members of security teams and facilitating cooperation through staff exchanges among participating CSIRTs/CERTs
- Increasing the maturity level of individual CSIRTs/CERTs regarding new software tools by exchanging information on tools developed by individual CSIRTs/CERTs that are beneficiaries of CEF cybersecurity calls
- Increasing cross-border and cross-sector collaboration among participating CSIRTs/CERTs by engaging in team building activities related to cybersecurity

Cybersecurity DSI: EC Investments

Initiative	Duration	EC Funds*	Agreements
SMART 2014/1079	2015-2018	1.8mEUR	CSP –Contract *(Preparatory Action)*
SMART 2015/1089	2016-2019	4.5mEUR	CSP -Contract
14 Projects from 14 Member States	2017-2019	10.8mEUR	Generic Services – Grant Action
11 Projects from 16 Member States	2018-2020	7.1mEUR	Generic Services – Grant Action

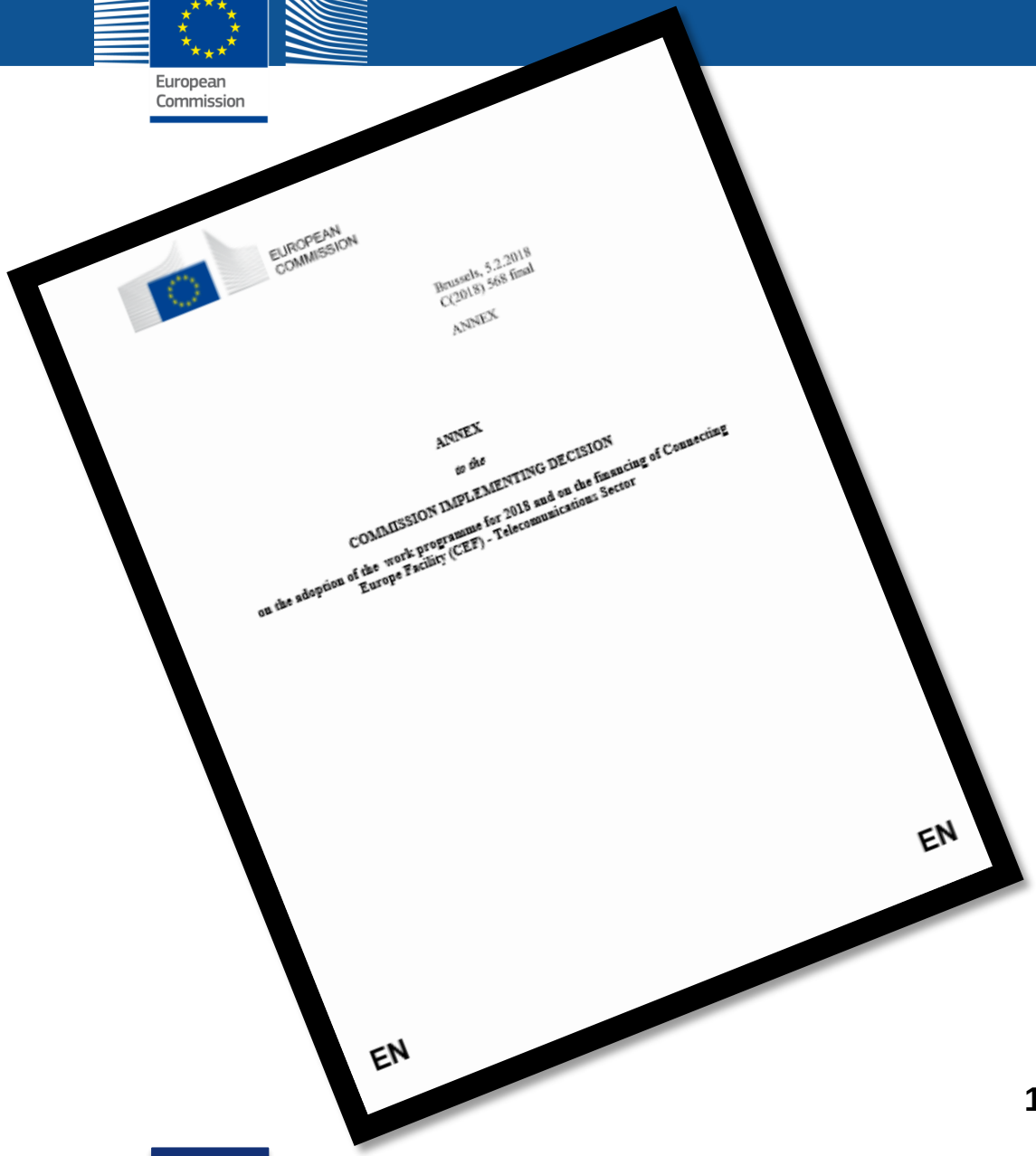
*** Approximate only**

CEF Work Programme 2018

20.5mEUR for Cybersecurity

13mEUR in 2018 call

Broadened Scope


EUROPEAN COMMISSION

Brussels, 5.2.2018
C(2018) 568 final

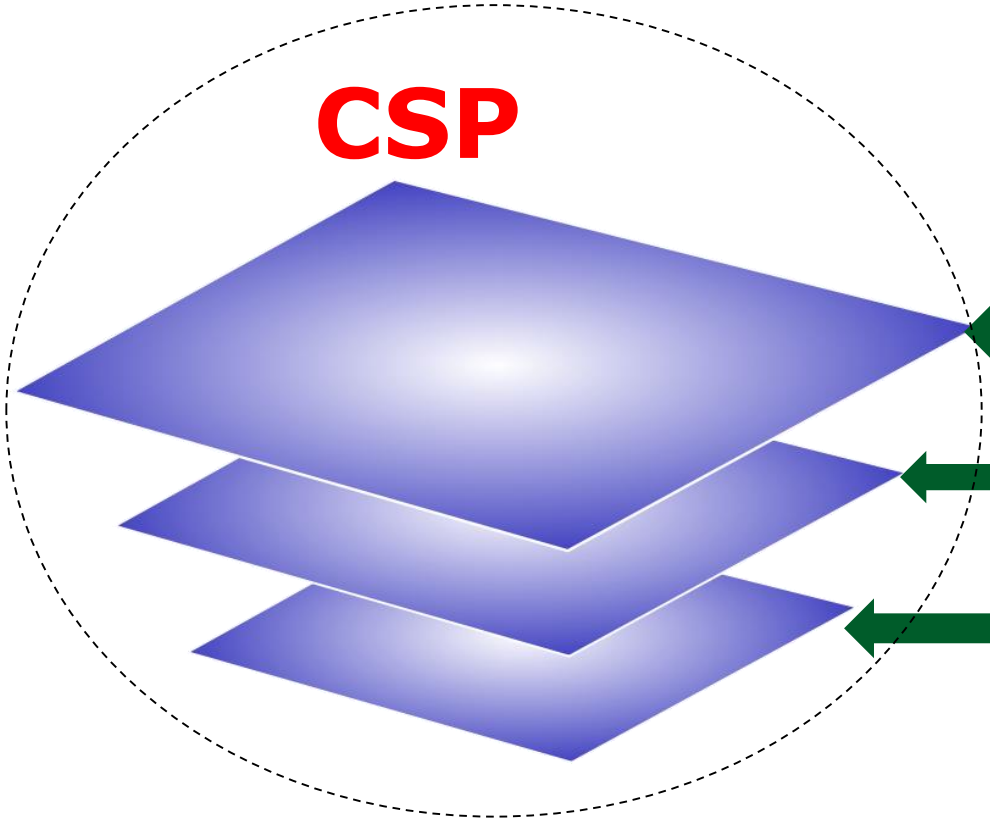
ANNEX

ANNEX
to the
COMMISSION IMPLEMENTING DECISION
on the adoption of the work programme for 2018 and on the financing of Connecting Europe Facility (CEF) - Telecommunications Sector

