EUROPEAN
COMMISSION

Brussels, 5.7.2016
C(2016) 4400 final

ANNEX 1

ANNEX

**CONTRACTUAL ARRANGEMENT
SETTING UP A PUBLIC-PRIVATE PARTNERSHIP IN THE AREA OF CYBERSECURITY INDUSTRIAL RESEARCH AND INNOVATION BETWEEN THE EUROPEAN UNION
AND THE EUROPEAN CYBERSECURITY ORGANISATION**

to the

Commission Decision

on the signing of a contractual arrangement setting up a public-private partnership in the area of cybersecurity industrial research and innovation between the European Union, represented by the Commission, and the stakeholder organisation

{SWD(2016) 210 final}
{SWD(2016) 215 final}
{SWD(2016) 216 final}

ANNEX

CONTRACTUAL ARRANGEMENT SETTING UP A PUBLIC-PRIVATE PARTNERSHIP IN THE AREA OF CYBERSECURITY INDUSTRIAL RESEARCH AND INNOVATION BETWEEN THE EUROPEAN UNION AND THE EUROPEAN CYBER SECURITY ORGANISATION

The European Union, represented by the Commission, and the European Cyber Security Organisation (ECSO) Association (registered offices: Rue Montoyer 10, 1000 Brussels, Belgium), hereinafter referred to as 'the Association' (jointly hereinafter referred to as 'the Parties'),

CONSIDERING THAT:

- The European Union's Horizon 2020 Framework Programme for research and innovation[1] may be implemented through public-private partnerships taking the form of a contractual arrangement between the partners committed to supporting the development and implementation of research and innovation activities of strategic importance to the Union's competitiveness and industrial leadership.

- The specific programme implementing Horizon 2020[2] has recognized that further public-private partnerships may be launched under Horizon 2020 where they meet the criteria defined in Article 25 of Regulation (EU) No 1291/2013.

- The rules for participation and dissemination in Horizon 2020[3] apply to the indirect actions to be financed by the Commission in the context of this arrangement.

- The Commission Communication of 21 September 2011 on *Partnering in Research and Innovation*[4] recognises that public-private partnerships in research and innovation are a means of strengthening the Union's competitiveness in key areas of industrial research.

---

[1] Regulation (EU) No 1291/2013 of the European Parliament and of the Council of 11 December 2013 establishing Horizon 2020 — the Framework Programme for Research and Innovation (2014-2020) and repealing Decision No 1982/2006/EC (OJ L 347, 20.12.2013, p. 104).

Regulation (EU) 2015/1017 of the European Parliament and of the Council of 25 June 2015 on the European Fund for Strategic Investments, the European Investment Advisory Hub and the European Investment Project Portal and amending Regulations (EU) No 1291/2013 and (EU) No 1316/2013 — the European Fund for Strategic Investments (OJ L 169, 1.7.2015, p. 1).

[2] Council Decision (EU) No 743/2013 establishing the specific programme implementing Horizon 2020 — the Framework Programme for Research and Innovation (2014-2020) and repealing Decisions 2006/971/EC, 2006/972/EC, 2006/973/EC, 2006/974/EC and 2006/975/EC (OJ L 347, 20.12.2013, p. 965).

[3] Regulation (EU) No 1290/2013 of the European Parliament and of the Council of 11 December 2013 laying down the rules for participation and dissemination in 'Horizon 2020 — the Framework Programme for Research and Innovation (2014-2020)' and repealing Regulation (EC) No 1906/2006 (OJ L 347, 20.12.2013, p. 81).

[4] COM(2011) 572.

- One of the key priorities of the European Cybersecurity Strategy[5] is to develop industrial and technological resources for cybersecurity, including through R&D investments and innovation.

- In its Communication *A Digital Single Market Strategy for Europe*[6], the Commission committed to initiate the establishment of a Public-Private Partnership on cybersecurity in the area of technologies and solutions for online network security in the first half of 2016, recognizing that specific gaps still exist in the fast moving area of technologies and solutions for online network security and that a more joined-up approach is therefore needed to step up the supply of more secure solutions by European industry and to stimulate their take-up by enterprises, public authorities, and citizens.