EN

EN

Next Steps: CSP Co-operation Mechanisms



Reporting/Notification Platform for SPOCs/NCAs

Facilities For European Level Sectoral ISACs with OES, DSPs, CCAM, Public Bodies

MeliCERTes For CSIRTs

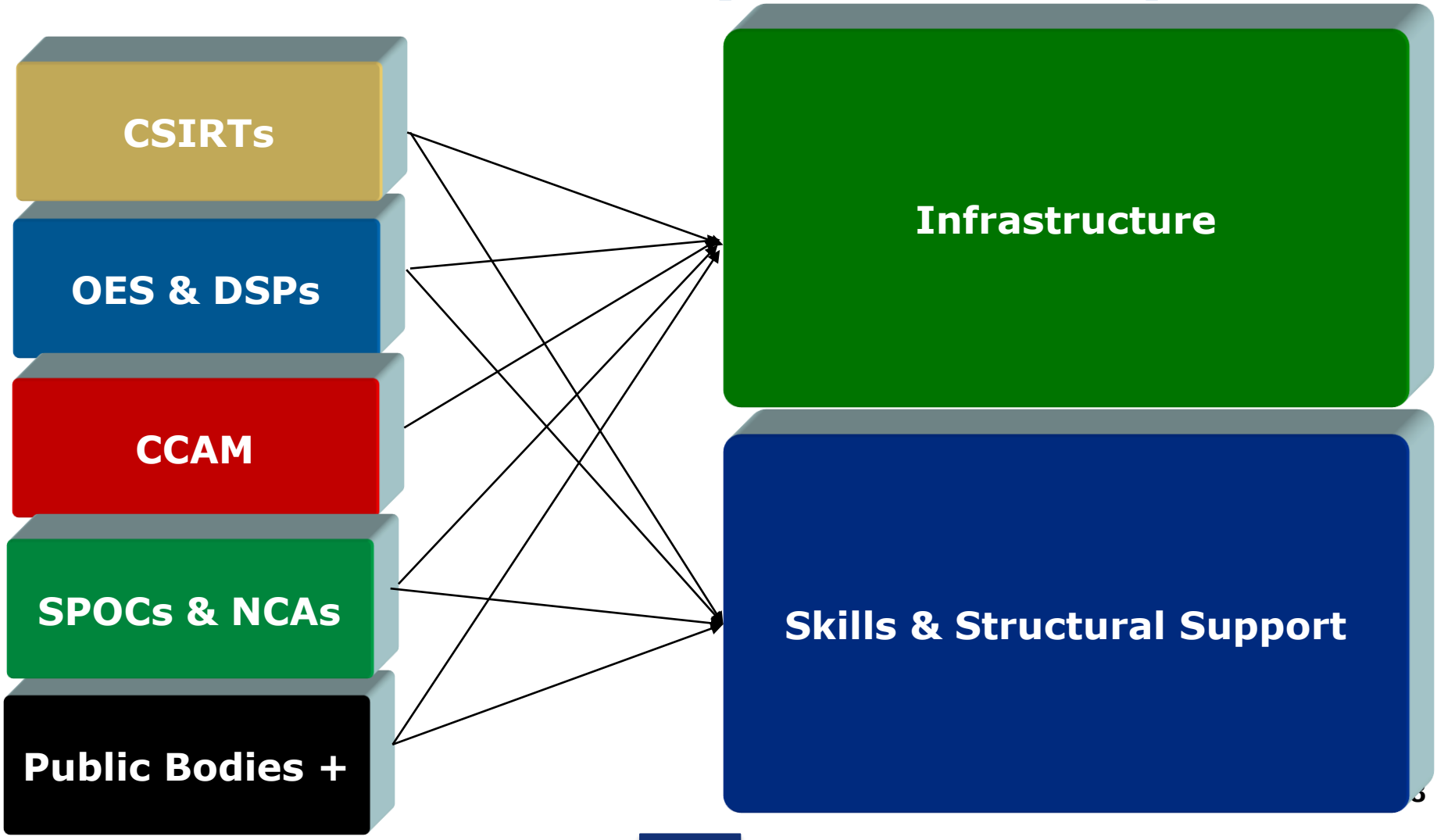
CEF 2018 Call: Key Facts

CLOSED, 22 Nov!