- The Commission Communication *Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry*[7] highlights that a comprehensive approach to cyber-resilience and cyber security industrial policy is needed, including research and innovation.

- The related industry proposal and the multi-annual research and innovation roadmap received from the Association (hereinafter referred to as "Industry Proposal") on 18 April 2016 have been evaluated by the Commission services, assisted by independent experts, and found to fulfil the criteria referred to in Article 25(3) of Regulation (EU) No 1291/2013. The related Industry Proposal for a partnership and the multi-annual research and innovation roadmap(enclosed) can be taken as a basis for the cooperation under the present arrangement.

- Pursuant to Article 3 of its Statutes, the Association will engage in a public-private partnership with the European Union to boost European cybersecurity research, development, innovation and use of European cybersecurity solutions as means to support and protect the development of the Digital Single Market in Europe, foster European cybersecurity leadership for job creation and prosperity, accelerate Europe’s innovation process, and raise the competitiveness of European cybersecurity industry on the global market.

- This contractual arrangement constitutes an agreement by the Parties to lend their best endeavours to achieve the objectives set out below. This arrangement shall give rise to no liability on the part of either Party vis-à-vis the other,

RECOGNISING THAT:

- The Parties’ respective responsibilities in the above areas are mutually reinforcing.

- Due regard should be given to the Parties’ respective competences and operational

[5] JOIN(2013) 1 final.

[6] COM(2015) 192 final.

[7] COM(2016) 410.

frameworks,

HAVE DECIDED THE FOLLOWING:

1. SCOPE: The present contractual arrangement establishes a public-private partnership between the Parties in the area of cybersecurity (hereinafter referred as “the partnership”), to be implemented in an open, transparent and efficient way. The general objectives of the partnership in support of Union policies, and in particular of the specific objectives of the Horizon 2020 Framework Programme, the European Cybersecurity Strategy and the Digital Single Market Strategy, are:

    - To foster cybersecurity market development, job and wealth creation in Europe through a long term investment commitment by cybersecurity industry, research and technology organisations (RTOs), academia, the European Commission, Member States' public administrations participating in the partnership as well as cybersecurity solution users;
    - To develop, pilot and bring to market, in an agreed strategic approach, technological solutions and services within an ecosystem that helps to support the goals of the European Digital Single Market;
    - To support the use of innovative trusted solutions and services for major societal and economic challenges in Europe, e.g. in different essential services providers, particularly in areas where Europe has a competitive advantage (e.g. health, energy, transport, internal security, public services / eGovernment, ICT mobile and fixed devices / networks, Industry 4.0);
    - To accelerate Europe’s innovation process and time to market by addressing the full innovation and value chain of cybersecurity in different application sectors;
    - To foster the development of Europe's cybersecurity industry by creating a Europe-wide technology and application base, building up competence and competitive European cybersecurity companies, including SMEs, facilitating the acceleration of business ecosystems and appropriate business models with a particular focus on SMEs, start-ups and high growth companies;
    - To mobilise and leverage public and private resources to provide contributions to the development and implementation of European cybersecurity policies, regulations and standards (e.g. contributions to European policies; support to implementing legislation like NIS Directive, eIDAS regulation; contributing to creation and updating of ETSI/CEN/CENELEC standards).
    - To increase the awareness and demonstrate the value of cybersecurity solutions for businesses (including decision makers) and the public sector to accelerate the take-up, but also to improve the cybersecurity awareness among citizens and skills development of experts.

2. SPECIFIC OBJECTIVES: The Parties will cooperate, taking into account the Industry Proposal, to develop, implement and support a multi-annual research and innovation agenda. The objectives of the Industry Proposal, including the Key Performance Indicators (KPIs), have been developed in cooperation with the different

stakeholders. The Industry Proposal provides evidence for consistency of the activities of the contractual agreement with existing European policies and initiatives. The Industry Proposal is also looking at how to avoid duplication with other R&D initiatives at European or national level.
The specific objectives of the partnership are to:

OBJECTIVES FOR IMPROVED COMPETITIVENESS

- Support the evolution of cybersecurity revenues in the European and global market, including positioning of the European industry and aiming at maintaining the European cybersecurity market share at least at 25% of the global market and attaining a yearly growth of the European cybersecurity market of at least 8% by 2020;
- Develop solutions leading towards the use of cybersecurity technologies in the fields of different vital infrastructure and service providers, in particular where Europe has a competitive advantage (e.g. health, energy, transport, internal security, public services / eGovernment, ICT mobile and fixed devices / networks, Industry 4.0);
- Support activities for increased industrial competitiveness of Europe through the development and implementation of cybersecurity industrial measures (e.g. standardisation, use of testing, validation, certification infrastructures as well as trust labelling procedures, best practices and pilots for innovative elements of the supply chain, link to regulations). The development of certification activities in cybersecurity will consider Regulation 765/2008 and Decision 768/2008 and certification provisions included in the General Data Protection Regulation 2016/679;
- Stimulate existing and new alliances and the ecosystems along and across the value chain that reinforce competitive capabilities of Europe's cybersecurity industry in existing market segments or help address new market segments;
- Support the development and link of clusters as a mechanism at local level and beyond (Regional / National) to develop the market and support SMEs and start-ups;
- Support the emergence of start-ups with products / services that effectively reach the market;
- Foster the creation of financial / investment instruments to support industry and innovation in IT and cybersecurity, helping to bring innovative solutions to full maturity as well as stabilize / develop SMEs: e.g. entrepreneurial (private fund) and venture capital (bank / financial entities) investments funds, cybersecurity bonds (corporate bonds).;
- Support innovation in companies with high growth potential to achieve next level in business developments and cross-border solution delivery.

INNOVATION OBJECTIVES

- Support the widest and best market uptake of innovative cybersecurity technologies and services for professional and private use by accelerating the

wide diffusion of cybersecurity technologies in many industry sectors and the emergence of new business opportunities;

- Make the innovation process more inclusive, sustainable and effective through the direct involvement of players along and across the full value chain, including those communities, like “white hackers” and “open source”, that could bring disruptive views and breakthrough innovation;
- Facilitate networking between different actors (suppliers, users, R&D centres, public actors etc.) to find synergies and decrease the effects of fragmentation in the cybersecurity field;
- Support the creation of European-wide ecosystem for networking, training, testing and experience exchange through a network of integrated technical exercises environments, also to validate technologies from a technical and business perspective;
- Contribute to activities for pre-standardisation and / or standardisation to support development and use of products and services that meet the requirements set out in relevant legislation;
- Support the development of a trusted European cybersecurity supply chain where relevant, for higher technological independence at National / European level, by creating a catalogue of trusted products and companies, and by increasing the visibility of SMEs, promoting the European cybersecurity offerings and allowing informed procurement;
- Support increased use of trusted European certified or labelled solutions introduced in the different markets / applications;
- Plan funding for disruptive innovation through accelerators and / or SME associations or clusters to improve funding opportunities for small players (start-ups, SMEs, high-growth companies).

SOCIETAL OBJECTIVES

- Maintain and develop employment in cybersecurity sectors (supply and users / operators) in the European Union;
- Develop and implement European approaches for cybersecurity, trust, privacy and data protection by design:
    - Develop new personalised and enhanced technologies, products and services adapted to consumers' and organisations’ needs that will respect security and integrity of data and ensurethe protection of personal data in a manner that is compliant with the new General Data Protection Regulation[8];
    - Foster trust in the data-driven economy, including through incentivizing the application of the principles of privacy, personal data protection and security by design as well as the cooperation with relevant authorities in case of data breaches and cyber incidents;

[8] 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) OJ 119 04.05.2016

- Support the implementation of eIDAS Regulation as well as the development and uptake of high-security authentication tools by citizens to protect their identity and assets in the cyber domain;
- Address acceptance of new cybersecurity technologies by society and consumers by identifying potential barriers.