- Cybersecurity **capability development** for different entities
- **€13** million in total
- **Grants**:
  - ✓ Co-funding up to 75% of the eligible costs of the action
  - ✓ Pre-financing: 50% within 30 days after signed grant agreement, balance on completion
  - ✓ Funding per proposal: Various, depending on the objective, EC (expected) contribution ranges from € 100,000 up to €1,000,000 per action
- Indicative duration of the actions: **24 months**

- *Link to call text: https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/apply-funding/2018-cyber-security*

CEF-TC-2018-3: Cyber Security



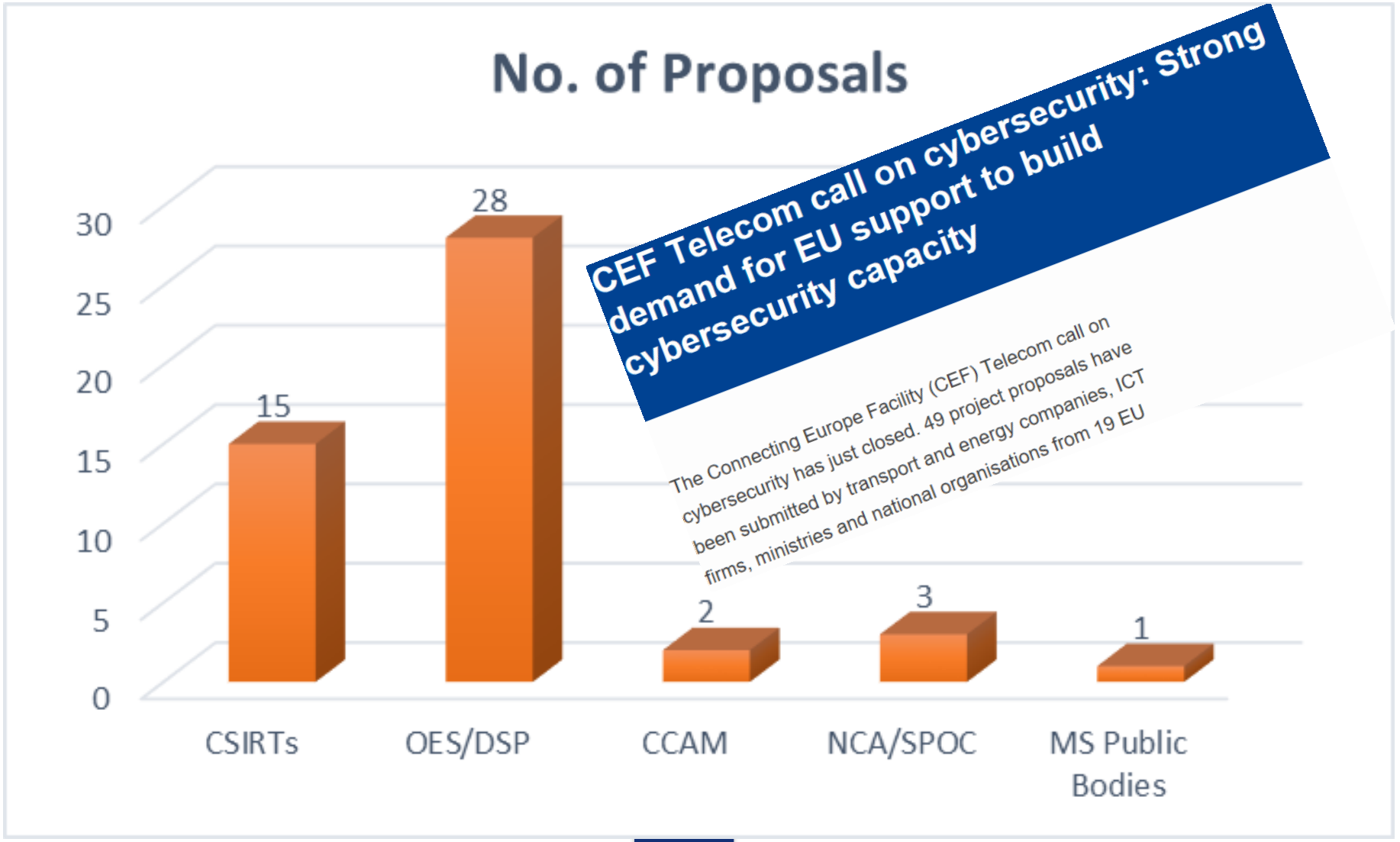
Capabilities Development: Infrastructure (for OES, DSPs)