- Develop education, training and skills on cybersecurity products and safe use of IT tools in Member States for individuals and professionals:
  - Support widespread know-how, education and skills in Europe through curricula to stimulate higher education;
  - Develop an ecosystem that supports the general awareness raising and basic-hygiene skills development in the cybersecurity field for citizens in Europe to help manage the risks that have come along with the ever-increasing digital dependencies of every-day actions of the citizens;
  - Foster the development of new cybersecurity training modules to be integrated into training programs in different educational levels to provide basic skills and awareness of cyber threats also in traditional educational training;
  - Support the increase of in-depth cybersecurity training and education opportunities for securing a skilled workforce for cybersecurity industry as well as provide cybersecurity experts for public sector organisations and critical infrastructure / essential service providers, in particular through the EIT Digital (European Institute of Innovation and Technology Knowledge and Innovation Community on Digital) action line on Privacy, Security & Trust.

OPERATIONAL OBJECTIVES

- Focus investments (R&I, capability, competence and capacity building) in the cybersecurity sectors driven by the partnership objectives and strategy:
  - Define in cooperation with the Commission, a Strategic Research and Innovation Agenda (SRIA) including its coordination with other sectorial Research and Innovation Strategies;
  - Link H2020 with other European and National funds (e.g. European Fund for Strategic Investments - EFSI, European Structural and Innovation Fund - ESIF, Connecting Europe Facility – CEF) contributing to the leverage factor, to bring innovation to market in an end to end approach;
  - Implement Europe-wide strategic projects for specific deployments of existing or near-to-market technologies that demonstrate the potential impact of cybersecurity products across sectors;
  - Encourage SME participation in this initiative so that they represent (target value) 20-25% of all participant organisations;
  - Encourage participation of users in the definition of R&I priorities and in R&I projects, contributing to bring innovations to the market.
- Provide efficiency, openness and transparency of the PPP Consultation Process:

- Support and monitoring the implementation of the partnership objectives, providing the European Commission with the information relative to the Key Performance Indicators of the PPP on cybersecurity and contributing to the control of the results of the R&I projects;
- Maintain an effective flow of information between partnership projects that overcomes barriers and promote synergies while respecting individual beneficiaries' interests and rights, enabling cooperation between projects in support of common targets to positively impact European society and economy.

- Coordinate the partnership implementation with EU Member States, Regions, other national public administrations participating in the partnership, Third Countries and other H2020 instruments and sectorial PPP's:
  - Cooperate with Third Countries to harmonise approaches in the cybersecurity market, in particular foster the development and use of international standards wherever possible;
  - Coordinate implementation of the partnership strategy also combined with regional and national activities and funds in the specific sectors;
  - Foster the creation of national PPPs and local / national cybersecurity association / clusters to better coordinate cybersecurity activities at regional level and market growth;
  - Coordinate with relevant sectorial PPP's in order to benefit from synergies and promote common standards and solutions.
- Dissemination and Awareness making the partnership action and results visible in Europe and internationally, to a broad range of public and private stakeholders:
  - Provide regular information and tangible examples about how cybersecurity, privacy and personal data protection respecting solutions contribute to trusted daily lives of individuals in the European Union and the economic sector by using various communication channels;
  - Organisation, contribution and support to the Annual Cybersecurity partnership conference, of Info-Days and Brokerage events.

3. ACTIVITIES, INVESTMENT and OUTPUTS: The research and innovation activities undertaken under this partnership may result in project proposals to be co-funded under the Horizon 2020 Framework Programme , subject to the Horizon 2020 rules on participation and dissemination. For the period 2017-2020, the Commission (DG Communications Networks, Content and Technology) intends to allocate an indicative financial envelope of EUR 450 million for those activities. The allocations will be included in the periodic Horizon 2020 work programmes.

The Association commits itself to attracting the stakeholder community's investment in research and innovation activities in the form of support, complementing the Commission's, for projects implementing the research and innovation agenda under the

Horizon 2020 Framework Programme, and of other outputs outside it, as referred to in point 6 and in the Annex.

4. GOVERNANCE: The Parties will establish a Partnership Board as the main mechanism for dialogue to reach the objectives of this contractual arrangement. The Board will comprise members nominated by the Association, ensuring proper representation of the wider community of stakeholders, and Commission representatives from the relevant services in charge of the Union financial contribution according to the modalities described in section 3 above.

The Partnership Board will establish its rules of procedure on the basis of a draft presented by the Commission, which will cover *inter alia* issues relating to confidentiality, transparency and the avoidance of conflicts of interest. The Parties may also meet at high level to review the work of the Board, take stock of progress achieved by the partnership and discuss further ways of enhancing cooperation.

The Association will decide on its own governance structures and implement the appropriate consultation processes, based on openness and transparency, to ensure that all relevant stakeholders are involved as appropriate in the preparation of the inputs to the Commission.

5. SPECIFIC COMMITMENTS BY THE COMMISSION: The Commission commits itself to giving due consideration to inputs and advice from the Association in order to identify research and innovation activities to be proposed for financial support under the Horizon 2020 Framework Programme. To that end, it undertakes to maintain regular dialogue with the Association during the preparatory phase of the drafting of the work programmes referred to in Article 5 of the specific programme. In this context, the Commission will ensure through the Partnership Board's rules of procedure that the inputs and advice received from the Association are developed with the involvement of all relevant stakeholders as appropriate and will pay particular attention to the openness to new members of the Association's governance structure.

6. SPECIFIC COMMITMENTS BY THE ASSOCIATION: The Association commits itself to providing inputs and advice to the Commission to achieve the objectives of the partnership, in particular to contribute to identifying research and innovation activities to be included in the Horizon 2020 work programmes in view of financial support following the calls for proposals. It also undertakes to:

- Leverage the partnership investments through sector investments of 3 times the total estimated partnership budget;
- Establish an open, transparent and inclusive approach to determining and updating the SRIA
- Increase the current level of investment in education, awareness and training across the supply chain and citizens;

- Facilitate, together with the public side, that at least 25% of the participants of the calls to be funded are SMEs, start-ups or high growth companies (50+% increase in annual revenue);
- Gather information to support the *ex post* assessment of the projects implemented under the partnership;
- Facilitate moving successful results into standards (for fast market uptake) and product enhancing services;
- Bring innovative results to market via systematic use of the whole set of funding tools (at European and national level; public and private), showing the benefits and the link between European / National funds, European policies and market growth;
- Implement a cross-fertilisation platform which gathers all main public deliverables from projects, supporting collaboration and clustering along main horizontal issues;
- Ensure that the achieved results are fully compliant with relevant Union legislation;
- Leverage the EIT Digital KIC (Knowledge and Innovation Community selected by the European Institute of Innovation and Technology) Privacy, Security & Trust action line to develop skills and competences in trust and security;
- Work with other PPPs to align goals and activities so as to ensure synergies;
- Disseminate successful results within and between sectors and across value chains through effective linking of participants;
- Actively involve all relevant sector players, in particular from the application areas, and put in place mechanism to secure their participation for the successful development of innovative new business models;
- Put in place governance structures which on the one hand promote openness, transparency and representativeness, and on the other hand ensure efficient management with minimal overheads.

The Association will provide to the Commission on an annual basis evidence that it is fulfilling its commitment to the objectives of the partnership, addressing the key performance indicators, and ensure that the specific commitments expressed in this Contractual Arrangement, in particular in terms of additional research and innovation investments (see Industry proposal), are respected. It will invite the Commission to attend its General Assembly and other relevant meetings, subject to its own procedures.

7. MONITORING: With due regard to their respective competences, institutional settings and operational frameworks, the Parties will regularly inform and consult each other, as appropriate, in particular in order to monitor the progress of the partnership towards its objectives and assess the impact of its activities and the leverage of additional investments. The key performance indicators will include the following:

IMPACT ON INDUSTRIAL COMPETITIVENESS AND THE ECONOMY

- European cybersecurity market share at least 25% of the global market;
- Yearly growth of the European cybersecurity market at least of 8% by 2020;
- Increase the number of certified companies and products based on the existing European Common Criteria or SOG-IS certification schemes, and other possible

future European ICT security certification frameworks, in particular those compliant with the provisions of Regulation 765/2008 and Decision 768/2008, to bridge the gap between Innovation and Market;