Examples being*: "acquisition and operation of cybersecurity IT systems (Security Operations Centres, firewalls, intrusion detection/prevention, monitoring equipment and software); training facilities; self-assessment security and reporting toolkits; auditing tools (vulnerability assessment, penetration testing); Security Incident and Event Management infrastructure; honeypots; simulation environments; other software tools for automation, risk and threat assessment, incident and event management, forensic computing."*

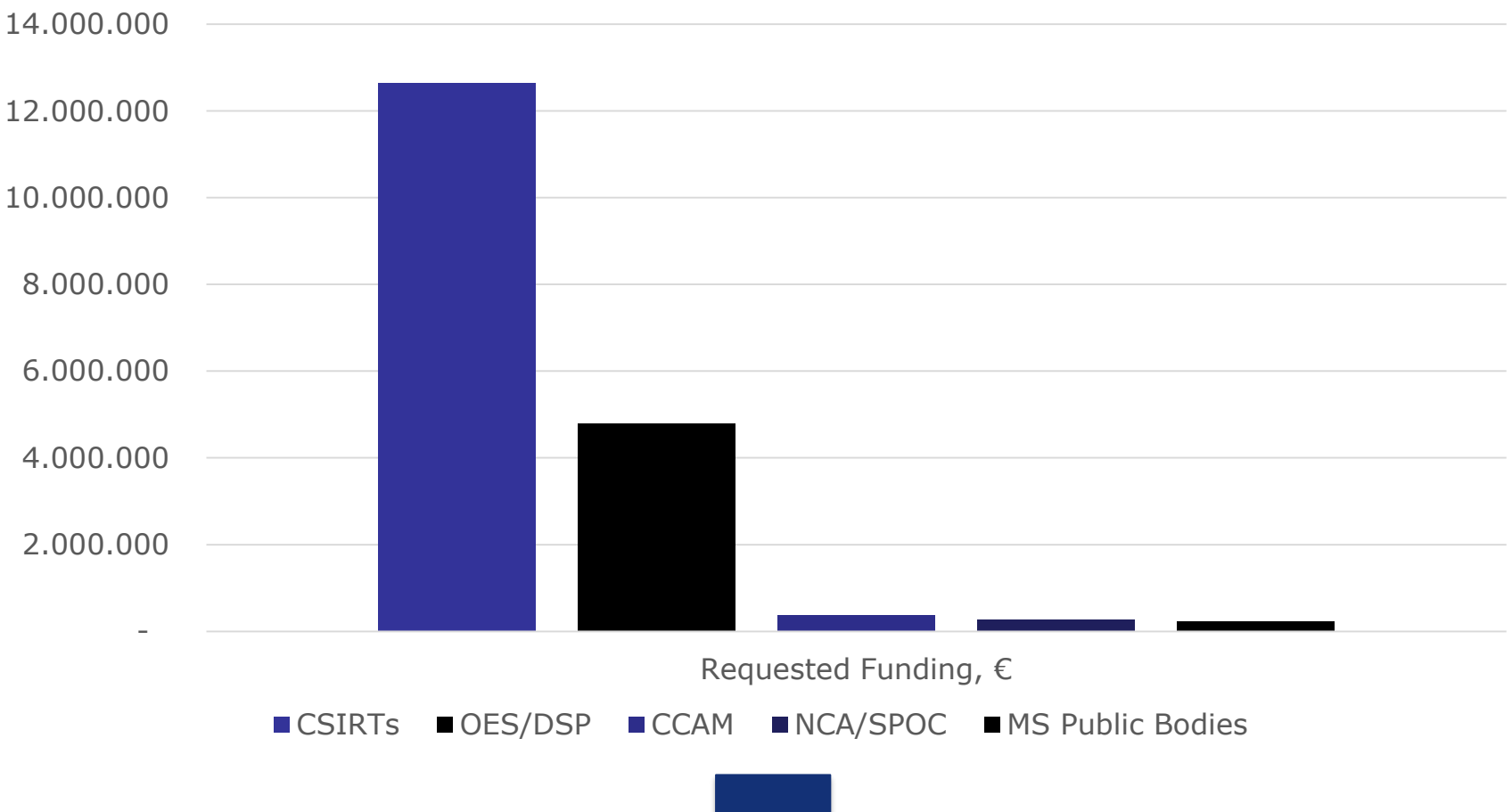
Capabilities Development: Skills and Structural Support

Examples being*: "staff awareness raising, awareness campaigns and training courses; "capture the flag" cybersecurity challenges, "Red and Blue teaming", hackathons, cyber exercises (including Europe-wide events); legal compliance and organisational analysis; risk management; business continuity and disaster recovery planning".*

CEF 2018 Call: Initial Feedback



Requested Budget: 18.3mEUR



2018 Call: Next Steps

- *Eligibility Checks* *-underway*
- *Evaluation* *-December to February 2019*
- *Results* *-April 2019*
- *Grant Agreements* *-April to August 2019*

Outlook 2019-2020

- *CEF Telecom 2019 Work Programme*
  - **Under deliberation –1st Draft Discussed with MS**
  - **Revised Draft to be circulated to MS prior to January CEF Telecom Committee**
  - **Likely to be finalised in Q1 2019**
  - **Basis for 2019 CEF Cybersecurity Call**
- *CEF Telecom 2020 Work Programme*
  - **Deliberations in 2019**

Next Multi-Annual Financial Framework 2021-2027

- *Commission Proposals Published on 6th June last*
  See: https://ec.europa.eu/commission/publications/connecting-europe-facility-digital-europe-and-space-programmes_en

- *New "Digital Europe Programme" proposed*
  - **5 Pillars –HPC, AI, Cyber, Skills, Deployment**
  - **9.2Billion EUR for 2021-2027**
  - **Includes 2Billion EUR for Cybersecurity to address fragmentation & low levels of investment**
- *CEF Final Year -2020 –DSIs (including Cybersecurity DSI) migrate to DEP*

Investing in the future: Digital Europe Programme

€2 billion for Cybersecurity to:

Support procurement of advanced equipment, tools & data infrastructures

Support the best use of European knowledge, capacity and skills

Ensure wide deployment of latest solutions across the economy

Reinforce capabilities for high level of network & information systems

Examples of level of ambition:

- By 2022: At least one cybersecurity competence centre per Member State
- By 2025: encryption techniques that can resist quantum computing

#EUBudget
#DigitalEurope

European Cybersecurity Industrial, Technology & Research Competence Centre & Network of National Coordination Centres

Building Cybersecurity Capabilities in Europe

A Competence Network and the Centre to…

- Retain and develop the cybersecurity technological and industrial capacities necessary to secure Digital Single Market
- Increase the competitiveness of the Union's cybersecurity industry
- Turn cybersecurity into a competitive advantage of other Union industries

European Cybersecurity Technology & Innovation Ecosystem

European Competence Centre:

- manage the funds foreseen for cybersecurity under Digital Europe and Horizon Europe 2021-2027
- facilitate and help coordinate the Network and Community to drive the cybersecurity technology agenda
- support joint investment by the EU, Member States and industry and support deployment of products and solutions.