- Monitor the take-up of research and innovation output coming from the partnership in the development of novel cybersecurity products and services;
- Increase participation to at least 15% of users in partnership projects by 2020;
- Implementation of at least 4 large scale projects funded by H2020 for critical infrastructure protection;
- At least 80% of funding to projects that have a technical solution or service as a final outcome;
- Increase SMEs and high growth companies (year-over-year growth over 50%) participation and funding in H2020 projects above the H2020 target of 20%;

SOCIO-ECONOMIC IMPACTS

- Growth of the cybersecurity related employment, expected target 10% growth per year;
- Development of cybersecurity companies, increasing job creation, keeping competences and capacities in Europe, while respecting Union law;
- Development of cybersecurity education and training for citizens and professionals to enhance the awareness of threats and needed skills for safe use of IT tools;
- Large scale international exercises using European based exercise ecosystem;
- Increase the use of security, privacy and data protection by design enhancing technology in public procurement, and contribute to the development of a prototype for a European catalogue of ICT standards for public procurement[9];

OPERATIONAL ASPECTS

- Monitor progress of the partnership implementation and of its R&I strategy: Number of R&I projects funded; Time to contract; Statistics of response to calls; Consistency of approved projects against partnership strategy and KPIs;
- Monitor progress against the multi-annual research and innovation roadmap: Number of systems and technologies developed in the relevant sector in partnership projects;
- Coordination of the partnership strategy implementation also combined with regional and national activities and funds in the specific sectors;
- Cooperation with Third Countries to develop coherent approaches in the cybersecurity market: identification and measure of common events, meetings and concrete activities (projects, standards, mutual recognition etc.);
- Dissemination of information and tangible examples on a quarterly basis about how cybersecurity, privacy and personal data protection respecting solutions contribute to trusted daily lives of individuals in the European Union and the

[9] COM(2016) 179 final EU eGovernment Action Plan 2016-2020, Accelerating the digital transformation of government

economic operators by using various communication channels like social media, web, video, articles and publications, press releases, success stories, etc;

- Awareness and information actions for promoting the PPP activities to a broad range of stakeholders: events with European and National Institutions, targeted Newsletters, social media, etc;
- Organisation, contribution and support to the Annual Cybersecurity partnership conference, starting in 2017, of Info-Days and Brokerage events.

The Commission will regularly monitor progress towards achievement of the objectives, for the duration of the contractual arrangement and for three years afterwards, in particular on the basis of evidence to be provided by the Association.

8. APPLICATION OF THIS ARRANGEMENT: Any provision of this contractual arrangement takes precedence over the related Industry Proposal and the multi-annual research and innovation roadmap, referred to above. Any issues relating to the interpretation and implementation of the arrangement will be resolved in consultation between the Parties. Amendments to this arrangement may be requested by either of the Parties by registered letter.

9. DURATION AND REVIEW: This contractual arrangement will enter into force on 05 July 2016 and remain in force until 31 December 2020. Either of the Parties may at any time communicate by registered letter its intention to terminate this arrangement, giving reasons for doing so. Both sides may terminate the Contractual Agreement regardless of the reasons stated. The termination will become effective three months after the receipt of this registered letter.

The Commission will undertake, with the assistance of independent experts, a review of the partnership, taking into account performance and progress towards its objectives, before the end of Horizon 2020.

The related Industry Proposal for a partnership (entitled "*European Cybersecurity Industry Proposal for a contractual Public-Private-Partnership*") and the multi-annual research and innovation roadmap for the partnership (entitled "*European Cybersecurity Strategic Research and Innovation Agenda (SRIA) for contractual Public-Private-Partnership (cPPP)*"), whose contents is the sole responsibility of their authors, constitute supporting documents and are enclosed to the present contractual arrangement.

Done in duplicate at Strasbourg on 05 July 2016,

FOR THE EUROPEAN COMMISSION	FOR THE EUROPEAN CYBER SECURITY ORGANISATION (ECSO) ASSOCIATION
Günther Oettinger Member of the Commission in charge of the Digital Economy & Society	ECSO Chairman