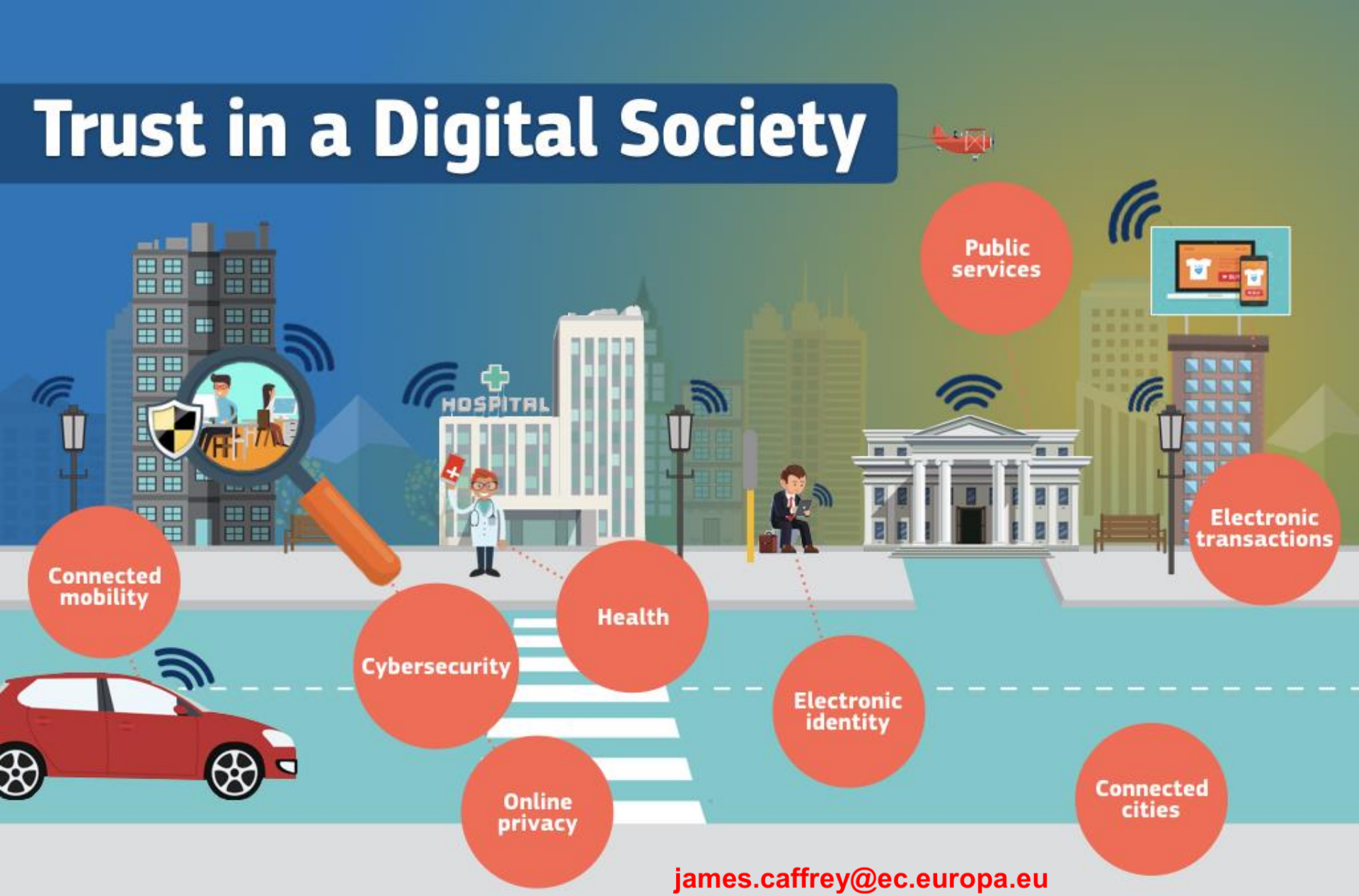
Network of National Coordination Centres:

- Nominated by Member States as the national contact point
- Objective: national capacity building and link with existing initiatives
- National Coordination Centres may receive funding
- National Coordination Centres may pass on financial support

Competence Community:

- A large, open, and diverse group of cybersecurity stakeholders from research and the private and public sectors, including both civilian and defence sectors

Trust in a Digital Society



james.caffrey@ec.europa.eu

European Commission | powered by **European Commission**, CONNECT Digital Society, Trust and Cybersecurity Directorate

bit.ly/**ECdigitalsociety**